**Міністерство освіти і науки України  
Національний технічний університет України  
«Київський політехнічний інститут імені Ігоря Сікорського»  
Факультет інформатики та обчислювальної техніки  
Кафедра обчислювальної техніки**

**Лабораторна робота №2**

з дисципліни  
«Технології розроблення системних програм»

на тему  
«Дослідження структури програм формату COM.»

Виконав: Перевірив:

студент групи ІП-84 доц. кафедри ОТ  
Ковалишин Олег Юрійович Павлов В. Г.  
номер залікової книжки: 8410

Київ 2020

**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**

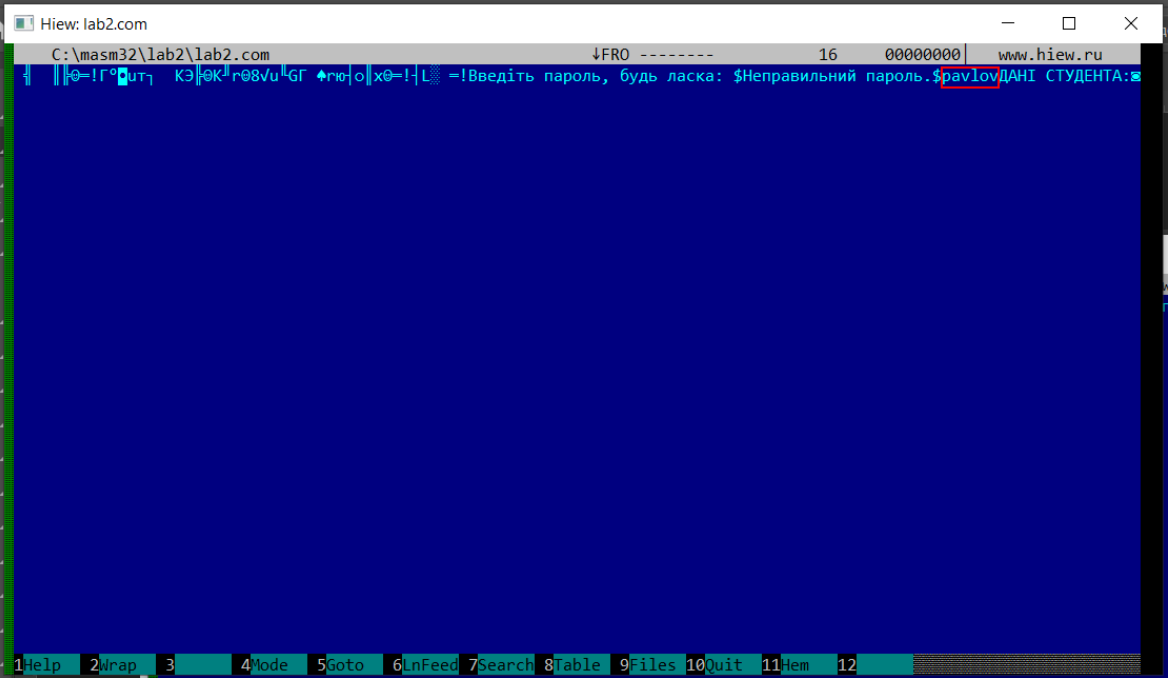
1. Вивчити структуру програм формату COM і застосування переривань BIOS та MS-DOS при роботі з консоллю.
2. Розробити програму на мові Асемблер, за допомогою якої на екран системної консолі по введеному паролю виводяться персональні дані студента – ПІБ, дата народження, номер залікової книжки тощо (див. 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.
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. Виконати шифрування пароля за допомогою функції XOR, 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.

**Вихідний код**

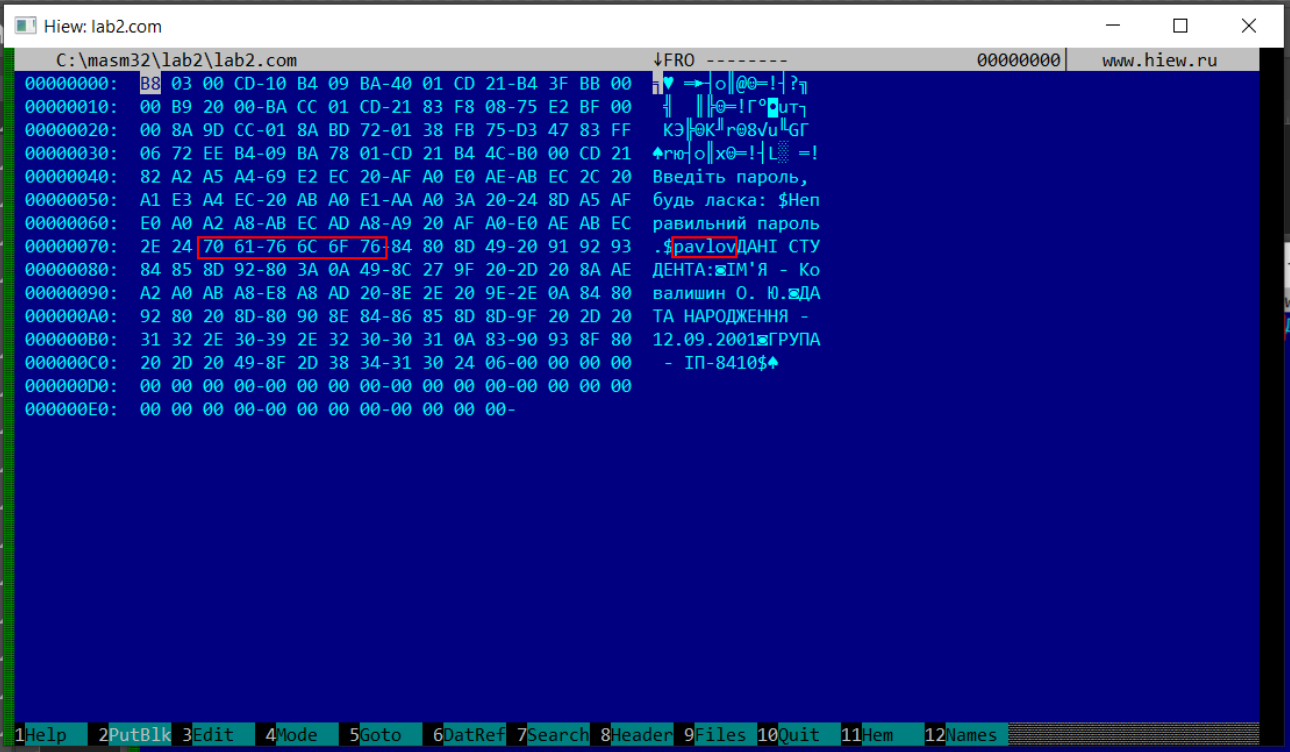
|  |  |  |  |
| --- | --- | --- | --- |
| **Default** | **Decode Default** | **XOR** | **Decode XOR** |
| .model tiny  .data  START\_MSG DB "Введiть пароль, будь ласка: $"  ERROR\_MSGDB "Неправильний пароль.$"  PASSWDDB "pavlov"  DATA DB "ДАНI СТУДЕНТА:", 10,  "IМ'Я - Ковалишин О. Ю.", 10,  "ДАТА НАРОДЖЕННЯ - 12.09.2001", 10,  "ГРУПА - IП-8410$"  PASSWD\_LEN DB 6  USR\_INPUTDB 32 DUP (?)  .code  org100h  .startup  MAIN:  ; CLEARING SCREEN  MOV AX, 03h  INT 10h  ; PRINTING START MESSAGE  MOV AH, 09h  MOV DX, offset START\_MSG  INT 21h  ; READING USER'S INPUT  MOV AH, 3Fh  MOV BX, 0  MOV CX, 32  MOV DX, offset USR\_INPUT  INT 21h  ; CHECKING LENGTH  CMP AX, 8  JNE MAIN  MOV DI, 0  VALIDATION:  ; COMPARING CHARACTERS  MOV BL, USR\_INPUT[DI]  MOV BH, PASSWD[DI]  CMP BL, BH  JNE MAIN  ; INCREASING COUNTER  INC DI  CMP DI, 6  JB VALIDATION  MOV AH, 09h  MOV DX, offset DATA  INT 21h  ; END PROCESS  EXIT:  MOV AH, 4Ch  MOV AL, 0  INT 21h  END | 1mov ax,3  int 010  mov ah,9  mov dx,00140 ;'☺@'  int 021 ;'!'  mov ah,03F ;'?'  mov bx,0  mov cx,00020 ;' '  mov dx,001CC ;'☺╠'  int 021 ;'!'  cmp ax,8  jnz 000000000 --↑1  mov di,0  2mov bl,[di][001CC]  mov bh,[di][00172]  cmp bl,bh  jnz 000000000 --↑1  inc di  cmp di,6  jc 000000021 --↑2  3mov ah,9  mov dx,00178 ;'☺x'  int 021 ;'!'  mov ah,04C ;'L'  mov al,0  int 021 ;'!'  and b,[bp][si][-05B5B],069 ;'i'  loop 000000033 --↑3  and [bx][-01F60],ch  scasb  stosw  in al,dx  sub al,020 ;' '  mov ax,[0A4E3]  in al,dx  and [bp][di][-01E60],ch  stosb  mov al,[0203A]  and al,08D ;'Н'  movsw  scasw  loopne 000000002 --↑1  mov [0ABA8],al  in al,dx  lodsw  test al,0A9 ;'й'  and [bx][-01F60],ch  scasb  stosw  in al,dx  and al,070 ;'p'  popa  jbe 0000000E2 --↓2  outsw  jbe 0FFFFFFFD --X  or b,[di][02049],091 ;'С'  xchg dx,ax  xchg bx,ax  test [di][-06D73],al  cmp b,[bp][si],00A  dec cx  mov [bx],fs  lahf  and [di],ch  and [bp][si][-05D52],cl  mov al,[0A8AB]  call 0FFFFAE3F --X  and [bp][0202E],cl  sahf  or al,cs:[si][-06D80]  and b,[bx][si],08D ;'Н'  adc b,[bx][si][-07B72],086 ;'Ж'  test [di][-06073],cx  and [di],ch  and [bx][di],dh  xor ch,[03930]  xor dh,cs:[bx][si]  xor [bx][di],dh  or al,[bp][di][-06C70]  pop w,[bx][si][02D20]  and [bx][di][-071],cl  sub ax,03438 ;'48'  xor [bx][si],si  and al,6  add [bx][si],al  add [bx][si],al  add [bx][si],al  add [bx][si],al  add [bx][si],al  add [bx][si],al  add [bx][si],al  add [bx][si],al  add [bx][si],al  add [bx][si],al  add [bx][si],al  add [bx][si],al  add [bx][si],al  add [bx][si],al  add [bx][si],al  add [bx][si],al | .model tiny  .data  START\_MSG DB "Введiть пароль, будь ласка: $"  ERROR\_MSG DB "Неправильний пароль.$"  PASSWD DB "bsd~}d"  PASSWD\_KEY DB 12h  DATA DB "ДАНI СТУДЕНТА:", 10,  "IМ'Я - Ковалишин О. Ю.", 10,  "ДАТА НАРОДЖЕННЯ - 12.09.2001", 10,  "ГРУПА - IП-8410$"  PASSWD\_LEN DB 6  USR\_INPUT DB 32 DUP (?)  .code  org 100h  .startup  MAIN:  ; CLEARING SCREEN  MOV AX, 03h  INT 10h  ; PRINTING START MESSAGE  MOV AH, 09h  MOV DX, offset START\_MSG  INT 21h  ; READING USER'S INPUT  MOV AH, 3Fh  MOV BX, 0  MOV CX, 32  MOV DX, offset USR\_INPUT  INT 21h  ; CHECKING LENGTH  CMP AX, 8  JNE MAIN  MOV DI, 0  VALIDATION:  ; COMPARING CHARACTERS  MOV BL, USR\_INPUT[DI]  XOR BL, PASSWD\_KEY  MOV BH, PASSWD[DI]  CMP BL, BH  JNE MAIN  ; INCREASING COUNTER  INC DI  CMP DI, 6  JB VALIDATION  ; PRINTING PERSONAL DATA  MOV AH, 09h  MOV DX, offset DATA  INT 21h    ; END PROCESS  EXIT:  MOV AH, 4Ch  MOV AL, 0  INT 21h  END | mov ax,3  int 010  mov ah,9  mov dx,00144 ;'☺d'  int 021 ;'!'  mov ah,03f ;'?'  mov bx,0  mov cx,00020 ;' '  mov dx,001d1 ;'☺╤'  int 021 ;'!'  cmp ax,8  jnz 000000000 --↑1  mov di,0  mov bl,[di][001d1]  xor bl,[0017c]  mov bh,[di][00176]  cmp bl,bh  jnz 000000000 --↑1  inc di  cmp di,6  jc 000000021 --↑2  mov ah,9  mov dx,0017d ;'☺}'  int 021 ;'!'  mov ah,04c ;'l'  mov al,0  int 021 ;'!'  and b,[bp][si][-05b5b],069 ;'i'  loop 000000037 --↑1  and [bx][-01f60],ch  scasb  stosw  in al,dx  sub al,020 ;' '  mov ax,[0a4e3]  in al,dx  and [bp][di][-01e60],ch  stosb  mov al,[0203a]  and al,08d ;'н'  movsw  scasw  loopne 000000006 --↑2  mov [0aba8],al  in al,dx  lodsw  test al,0a9 ;'й'  and [bx][-01f60],ch  scasb  stosw  in al,dx  and al,062 ;'b'  jnc 0000000dd --↓3  jle 0000000f8 --x  adc al,fs:[si][-07280]  dec cx  and [bx][di][-06c6e],dl  test [di][-06d73],al  cmp b,[bp][si],00a  dec cx  mov [bx],fs  lahf  and [di],ch  and [bp][si][-05d52],cl  mov al,[0a8ab]  call 0ffffae44 --x  and [bp][0202e],cl  sahf  or al,cs:[si][-06d80]  and b,[bx][si],08d ;'н'  adc b,[bx][si][-07b72],086 ;'ж'  test [di][-06073],cx  and [di],ch  and [bx][di],dh  xor ch,[03930]  xor dh,cs:[bx][si]  xor [bx][di],dh  or al,[bp][di][-06c70]  pop w,[bx][si][02d20]  and [bx][di][-071],cl  sub ax,03438 ;'48'  xor [bx][si],si  and al,6  add [bx][si],al  add [bx][si],al  add [bx][si],al  add [bx][si],al  add [bx][si],al  add [bx][si],al  add [bx][si],al  add [bx][si],al  add [bx][si],al  add [bx][si],al  add [bx][si],al  add [bx][si],al  add [bx][si],al  add [bx][si],al  add [bx][si],al  add [bx][si],al |

**Скріншоти**

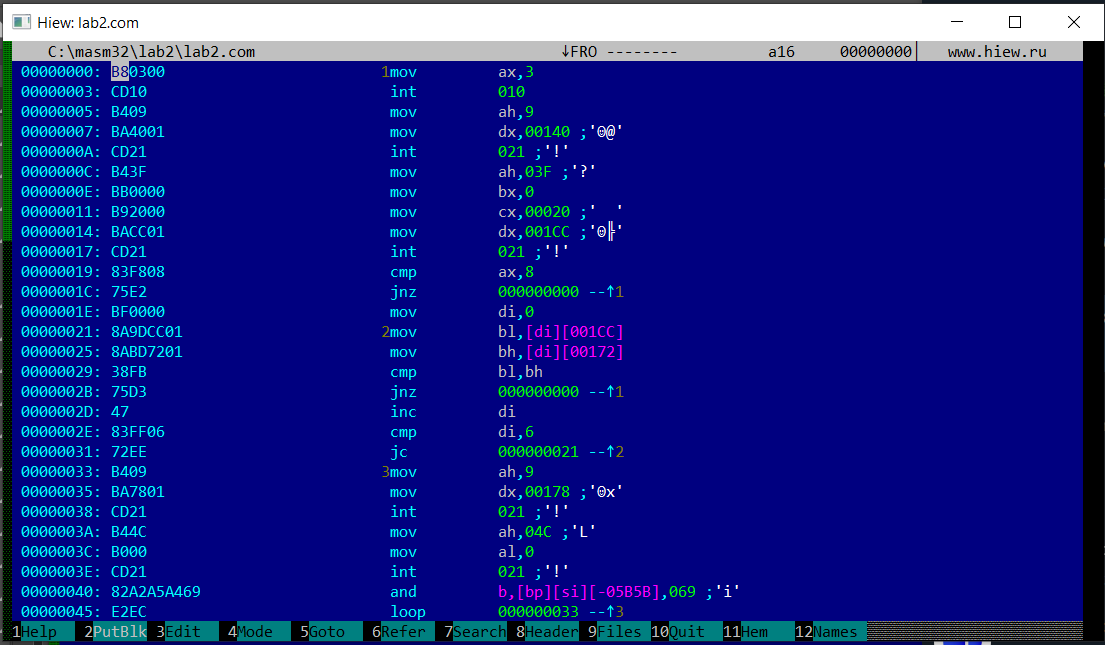
Default-Text:



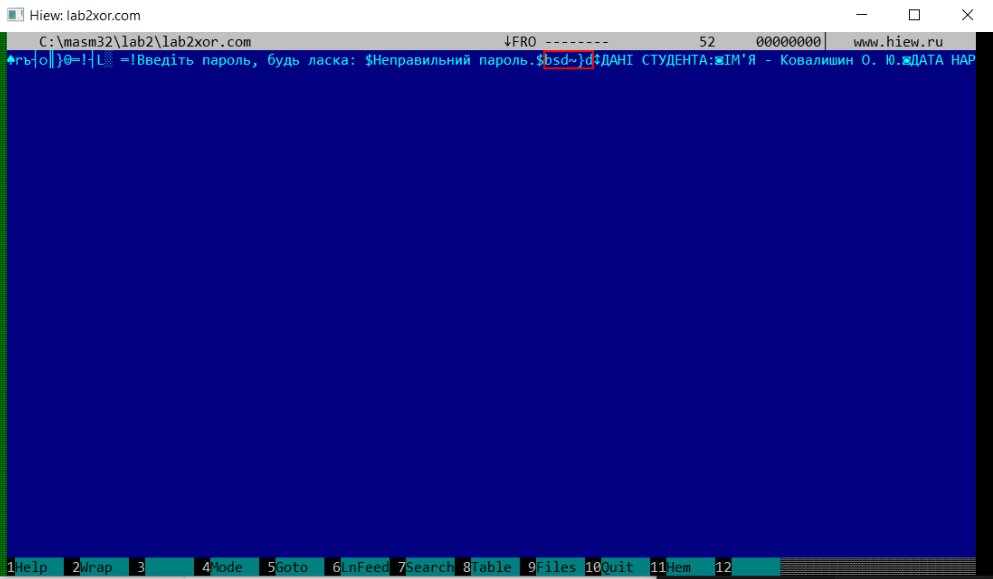
Default-Hex:

****

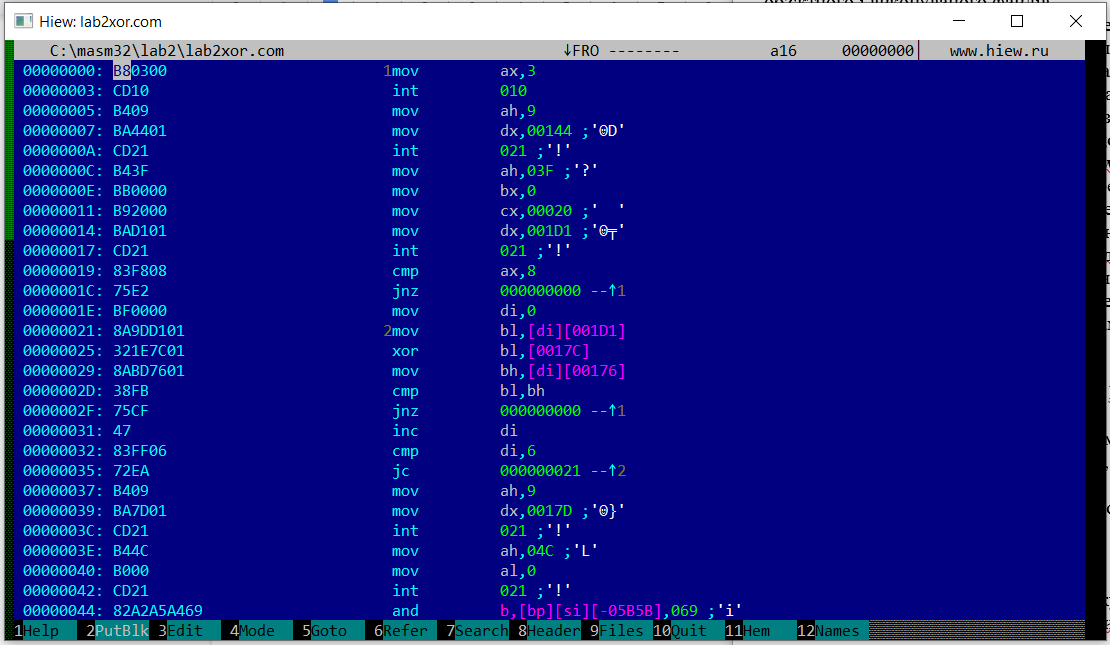
Default-Decode:

****

XOR-Text:



XOR-Decode:



**Команди MOV**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Код** | **Префікс** | **Код операції** | **Mod R/M** | **SIB** | **Зсув** | **Безпосер. операнд** |
| **mov** ax, 3 | - | B8 | - | - | - | 03 00 |
| **mov** ah, 9 | - | B4 | - | - | - | 09 |
| **mov** ah, 03F | - | B4 | - | - | - | 3F |
| **mov** bx, 0 | - | BB | - | - | - | 00 00 |
| **mov** cx, 00020 | - | B9 | - | - | - | 20 00 |
| **mov** dx, 001D1 | - | BA | - | - | - | D1 01 |
| **mov** di, 0 | - | BF | - | - | - | 00 00 |
| **mov** bl, [di][001D1] | - | 8А | |  |  |  |  |  | | --- | --- | --- | --- | --- | | 1 | 0 | 0 | 1 | **9** | | 1 | 1 | 0 | 1 | **D** | | - | D1 01 | - |
| **mov** bh, [di][00176] | - | 8A | |  |  |  |  |  | | --- | --- | --- | --- | --- | | 1 | 0 | 1 | 1 | **B** | | 1 | 1 | 0 | 1 | **D** | | - | 76 01 | - |
| **mov** ah, 9 | - | B4 | - | - | - | 09 |
| **mov** dx, 0017D | - | BA | - | - | - | 7D 01 |
| **mov** ah, 04C | - | B4 | - | - | - | 4C |
| **mov** al, 0 | - | B0 | - | - | - | 00 |

**Висновки**

Склавши дві версії програми та провівши аналіз виконуваного файлу в редакторі HIEW32, ми здобули навички написання MS-DOS застосунків,  
а також роботи з системними перериваннями. Було підключено підтримку кириличного введення та виведення тексту. Існуючу програму було удосконалено шифруванням функцією XOR для приховування явного паролю.

Таким чином, було доведено, що числові константи, рядки, змінні, команди,  
а також чутливі дані можуть бути явно виявлені у вихідному коді .COM-файлів. Крім того, було виявлено, що введений у редакторі masm-код link16.exe інтерпретує у 16-бітний формат.

Лістинг, згенерований HIEW32 містить значні відмінності від початкового коду у asm-файлі. Проаналізовано структуру, роботу, функції згенерованих команд. Було виписано команди MOV, розібрано їх на схему будови команд. Виконано инші вимоги лабораторної роботи.