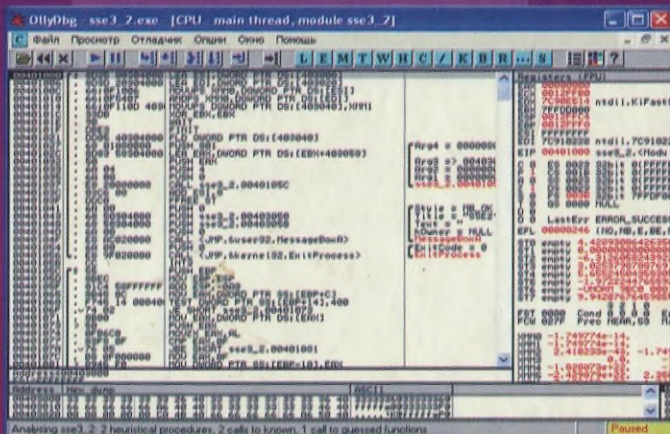


## СИСТЕМНЕ ПРОГРАМУВАННЯ

```
WndProc proc hWnd:HWND, uMsg:UINT,  
wParam:WPARAM, lParam:LPARAM  
LOCAL hdc:HDC  
LOCAL ps:PAINTSTRUCT  
.IF uMsg==WM_DESTROY  
    invoke PostQuitMessage,NULL  
.ELSEIF uMsg==WM_CHAR  
    push wParam  
    pop char  
    invoke InvalidateRect, hWnd,NULL,TRUE  
.ELSEIF uMsg==WM_PAINT  
    invoke BeginPaint,hWnd, ADDR ps  
    mov    hdc,eax
```

```
invoke TextOut,hdc,  
20,20,  
    addr char,  
1
```

```
invoke EndPaint,hWnd, ADDR
```



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ  
“ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ”

**О. М. Рисований**

# **СИСТЕМНЕ ПРОГРАМУВАННЯ**

Затверджено Міністерством освіти і науки України  
як підручник для студентів спеціальностей 7.091501 “Комп’ютерні системи та мережі”, 7.091502 “Системне програмування”,  
7.091503 “Спеціалізовані комп’ютерні системи”

**Харків 2009**

ББК 32.973-018.1

P54

УДК 004.42

Рецензенти:

*І. О. Фурман*, д-р техн. наук, проф., академік АН Вищої школи України,  
Харківський національний технічний університет  
сільського господарства;

*Г. Ф. Кривуля*, д-р техн. наук, проф., Харківський державний технічний  
університет радіоелектроніки;

*Г. І. Загарій*, д-р техн. наук, проф., Українська державна академія  
залізничного транспорту.

Гриф надано Міністерством освіти і науки України,  
лист № 1.4/18-Г-115 від 10.01.09

P54 **Рисований О. М.** Системне програмування: Підручник. - Х.: "Слово", 2009. - 848 с.

Розглянуто широке коло питань, починаючи з основ програмування на асемблері з використанням базової системи команд та закінчуючи використанням сучасних технологій обробки даних, таких, як MMX, SSE, SSE2, SSE3, SSE4. Крім того, розглянуто питання віконного програмування та організації керування апаратними пристроями. Теоретичний матеріал підкріплено великою кількістю прикладів програмного коду від самих коротких програм до програм середньої складності, виконаних в макроасемблері `masm32`. Програми з використанням команд SSE2 - SSE4 виконані в пакеті Visual Studio 2008. Всі програми протестовані за допомогою налагоджувача OllyDbg.

Призначено для студентів спеціальностей 7.091501 "Комп'ютерні системи та мережі", 7.091502 "Системне програмування", 7.091503 "Спеціалізовані комп'ютерні системи". Також може бути корисним для спеціалістів.

**ББК 32.973-018.1**

© О.М. Рисований, 2009

## ЗМІСТ

<b>ВСТУП.....</b>	<b>12</b>
<b>1. АРХІТЕКТУРНІ ОСОБЛИВОСТІ 32-РІЗРЯДНОГО МП INTEL.....</b>	<b>16</b>
1.1. Типи даних МП Intel.....	16
1.2. Регістри МП Intel.....	18
1.3. Організація пам'яті МП Intel.....	29
1.4. Способи адресації МП Intel.....	36
1.5. Контрольні запитання .....	48
<b>2. ЕТАПИ СТВОРЕННЯ ПРОГРАМИ НА МОВІ АСЕМБЛЕРУ .....</b>	<b>49</b>
2.1. Підготовка тексту програми .....	50
2.2. Асемблювання програми.....	50
2.3. Компонування програми .....	53
2.4. Налаштування програми.....	55
2.5. Редактори тексту .....	55
2.6. Контрольні запитання .....	56
<b>3. ДИРЕКТИВИ І ОПЕРАНДИ АСЕМБЛЕРУ.....</b>	<b>57</b>
3.1. Директиви асемблеру .....	57
3.1.1. Директиви MODEL, DATA, CONST, STACK, CODE .....	57
3.1.2. Директиви SEGMENT та ENDS .....	61
3.1.3. Директиви PROC та ENDP .....	62
3.1.4. Директива ASSUME .....	63
3.1.5. Директива ORG .....	63
3.1.6. Директиви визначення даних DB, DW, DD, DF, DP, DQ, DT.....	63
3.1.7. Директиви символічних констант: =, EQU, TEXTEQU .....	65
3.1.8. Директива END.....	67
3.1.9. Директива LABEL.....	67
3.1.10. Директива ALIGN.....	67
3.1.11. Директива LOCALS.....	68
3.2. Оператори мови асемблеру.....	68
3.3. Лабораторна робота “Подання даних”.....	73
3.4. Контрольні запитання .....	85
<b>4. ОПЕРАЦІЇ ПЕРЕСИЛАННЯ ДАНИХ .....</b>	<b>86</b>
4.1. Команди пересилання даних загального призначення .....	86

4.2. Організація роботи зі стеком.....	90
4.3. Команди пересилання, що працюють з акумулятором .....	95
4.4. Команди пересилання типу адреса - об'єкт.....	98
4.5. Команди пересилання бітів умов .....	99
4.6. Контрольні запитання .....	100
<b>5. АРИФМЕТИЧНІ ТА ЛОГІЧНІ ОПЕРАЦІЇ.....</b>	<b>101</b>
5.1. Арифметичні операції.....	101
5.2. Логічні операції .....	123
5.3. Лабораторна робота “Програмування арифметичних виразів” .....	129
5.4. Додатковий матеріал про налагоджувач OLLYDBG.....	135
5.5. Контрольні запитання .....	138
<b>6. ОРГАНІЗАЦІЯ РОЗГАЛУЖЕНЬ В ПРОГРАМАХ.....</b>	<b>140</b>
6.1. Команди передачі керування.....	140
6.2. Команди обробки бігів та байтів.....	158
6.3. Контрольні запитання .....	162
<b>7. ПРОЦЕДУРИ .....</b>	<b>164</b>
7.1. Директива LOCAL .....	164
7.2. Директива INVOKE .....	165
7.3. Оператор ADDR .....	165
7.4. Директива PROTO.....	166
7.5. Оператор USES.....	167
7.6. Організація процедур та їх дослідження .....	167
7.7. Windows API-подібні процедури .....	173
7.8. Непрямий виклик процедур .....	176
7.9. Використання загальних змінних у процедурах.....	180
7.10. Лабораторна робота “Передача параметрів через таблицю адреси” .....	196
7.11. Лабораторна робота “API-подібні процедури ”.....	199
7.12. Лабораторна робота “Зовнішні процедури”.....	203
7.13. Контрольні запитання .....	210
<b>8. ОРГАНІЗАЦІЯ ВВЕДЕННЯ - ВИВЕДЕННЯ В WIN32.....</b>	<b>212</b>
8.1. Загальні відомості .....	212
8.2. Набір символів і API-функції Windows.....	215
8.3. Типи даних Windows.....	215
8.4. Дескриптори консолі.....	216

8.5. АРІ-функції консолі в Win32 .....	217
8.6. Виведення повідомлень.....	221
8.7. Виведення чисел .....	229
8.8. Введення з консолі.....	239
8.9. Керування кольором.....	244
8.10. Лабораторна робота “Масиви” .....	249
8.11. Завдання для практичного виконання .....	260
8.12. Контрольні запитання .....	261
<b>9. ФАЙЛИ.....</b>	<b>262</b>
9.1. Створення файла.....	265
9.2. Читання файла.....	268
9.3. Лабораторна робота “Файли” .....	279
9.4. Контрольні запитання .....	285
<b>10. СПІВПРОЦЕСОР ТА ЙОГО ВИКОРИСТАННЯ.....</b>	<b>286</b>
10.1. Типи даних співпроцесора .....	287
10.2. Архітектура співпроцесора .....	288
10.3. Система команд математичного співпроцесора.....	292
10.3.1. Команди передачі даних.....	294
10.3.2. Команди порівняння .....	299
10.3.3. Арифметичні команди .....	309
10.3.4. Трансцендентні команди .....	332
10.3.5. Команди маніпуляції константами .....	340
10.3.6. Команди керування.....	341
10.4. Лабораторна робота “Обробка даних у співпроцесорі” .....	342
10.5. Завдання для практичного виконання .....	359
10.6. Контрольні запитання .....	360
<b>11. РЯДКИ .....</b>	<b>361</b>
11.1. Обробка рядків.....	361
11.2. Лабораторна робота “Рядки” .....	383
11.3. Контрольні запитання .....	388
<b>12. ЛОГІЧНІ СТРУКТУРИ ВИСОКОГО РІВНЯ.....</b>	<b>389</b>
12.1. Директива IF .....	389
12.2. Логічна структура switch.....	399
12.3. Логічна структура switch\$.....	399
12.4. Логічні структури .REPEAT та .WHILE .....	400
12.5. Директива .BREAK .....	410

12.6 Директива .CONTINUE .....	411
12.7. Завдання для практичного виконання.....	411
12.8. Лабораторна робота “Директиви умовного асемблювання”.....	412
12.9. Лабораторна робота “Двовимірні масиви”.....	418
12.10. Контрольні запитання .....	419
<b>13. СТРУКТУРИ.....</b>	<b>420</b>
13.1. Організація структур.....	420
13.2. Лабораторна робота “Структури”.....	426
13.3. Структура MSGBOXPARAMS в функції MessageBoxIndirect .....	431
13.4. Контрольні запитання .....	439
<b>14. МАКРОВИЗНАЧЕННЯ .....</b>	<b>440</b>
14.1. Введення в макровизначення .....	440
14.2. Директиви MACRO і ENDM .....	440
14.3. Директива LOCAL .....	443
14.4. Булеві вирази .....	443
14.5. Оператори в макровизначеннях .....	447
14.6. Оператор заміни .....	447
14.7. Оператор виразу .....	450
14.8. Оператор виділення тексту.....	451
14.9. Оператор виділення символу .....	451
14.10. Додаткові макровизначення і директиви .....	451
14.11. Категорії макросів в masm32 .....	455
14.12. Лабораторна робота “Макроси”.....	460
14.13. Контрольні запитання .....	465
<b>15. ДИНАМІЧНІ БІБЛІОТЕКИ .....</b>	<b>466</b>
15.1. Створення динамічних бібліотек та їх використання .....	466
15.2. Функція точки входу в DLL .....	471
15.3. Угорська нотація .....	472
15.4. Лабораторна робота “DLL-файли”.....	473
15.5. Контрольні запитання .....	481
<b>16. MMX-РОЗШИРЕННЯ.....</b>	<b>482</b>
16.1. MMX-команди передачі даних .....	485
16.2. Арифметичні MMX-команди .....	486
16.2.1. Команди додавання .....	486
16.2.2. Команди віднімання .....	491

16.2.3. Команди множення .....	496
16.3. MMX-команди пакування та розпакування даних .....	498
16.4. MMX-команди порівняння .....	507
16.5. Логічні MMX-команди.....	510
16.6. Команди зсуву.....	511
16.7. MMX-команди в Pentium III .....	514
16.8. MMX-команди в Pentium IV .....	515
16.9. Лабораторна робота “MMX-команди”.....	517
16.10. Контрольні запитання .....	528
<b>17. SSE-РОЗШИРЕННЯ .....</b>	<b>529</b>
17.1. Команди пересилання даних.....	532
17.2. Арифметичні команди.....	537
17.2.1. Команди додавання.....	537
17.2.2. Команди віднімання.....	541
17.2.3. Команди паралельного та скалярного множення.....	542
17.2.4. Команди паралельного та скалярного ділення .....	543
17.2.5. Додаткові арифметичні команди .....	543
17.3. Команди порівняння .....	548
17.4. Команди перетворення .....	553
17.5. Логічні команди .....	556
17.6. Команди керування станом.....	558
17.7. Команди розпаковування даних .....	559
17.8. Команди керування кешуванням.....	561
17.9. Лабораторна робота “SSE-команди” .....	562
17.10. Контрольні запитання .....	569
<b>18. SSE2-РОЗШИРЕННЯ .....</b>	<b>570</b>
18.1. Команди передавання даних .....	573
18.1.1. Обмін 128-bit кодами між оперативною пам’яттю (ОЗП) та регістрами xmm .....	573
18.1.2. Обмін 64-розрядними кодами між ОЗП і регістрами xmm.....	574
18.1.3. Використання масок .....	574
18.2. Арифметичні операції .....	575
18.2.1. Паралельні операції з упакованими числами .....	575
18.2.2. Арифметичні операції зі скалярними числами.....	577
18.3. Команди порівняння.....	579
18.3.1. Порівняння без зміни стану розрядів EFLAGS .....	579



18.3.2. Команди порівняння, які змінюють регістр EFLAGS .....	581
18.4. Логічні операції .....	581
18.5. Команди розпаковування і розподілення даних .....	582
18.6. Команди перетворення форматів даних .....	584
18.6.1. Групові перетворення форматів даних .....	584
18.6.2. Перетворення формату одного числа .....	588
18.7. Керування кешем .....	590
18.8. Операції з цілими числами.	
Нові можливості інструкцій MMX .....	590
18.9. Лабораторна робота “SSE2-команди” .....	591
18.10. Контрольні запитання .....	599
<b>19. SSE3-ПОЗШИРЕННЯ.....</b>	<b>600</b>
19.1. Перетворення чисел з плаваючою точкою (x87) в цілі числа .....	600
19.2. Дублювання даних .....	600
19.3. Завантаження невірвняних змінних.....	602
19.4. Одночасне додавання/віднімання .....	602
19.5. Горизонтальне додавання/віднімання .....	603
19.6. Синхронізація потоків.....	605
19.7. Використання SSE3 в розробці і оптимізації програм.....	605
19.7.1. Розрахункові завдання, що використовують x87 FPU .....	605
19.7.2. Обчислення з комплексними числами.....	608
19.7.3. Кодування відео.....	608
19.7.4. Векторні операції.....	609
19.8. SSSE3-доповнення .....	610
19.9. Лабораторна робота “SSE3-команди” .....	612
19.10. Контрольні запитання .....	613
<b>20. SSE4-ПОЗШИРЕННЯ.....</b>	<b>614</b>
20.1. SSE4.1-розширення.....	614
20.1.1. Прискорення відео.....	614
20.1.2. Векторні примітиви .....	615
20.1.3. Вставки/витягання .....	616
20.1.4. Скалярне множення векторів.....	616
20.1.5. Змішування.....	616
20.1.6. Перевірка бітів .....	617
20.1.7. Округлення.....	617
20.1.8. Читання WC пам’яті .....	617
20.2. SSE4.2-розширення.....	618

20.2.1. Обробка рядків .....	618
20.2.2. Підрахунок контрольної суми CRC32.....	619
20.2.3. Підрахунок популяції одиничних бітів .....	619
20.2.4. Векторні примітиви.....	619
20.3. Завдання для практичного використання.....	619
20.4. Контрольні запитання .....	619
<b>21. ОСНОВИ СТВОРЕННЯ ВІКНА ОС WINDOWS .....</b>	<b>620</b>
21.1. Створення вікна .....	620
21.2. Обробка повідомлень .....	627
21.3. Перерисовування вікна.....	630
21.4. Атрибути кольору та фону вікна.....	635
21.5. Загальні відомості про ресурси .....	635
21.5.1. Меню .....	636
21.5.2. Ресурси в Visual Studio 2008 .....	640
21.6. Функції підтримки вікон.....	642
21.7. Смуги прокрутки .....	644
21.8. Лабораторна робота “Windows-застосування” .....	645
21.9. Контрольні запитання .....	648
<b>22. РАСТРОВІ ЗОБРАЖЕННЯ.....</b>	<b>649</b>
22.1. Включення bmp-файла з використанням константи .....	649
22.2. Включення шляху знаходження bmp-файла .....	654
22.3. Створення зображення іконки.....	658
22.4. Завдання для практичного виконання .....	659
22.5. Контрольні запитання .....	659
<b>23. ГРАФІЧНІ МОЖЛИВОСТІ ТА ШРИФТИ ОС WINDOWS .....</b>	<b>660</b>
23.1. Обробка повідомлень WM_PAINT .....	661
23.2. Контекст пристрою .....	661
23.3. Графічні примітиви .....	662
23.3.1. Лінії та криві .....	663
23.3.2. Замкнуті фігури .....	665
23.4. Перо .....	669
23.4.1. Стандартне перо .....	669
23.4.2. Просте перо.....	670
23.4.3. Розширене перо .....	673
23.4.4. Косметичне перо .....	674
23.4.5. Геометричне перо.....	675
23.5. Щітки.....	676

23.5.1.	Стандартні щітки .....	676
23.5.2.	Щітка користувача.....	677
23.5.3.	Суцільні щітки .....	677
23.5.4.	Штрихові щітки .....	677
23.5.5.	Растрові щітки.....	678
23.5.6.	Структура LOGBRUSH і функція CreateBrushIndirect .....	678
23.6.	Зміна характеристик графічних інструментів .....	680
23.7.	Створення логічних шрифтів.....	690
23.8.	Виведення тексту .....	691
23.9.	Лабораторна робота “Графічні примітиви”.....	707
23.10.	Контрольні запитання .....	707
<b>24.</b>	<b>ОБРОБКА ПОВІДОМЛЕНЬ ВІД КЛАВІАТУРИ.....</b>	<b>708</b>
24.1.	Типи повідомлень від клавіатури та їх обробка.....	708
24.2.	Віртуальні коди клавіш .....	711
24.3.	Лабораторна робота “Обробка повідомлень від клавіатури” .....	717
24.4.	Контрольні запитання .....	718
<b>25.</b>	<b>ОБРОБКА ПОВІДОМЛЕНЬ ВІД МИШКИ.....</b>	<b>719</b>
25.1.	Керування мишкою.....	719
25.2.	Системний набір курсорів.....	724
25.3.	Захоплення миші.....	729
25.4.	Лабораторна робота “Обробка повідомлень від мишки”.....	730
25.5.	Контрольні запитання .....	731
<b>26.</b>	<b>ДІАЛОГОВЕ ВІКНО .....</b>	<b>731</b>
26.1.	Модальне діалогове вікно .....	736
26.2.	Немодальне діалогове вікно.....	738
26.3.	Стиль вікна (префікс WS_).....	739
26.4.	Опції створення вікна (префікс CW_) .....	741
26.5.	Органи керування діалогового вікна.....	742
26.6.	Типи діалогових вікон.....	743
26.6.1.	Діалогове вікно як основне.....	743
26.6.2.	Діалогове вікно як допоміжне .....	744
26.7.	Створення ресурсів для діалогового вікна в Visual Studio 2008.....	744
26.8.	Дослідження коду програм за допомогою OllyDbg.....	744
26.9.	Лабораторна робота “Дослідження коду програм” .....	752
26.10.	Контрольні запитання .....	752
<b>27.</b>	<b>ДОЧІРНЄ ВІКНО.....</b>	<b>754</b>

27.1. Основи створення дочірнього вікна .....	754
27.2. Лабораторна робота “Дочірнє вікно” .....	759
27.3. Контрольні запитання .....	760
<b>28. КЕРУВАННЯ ПАМ’ЯТТЮ.....</b>	<b>761</b>
28.1. API-функції керування пам’яттю.....	762
28.2. Приклад використання блока пам’яті.....	765
28.3. Іконка в панелі завдань system tray .....	771
28.4. Лабораторна робота “ Керування пам’яттю”.....	772
28.5. Контрольні запитання .....	773
<b>29. РЕЄСТР .....</b>	<b>774</b>
29.1. Структура реєстру .....	775
29.2. Створення та відкриття ключів .....	783
29.3. Лабораторна робота “Реєстр”.....	791
29.4. Контрольні запитання .....	792
<b>30. ДРАЙВЕРИ .....</b>	<b>793</b>
30.1. Основні поняття про драйвери.....	793
30.2. Одно- та багаторівневі драйвери.....	794
30.3. Керування драйвером.....	794
30.4. Програмування звукового каналу .....	799
30.5. Лабораторна робота “Драйвер звукового каналу” .....	803
30.6. Контрольні запитання .....	803
<b>31. ОСНОВИ ПЕРЕХОПЛЕННЯ API-ФУНКЦІЙ У WINDOWS .....</b>	<b>804</b>
31.1. Загальні повідомлення про перехвати .....	804
31.2. Встановлення перехватів .....	804
31.3. Контрольні запитання .....	812
<b>ДОДАТКИ .....</b>	<b>813</b>
<b>Додаток 1.</b> Система базових команд МП платформи x86.....	813
<b>Додаток 2.</b> Таблиці кодування символів.....	823
<b>Додаток 3.</b> API-функції, які часто використовуються.....	826
<b>Додаток 4.</b> Арифметичні задачі для практичного використання .....	830
<b>Додаток 5.</b> Методичні вказівки до виконання курсового проекту за курсом “Системне програмування”.....	832
<b>СПИСОК ЛІТЕРАТУРИ .....</b>	<b>847</b>