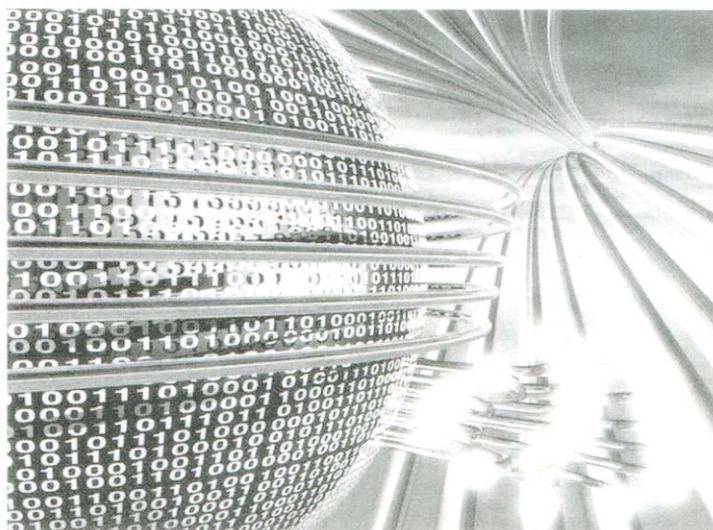


О.М. Рисований

# СИСТЕМНЕ ПРОГРАМУВАННЯ



Підручник  
Том 1

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ  
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

**О. М. Рисований**

# **СИСТЕМНЕ ПРОГРАМУВАННЯ**

**Том 1**

Підручник

для студентів напрямку “Компютерна інженерія”  
вищих навчальних закладів

Видання четверте: виправлено та доповнено

Затверджено Міністерством освіти і науки України

Харків 2015

ББК 32.973-018.14  
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 [Текст]: підручник для студентів напрямку “Комп’ютерна інженерія” вищих навчальних закладів в 2-х томах. Том 1. - Видання четверте: виправлено та доповнено – Х.: “Слово”, 2015. – 576 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 - SSE4, AVX. Крім того, розглянуто питання віконного програмування та організації управління 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. Всі програми протестовані за допомогою налагоджувача OllyDbg.

Призначено для студентів спеціальностей 6.050102-01 «Комп’ютерні системи та мережі», 6.050102-02 «Системне програмування» і 6.050102-03 «Спеціалізовані комп’ютерні системи». Також може бути корисним для спеціалістів.

**ББК 32.973-018.1**

© О.М. Рисований, 2015

## ЗМІСТ

<b>ВСТУП</b> .....	<b>9</b>
<b>1. ЕТАПИ СТВОРЕННЯ ПРОГРАМИ МОВОЮ АСЕМБЛЕРА</b> .....	<b>13</b>
1.1. Підготовка вихідного тексту програми в Masm32.....	14
1.2. Отримання об'єктного коду в Masm32.....	16
1.3. Отримання виконуваного файлу програми в Masm32.....	48
1.4. Зменшення розміру програми за рахунок ключів компіляції та лінування в Masm32.....	18
1.5. Налаштування програми.....	20
1.6. Редактори тексту.....	20
1.7. Налаштування середовища Visual Studio 2013.....	21
1.8. Угорська нотація.....	28
<b>2. АРХІТЕКТУРА МІКРОПРОЦЕСОРА INTEL</b> .....	<b>27</b>
2.1. Архітектурні особливості 32-розрядного МП Intel .....	27
2.1.1. Типи даних МП Intel.....	27
2.1.2. Регістри 32-розрядного МП Intel.....	29
2.1.3. Моделі пам'яті МП Intel.....	35
2.1.4. Способи адресації 32-розрядного МП Intel.....	38
2.2. Архітектурні особливості 64-розрядного МП Intel .....	49
2.2.1. Угода про виклики параметрів функцій.....	49
2.2.2. Регістри архітектури x64 .....	49
2.2.3. Використання регістрів архітектури x64.....	51
2.2.4. Скалярні типи даних архітектури x64 .....	53
2.2.5. Використання стека архітектури x64.....	53
<b>3. ОСНОВНІ ДИРЕКТИВИ ТА ОПЕРАНДИ АСЕМБЛЕРА</b> .....	<b>56</b>
3.1. Директиви асемблера .....	56
3.1.1. Директиви MODEL, DATA, CONST, STACK, CODE .....	56
3.1.2. Директиви SEGMENT та ENDS.....	58
3.1.3. Директиви PROC та ENDP.....	60
3.1.4. Директива ASSUME .....	60
3.1.5. Директива ORG .....	61
3.1.6. Директиви визначення даних DB, DW, DD, DF, DP, DQ, DT .....	61
3.1.7. Директиви символічних констант: =, EQU, TEXTEQU .....	63
3.1.8. Директива END .....	64
3.1.9. Директива LABEL.....	64
3.1.10. Директива ALIGN.....	64
3.1.11. Директива LOCALS .....	65
3.1.12. Директиви керування файлами INCLUDE, INCLUDELIB.....	65
3.2. Оператори мови асемблера.....	65
3.3. Лабораторна робота «Подання даних».....	69
<b>4. ОПЕРАЦІЇ ПЕРЕСИЛАННЯ ДАНИХ</b> .....	<b>80</b>
4.1. Команди пересилання даних загального призначення.....	80
4.2. Команди роботи зі стеком.....	83

4.3. Команди роботи з адресами і вказівником.....	88
4.4. Команди перетворення даних.....	89
4.5. Команди введення та виведення в порт.....	90
4.6. Команди пересилання бітів умов .....	90
<b>5. ОСНОВНІ АРИФМЕТИЧНІ ОПЕРАЦІЇ.....</b>	<b>92</b>
5.1. Арифметичні операції.....	92
5.2. Лабораторна робота «Програмування арифметичних операцій» .....	112
5.3. Додатковий матеріал про налагоджувач OLLYDBG.....	118
<b>6. ЛОГІЧНІ КОМАНДИ ТА КОМАНДИ ЗСУВУ.....</b>	<b>123</b>
6.1. Команди булевих операцій.....	123
6.2. Команди перевірки і модифікації бітів.....	124
6.3. Команди сканування бітів.....	126
6.4. Команди зсуву (зрушення) і циклічного зсуву .....	127
6.4.1. Команди зсуву .....	127
6.4.2. Команди циклічного зсуву.....	129
6.4.3. Команди подвійного зсуву.....	129
6.5. Команди установки байта за умовою.....	130
6.6. Команда перевірки .....	131
<b>7. КОМАНДИ ПЕРЕДАННЯ КЕРУВАННЯ.....</b>	<b>133</b>
7.1. Команда безумовного переходу JMP.....	133
7.2. Команди умовної передавання керування Jcc .....	134
7.3. Команди керування циклами LOOPx.....	143
<b>8. ПРОЦЕДУРИ.....</b>	<b>147</b>
8.1. Виклик (команда CALL) процедури та її повернення (команда RET).....	147
8.2. Угоди про виклик функцій.....	148
8.3. Команди керування стеком при виконанні процедур.....	149
8.4. Директива LOCAL.....	151
8.5. Директива INVOKE.....	151
8.6. Оператор ADDR .....	152
8.7. Директива PROTO.....	152
8.8. Оператор USES.....	153
8.9. Організація процедур та їх дослідження .....	153
8.10. Windows API-подібні процедури .....	158
8.11. Непрямий виклик процедур.....	160
8.12. Використання загальних змінних у процедурах.....	163
8.13. Лабораторна робота «Передача параметрів через таблицю адрес».....	174
8.14. Лабораторна робота «API-подібні процедури».....	178
8.15. Лабораторна робота «Зовнішні процедури» .....	180
<b>9. ОРГАНІЗАЦІЯ ВВЕДЕННЯ - ВИВЕДЕННЯ В WIN32 .....</b>	<b>184</b>
9.1. Загальні відомості .....	184
9.2. Набір символів і API-функції Windows .....	186
9.3. Типи даних Windows.....	186

9.4. Дескриптори консолі .....	187
9.5. API-функції консолі в Win32 .....	188
9.6. Виведення повідомлень .....	190
9.7. Виведення чисел.....	197
9.8. Введення з консолі.....	207
9.9. Керування кольором .....	209
9.10. Лабораторна робота «Введення-виведення даних».....	212
<b>10. ДИНАМІЧНІ БІБЛІОТЕКИ .....</b>	<b>224</b>
10.1. Створення динамічних бібліотек та їх використання .....	225
10.2. Функція точки входу в DLL .....	228
10.3. Лабораторна робота “DLL-файли”.....	232
<b>11. ФАЙЛИ .....</b>	<b>236</b>
11.1. Створення файлу.....	238
11.2. Читання файлу.....	241
11.3. Переміщення файлового вказівника.....	244
11.4. Файлові операції засобами ShellAPI.....	249
11.5. Лабораторна робота «Файли» .....	253
<b>12. АРИФМЕТИЧНИЙ СПІВПРОЦЕСОР .....</b>	<b>258</b>
12.1. Типи даних співпроцесора .....	258
12.2. Архітектура співпроцесора .....	260
12.3. Система команд математичного співпроцесора .....	262
12.3.1. Команди передавання даних.....	264
12.3.2. Команди порівняння .....	268
12.3.3. Арифметичні команди .....	275
12.3.4. Трансцендентні команди .....	292
12.3.5. Команди маніпуляції константами .....	299
12.3.6. Команди керування .....	299
12.4. Лабораторна робота «Обробка даних у співпроцесорі» .....	300
<b>13. РЯДКИ .....</b>	<b>316</b>
13.1. Обробка рядків .....	316
13.2. Лабораторна робота «Рядки» .....	334
<b>14. МАКРОВИЗНАЧЕННЯ.....</b>	<b>342</b>
14.1. Введення в макровизначення .....	342
14.1.1. Порівняльний аналіз процедур і макрозасобів .....	342
14.1.2. Місця використання макровизначень.....	343
14.2. Директиви MACRO і ENDM.....	344
14.3. Директива LOCAL.....	348
14.4. Булеві вирази.....	348
14.5. Оператори в макровизначеннях.....	352
14.5.1. Оператор заміни (&).....	352
14.5.2. Оператор виразу (%).....	354
14.5.3. Оператор виділення тексту (⇨) .....	354
14.5.4. Оператор виділення символу (!).....	355
14.5.5. Оператор макрокоментаря (;).....	355

14.6. Додаткові макровизначення і директиви.....	355
14.6.1. Директива REPT.....	355
14.6.2. Директива IRP.....	356
14.6.3. Директива IRPC.....	<b>357</b>
14.7. Макроси циклів: FOR, FORC, REPEAT, WHILE.....	358
14.8. Категорії макросів в <code>masm32</code> .....	360
14.9. Макрос <code>@</code> для запису команд в один рядок.....	364
14.10. Лабораторна робота “Макроси”.....	366
<b>15. ЛОГІЧНІ КОНСТРУКЦІ ВИСОКОГО РІВНЯ.....</b>	<b>371</b>
15.1. Директива IF.....	371
15.2. Логічна директива <code>switch</code> .....	380
15.3. Логічна директива <code>switch\$</code> .....	380
15.4. Логічні директиви <code>.REPEAT</code> та <code>.WHILE</code> .....	381
15.5. Директива <code>.BREAK</code> .....	388
15.6. Директива <code>.CONTINUE</code> .....	388
15.7. Лабораторна робота “Директиви умовного асемблювання”.....	389
15.8. Лабораторна робота “Двовимірні масиви”.....	396
<b>16. СТРУКТУРИ.....</b>	<b>403</b>
16.1. Організація структур.....	403
16.2. Структура <code>SYSTEMTIME</code> для визначення системного часу.....	406
16.3. Структура <code>MSGBOXPARAMS</code> в функції <code>MessageBoxIndirect</code> .....	408
16.4. Складні структури.....	412
16.5. Створення зображення іконки.....	412
16.6. Лабораторна робота “Структури”.....	413
<b>17. АНТИНАЛАГОДЖУВАЛЬНІ ПРИЙОМИ.....</b>	<b>419</b>
17.1. Трасування в <code>x86</code> -процесорах.....	419
17.2. Переривання в масці.....	420
17.3. Трасування за часом виконання інструкцій.....	421
17.4. Обробка виключень.....	422
<b>18. MMX-РОЗШИРЕННЯ.....</b>	<b>426</b>
18.1. MMX-команди передачі даних.....	429
18.2. Арифметичні MMX-команди.....	429
18.2.1. Команди додавання.....	429
18.2.2. Команди віднімання.....	434
18.2.3. Команди множення.....	438
18.3. MMX-команди пакування та розпакування даних.....	441
18.4. MMX-команди порівняння.....	449
18.5. Логічні MMX-команди.....	453
18.6. Команди зсуву.....	454
18.7. MMX-команди в Pentium III.....	456
18.8. MMX-команди в Pentium IV.....	461
18.9. Лабораторна робота “MMX-команди”.....	462
<b>19. SSE-РОЗШИРЕННЯ.....</b>	<b>470</b>
19.1. Команди пересилання даних.....	474

19.2. Арифметичні команди .....	478
19.2.1. Команди додавання.....	478
19.2.2. Команди віднімання.....	480
19.2.3. Команди паралельного та скалярного множення .....	481
19.2.4. Команди паралельного та скалярного ділення .....	482
19.2.5. Додаткові арифметичні команди .....	484
19.3. Команди порівняння .....	490
19.4. Команди перетворення .....	496
19.5. Логічні команди .....	499
19.6. Команди управління станом.....	500
19.7. Команди розпаковування даних.....	501
19.8. Команди управління кешуванням.....	504
19.9. Асемблювання та компонування програми через безпосереднє звертання до Visual Studio 2008.....	505
19.10. Лабораторна робота “SSE-команди” .....	507
<b>20. SSE2-РОЗШИРЕННЯ.....</b>	<b>512</b>
20.1. Команди передавання даних .....	514
20.1.1. Обмін 128-bit кодами між оперативною пам’яттю (ОЗП) та регістрами xmm .....	514
20.1.2. Обмін 64-розрядними кодами між ОЗП і регістрами xmm.....	515
20.1.3. Використання масок .....	516
20.2. Арифметичні операції.....	519
20.2.1. Паралельні операції з упакованими числами.....	519
20.2.2. Арифметичні операції зі скалярними числами.....	522
20.3. Команди порівняння .....	525
20.3.1. Порівняння без зміни стану розрядів EFLAGS .....	525
20.3.2. Команди порівняння, які змінюють регістр EFLAGS .....	526
20.4. Логічні операції.....	527
20.5. Команди розпаковування і розподілення даних .....	528
20.6. Команди перетворення форматів даних.....	529
20.6.1. Групові перетворення форматів даних.....	529
20.6.2. Перетворення формату одного числа.....	533
20.7. Управління кешем.....	534
20.8. Операції з цілими числами. Нові можливості інструкцій MMX .....	534
20.9. Асемблювання через безпосередній запис до каталогу Visual Studio 2008 та компонування через masm32.....	535
20.10. Асемблювання та компонування через безпосереднє звертання до Visual Studio 2010 .....	536
20.11. Лабораторна робота “SSE2-команди” .....	538
<b>21. SSE3-РОЗШИРЕННЯ.....</b>	<b>546</b>
21.1. Перетворення чисел з плаваючою точкою (x87) в цілі числа.....	546
21.2. Дублювання даних .....	546
21.3. Завантаження невіривняних змінних.....	547



21.4. Одночасне додавання/віднімання .....	548
21.5. Горизонтальне додавання/віднімання.....	548
21.6. Синхронізація потоків.....	550
21.7. Використання SSE3 в розробці і оптимізації програм .....	550
21.7.1. Розрахункові завдання, що використовують x87 FPU .....	550
21.7.2. Обчислення з комплексними числами.....	552
21.7.3. Кодування відео.....	552
21.7.4. Векторні операції.....	553
21.8. SSSE3-доповнення .....	554
21.9. Лабораторна робота “SSE3-команди” .....	556
<b>22. SSE4-РОЗШИРЕННЯ.....</b>	<b>558</b>
22.1. SSE4.1-розширення.....	558
22.1.1. Прискорення відео.....	558
22.1.2. Векторні примітиви.....	559
22.1.3. Вставки/витягання.....	559
22.1.4. Скалярне множення векторів.....	560
22.1.5. Змішування.....	560
22.1.6. Перевірка бітів.....	560
22.1.7. Округлення.....	560
22.1.8. Читання WC пам’яті.....	561
22.2. SSE4.2-розширення.....	561
22.2.1. Обробка рядків.....	561
22.2.2. Підрахунок контрольної суми CRC32 .....	562
22.2.3. Підрахунок популяції одиничних бітів.....	562
22.2.4. Векторні примітиви.....	562
22.3. Формати даних SSE 1-4 команд.....	562
<b>23. AVX-РОЗШИРЕННЯ.....</b>	<b>564</b>
23.1. Особливості використання команд AVX-розширення .....	564
23.2. Схема кодування .....	565
23.3. Набір команд AVX.....	565
23.4. Використання AVX-інструкцій.....	566
23.5. Лабораторна робота “AVX-команди” .....	572
<b>СПИСОК ЛІТЕРАТУРИ .....</b>	<b>575</b>