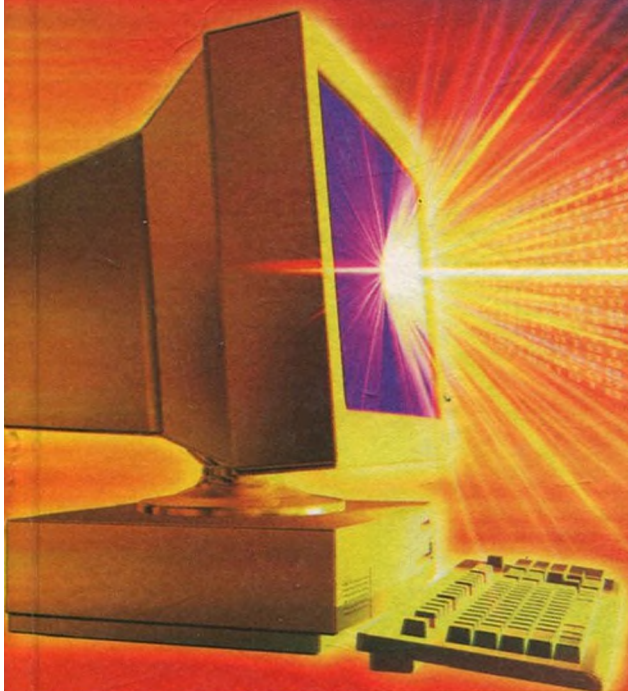


004. 7
М 54

МЕТОДИ ТА МОДЕЛІ РОЗРОБЛЕННЯ **КОМП'ЮТЕРНИХ СИСТЕМ І МЕРЕЖ**

Монографія



Пономаренко В. С.

Мінухін С. В.

Кавун С. В.

Лосєв М. Ю.

Павленко Л. А.

Федорченко В. М.

Парфьонов Ю. Е.

Задачин В. М.

Євсєєв С. И.

МЕТОДИ ТА МОДЕЛІ РОЗРОБЛЕННЯ КОМП'ЮТЕРНИХ СИСТЕМ І МЕРЕЖ

Монографія

Харків. Вид. ХНЕУ, 2008

УДК 004.7
ББК 32 973
П56

Рецензенти: докт техн наук, професор, зав кафедри системного аналізу і управління Національного технічного університету "ХПІ" *Куценко О. С.*; докт. техн. наук, професор, зав. кафедри інформаційних управляючих систем Харківського національного університету радіоелектроніки *Левикін В. М.*; докт техн. наук, професор, начальник учебного центра CAO/CAM/CAE Національного аерокосмічного університету ім. М. Є. Жуковського "ХАІ" *Гребенніков О. Г.*

**Рекомендовано до видання рішенням вченої ради
Харківського національного економічного університету.**
Протокол №9 від 21.04.2008 р.

Пономаренко В. С.
П56 Методи та моделі розроблення комп'ютерних систем і мереж
Монографія / В. С. Пономаренко, С. В. Мінухін, С. В. Кавун, М. Ю. Лосєв, Л. А. Павленко, В. М. Федорченко, Ю. Е. Парфьонов, В. М. Задачин, С. П. Євсєєв; Заг. редакція докт. екон. наук, професора Пономаренка В. С. – Харків: Вид, ХНЕУ, 2008. – 316 с. (Укр. мов)

Розкрито питання, пов'язані з розглядом сучасних проблем з аналізу систем, зокрема, уточнення положень та понять з позицій системного підходу, проаналізовано стан і перспективи впровадження розподілених інформаційних систем на прикладі GRID та геоінформаційних систем. Розглянуто питання безпеки в корпоративних системах за допомогою визначення напрямків захисту інформації у процесах документообігу й побудови ефективних алгоритмів кодування.

Рекомендовано для фахівців у сфері проектування та експлуатації інформаційних систем і програмного забезпечення, системних аналітиків, фахівців установ у сфері захисту навколишнього середовища

ISBN ISBN 978-966-676-309-2

**УДК 004.7
ББК 32.973**

© Пономаренко В. С , Мінухін С. В.,
Кавун С. В., Лосєв М. Ю.,
Павленко Л. А. , Федорченко В. М.,
Парфьонов Ю. Е., Задачин В. М.,
Євсєєв С. П.
2009

Зміст

Вступ	3
Розділ 1. Моделі та методи розподілу ресурсів у GRID-мережах	4
1.1. Рівні архітектури і стандарти GRID-мереж	4
1.2. Моделі управління завданнями у GRID-мережах	15
1.3. Ранговий підхід до вирішення завдань булевого програмування для планування ресурсів у GRID-мережах	19
1.4. Класифікація методів розв'язання задач дискретної оптимізації для планування ресурсів у GRID-мережах	24
1.5. Аналіз ефективності послідовних і паралельних алгоритмів для реалізації завдань у GRID-мережах	29
Розділ 2. Моделювання процесів комп'ютерних систем (КС)	31
2.1. Підходи до моделювання КС як складної системи у складі ІС	31
2.1.1. Поняття системи. Властивості складних систем	31
2.1.2. Поняття моделі й моделювання. Фактори, що спричиняють необхідність моделювання Переваги та недоліки моделей	36
2.1.3. Класифікація моделей	39
2.1.4. Методи дослідження моделей	42
2.1.5. Етапи моделювання	43
2.2. Імітаційне моделювання складних систем	47
2.2.1. Основні принципи імітаційного моделювання	47
2.2.2. Принципи й методи побудови ІМ	48
2.2.3. Основні методи імітаційного моделювання	51
2.2.4. Випадкові події та їхня імітація	52
2.2.5. Імітація безперервних випадкових величин	54
2.2.6. Алгоритми одержання значень систем випадкових величин (випадкових векторів)	58
2.2.7. Імітація випадкових процесів	61
2.3. Моделювання локальних корпоративних мереж (ЛКМ) програмними засобами імітаційного моделювання	66
2.3.1. Основні можливості й характеристики пакета моделювання NetCracker Pro 3.1	66
2.3.2. Принципи використання пакета моделювання NetCracker Pro 3.1 для моделювання локальних корпоративних мереж (ЛКМ)	67

2.3.3 Методика побудови моделі ЛКМ у пакеті моделювання NetCracker Pro 3.1	73
2.3.4. Методика побудови багаторівневих проектів ЛКМ у пакеті моделювання NetCracker Pro 3.1	79
2.3.5. Одержання статистики моделювання й аналіз результатів дослідження	85
2 4. Результати моделювання і їхній аналіз	88
2.4.1. Основні можливості й характеристики пакета моделювання NetSim Boson	93
2.4.2. Організація моделювання КМ в пакетах моделювання NetSim Boson и NetCracker Pro 3.1	97
2 4 3 Методика побудови моделі КМ у середовищі NetSim Boson	103
Розділ 3. Аналіз міжнародних стандартів із питань захисту інформації в комп'ютерних системах	103
3.1. Стандарт ISO	104
3.2. Стандарти ЕСМА	109
3 3. Система стандартів Міністерства оборони США в галузі комп'ютерної безпеки	114
3.4. Методи й механізми захисту мереж	118
3.5. Особливості захисту різних класів мереж	121
3.6. Організаційні заходи забезпечення захисту інформації	126
3.7. Симетрична модель захисту мережі	132
Розділ 4. Підвищення ефективності обміну даними на основі моделювання ймовірно-часових характеристик цифрових мереж	148
4.1. Управління потоком повідомлень у цифрових мережах	149
4.2. Аналіз методів підвищення ефективності обміну інформацією в цифрових мережах	153
4.2.1. Аналіз ефективності обміну інформацією в цифрових мережах	153
4.2.2. Аналіз методів підвищення достовірності передачі інформації в мережах обміну даними	155
4.3. Розробка математичної моделі обміну даними з локалізацією помилок в інформації яка передається	161

Розділ 5. Геоінформаційні технології в розробці систем еколого-економічного моніторингу	171
5.1. Стан та актуальність еколого-економічного моніторингу	171
5.2. Зв'язок між екологічним та економічним моніторингом і необхідністю використання методів та моделей геоінформаційних технологій	177
5.3. Застосування геоінформаційних систем	186
5.4. Головні можливості пакета ArcView GIS	194
5.5. Актуальність використання геоінформаційних технологій у розробці систем еколого-економічного моніторингу Харківської області	205
Розділ 6. Підвищення безпеки інформаційної системи на основі реалізації інфраструктури відкритого ключа з використанням криптопримітивів на ідентифікаторах	207
6.1. Аналіз систем електронних документів. Загальні відомості про інфраструктуру відкритого ключа	208
6.1.1. Основи IBK	208
6.1.2. Характеристика сертифікатів X.509v3	208
6.1.3. Центр сертифікації	209
6.1.4. Центр реєстрації	211
6.1.5. Сервери каталогів LDAP	211
6.1.6. Зберігання ключів і відкликання сертифікатів	212
6.1.7. Створення ієрархії сертифікаційних центрів	214
6.2. Актуальність і проблеми використання інфраструктури відкритого ключа	214
6.3. Огляд розвитку інфраструктури відкритого ключа	217
6.4. Інтеграція в операційних системах	219
6.5. Рівень значимості інфраструктури відкритого ключа, заснованої на ідентифікаторах	220
Розділ 7. Моделювання процесу контролю і управління обміном інформацією в цифрових мережах	226
7.1. Алгоритм інформаційного обміну даними з адресним перезапитом	227
7.2. Методика аналізу ймовірісно-часових характеристик процесу передачі інформації в цифрових мережах	229
7.3. Розробка математичної моделі інформаційного обміну на основі протоколу передачі даних з адресним перезапитом	232

Розділ 8. Моделі й методи розробки інформаційних систем для вирішення завдань управління інженерними міськими мережами	239
8.1. Огляд наявних систем для інженерних мереж. Базові класи	241
8.2. Побудова інтеграційних систем муніципальних ГІС	243
8.3. Моделювання фізичних процесів в інженерних мережах і спеціалізований ГІС	247
8.4. Питання вибору програмних засобів	250
Розділ 9. Криптосистеми на основі теоретико-кодкових схем з еліптичними кодами в системах захисту ІС	251
9.1. Методи побудови несиметричних теоретико-кодкових схем	252
9.2. Несиметричні криптосистеми на теоретико-кодкових схемах з використанням еліптичних кодів	256
9.3. Алгоритми формування кодограми в теоретико-кодкових схемах на еліптичних кодах	283
9.4. Алгоритми декодування кодограми в теоретико-кодкових схемах на еліптичних кодах	270
9.5. Засоби модифікації теоретико-кодкових схем на алгебраїчних блокових кодах	277
9.6. Засоби маскувння еліптичних кодів у модифікованих теоретико-кодкових схемах а використанням параметрів кривої у якості секретних даних	282
9.7. Способи маскувння еліптичних кодів у модифікованих теоретико-кодкових схемах з використанням символів модифікації коду в якості секретних даних	287
9.8. Алгоритми кодування й декодування інформації з використанням модифікованих теоретико-кодкових схем на еліптичних кодах	294
9.9. Дослідження властивостей модифікованих теоретико-кодкових схем з еліптичними кодами	297
Висновки	301
Використана література	303