

621.384  
А 45

**М.І. НАУМЕНКО, Ю.В. СТАСЄВ, О.О. КУЗНЕЦОВ,  
С.П. ЄВСЄЄВ**

# **АЛГЕБРАЇЧНІ МЕТОДИ ПОБУДОВИ СИГНАЛЬНО-КОДОВИХ КОНСТРУКЦІЙ**

**Монографія**



621.391  
A 45

Міністерство оборони України  
ХАРКІВСЬКИЙ УНІВЕРСИТЕТ ПОВІТРЯНИХ СИЛ  
імені ІВАНА КОЖЕДУБА

М.І. Науменко, Ю.В. Стасєв, О.О. Кузнецов, С.П. Євсєєв

# АЛГЕБРАЇЧНІ МЕТОДИ ПОБУДОВИ СИГНАЛЬНО-КОДОВИХ КОНСТРУКЦІЙ

*Монографія*



Харків  
2007

УДК 621.391

ББК 32.96: 68.51 Я73

**A77**

Рецензенти: *В.А. Краснобаев*, доктор технічних наук, професор  
*С.В. Смеляков*, доктор фізико-математичних наук, професор

**ISBN 978-966-468-000-1**

**A77** Алгебраїчні методи побудови сигнально-кодових конструкцій: Монографія.  
М.І. Науменко, Ю.В. Стасєв, О.О. Кузнецов, С.П. Євсєєв. – Х.: ХУПС, 2007. – 363 с.

Досліджується проблема забезпечення ефективності функціонування систем і засобів зв'язку в умовах ведення радіоелектронної боротьби та при складних перешкодових обставинах. Розглядаються методи підвищення завадостійкості, імітостійкості й скритності радіоканалів управління.

Викладається алгебраїчна теорія блокових кодів, досліджуються найважливіші класи кодів, методи їх побудови й декодування. Досліджуються методи синтезу складних систем сигналів з поліпшеними кореляційними, ансамблевими і структурними властивостями. Викладаються теоретичні основи та методи побудови сигнально-кодових конструкцій для підвищення завадостійкості, імітостійкості й скритності цифрових систем зв'язку.

Для викладачів, наукових та інженерно-технічних співробітників в галузі радіотехніки, систем зв'язку, обчислювальної техніки й автоматизованих систем управління, а також для ад'юнктів, аспірантів і студентів старших курсів відповідних спеціальностей.

УДК 621.391

ББК 32.96: 68.51 Я73

Затверджена до друку Вченою Радою Харківського університету  
Повітряних Сил ім. Івана Кожедуба (протокол № 63 від 7 грудня 2007 року)

© М.І. Науменко, Ю.В. Стасєв, О.О. Кузнецов, С.П. Євсєєв, 2007

© Харківський університет Повітряних Сил ім. Івана Кожедуба, 2007

**ISBN 978-966-468-0**

## ЗМІСТ

|                                                                                                                                                                                                  |     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| ВСТУП.....                                                                                                                                                                                       | 6   |
| Розділ 1. ПРОБЛЕМА ЗАБЕЗПЕЧЕННЯ ЗАВАДОСТІЙКОСТІ, ІМІТОСТІЙКОСТІ<br>ТА СКРИТНОСТІ ЗВ'ЯЗКУ .....                                                                                                   | 9   |
| 1.1. Проблема забезпечення ефективності функціонування систем<br>і засобів зв'язку в умовах застосування зловмисником<br>радіоелектронної розвідки та ведення радіоелектронної<br>боротьби ..... | 9   |
| 1.2. Необхідні й достатні умови реалізації динамічного<br>режиму функціонування цифрової системи зв'язку .....                                                                                   | 14  |
| 1.3. Математична модель і структурна схема цифрової<br>системи зв'язку .....                                                                                                                     | 18  |
| 1.4. Критерії та показники оцінки завадостійкості, імітостійкості<br>й скритності систем і засобів зв'язку .....                                                                                 | 20  |
| 1.4.1. Критерії й показники оцінки завадостійкості .....                                                                                                                                         | 20  |
| 1.4.2. Критерії й показники оцінки імітостійкості .....                                                                                                                                          | 22  |
| 1.4.3. Критерії й показники оцінки скритності .....                                                                                                                                              | 26  |
| Розділ 2. ЗАГАЛЬНІ ПОЛОЖЕННЯ ТЕОРІЇ ПОЛІВ ГАЛУА .....                                                                                                                                            | 31  |
| 2.1. Вступ до алгебри. Основні терміни і визначення .....                                                                                                                                        | 31  |
| 2.2. Структура скінченних полів та їх властивості .....                                                                                                                                          | 40  |
| 2.3. Спектральні перетворення в скінченних полях .....                                                                                                                                           | 52  |
| Розділ 3. ОСНОВИ АЛГЕБРАЇЧНОЇ ТЕОРІЇ БЛОКОВІХ КОДІВ .....                                                                                                                                        | 57  |
| 3.1. Основна проблема теорії завадостійкого кодування .....                                                                                                                                      | 57  |
| 3.2. Методи побудови циклічних кодів та їх підкласи .....                                                                                                                                        | 61  |
| 3.3. Методи побудови альтернантних кодів та їх підкласи.....                                                                                                                                     | 70  |
| 3.4. Методи побудови лінійних блокових кодів<br>із застосуванням математичного апарата теорії алгебраїчних кривих .....                                                                          | 78  |
| 3.5. Методи та алгоритми кодування<br>алгеброгеометричними кодами.....                                                                                                                           | 88  |
| 3.6. Методи та алгоритми декодування алгеброгеометричних<br>кодів .....                                                                                                                          | 93  |
| 3.6.1. Аналіз відомих методів декодування недвійкових<br>блокових кодів.....                                                                                                                     | 93  |
| 3.6.2. Декодування алгебраїчних кодів методом Берлекемпа .....                                                                                                                                   | 97  |
| 3.6.3. Алгебраїчне декодування алгеброгеометричних кодів .....                                                                                                                                   | 107 |
| 3.6.4. Переставне декодування алгеброгеометричних кодів .....                                                                                                                                    | 121 |
| 3.6.5. Мажоритарне декодування алгеброгеометричних кодів ...                                                                                                                                     | 124 |
| Розділ 4. АЛГЕБРАЇЧНІ МЕТОДИ ПОБУДОВИ СКЛАДНИХ СИСТЕМ<br>СИГНАЛІВ .....                                                                                                                          | 132 |
| 4.1. Методи синтезу ансамблів дискретних сигналів .....                                                                                                                                          | 132 |
| 4.2. Побудова ансамблів ортогональних дискретних сигналів.                                                                                                                                       |     |



|                                                                                                                                                                                                        |     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Методи комплексного поліпшення їх характеристик .....                                                                                                                                                  | 141 |
| 4.3. Складові дискретні системи сигналів .....                                                                                                                                                         | 154 |
| 4.4. Нелінійні сигнали з псевдовипадковою перестройкою<br>робочої частоти .....                                                                                                                        | 166 |
| 4.5. Аналіз завадостійкості, імітостійкості й скритності радіосистем<br>при використанні складових систем сигналів .....                                                                               | 174 |
| Розділ 5. СИНТЕЗ АНСАМБЛІВ СИГНАЛІВ З ВИКОРИСТАННЯМ МЕТОДІВ<br>ЗАВАДОСТІЙКОГО КОДУВАННЯ .....                                                                                                          | 193 |
| 5.1. Метод формування псевдовипадкових послідовностей<br>з поліпшеними автокореляційними властивостями .....                                                                                           | 193 |
| 5.2. Алгоритми формування псевдовипадкових послідовностей<br>з поліпшеними автокореляційними властивостями .....                                                                                       | 200 |
| 5.3. Дослідження кореляційних, ансамблевих і структурних<br>властивостей сформованих псевдовипадкових послідовностей .....                                                                             | 207 |
| 5.4. Основні властивості переставних перетворень .....                                                                                                                                                 | 211 |
| 5.5. Метод формування псевдовипадкових послідовностей<br>з поліпшеними взаємокореляційними властивостями .....                                                                                         | 216 |
| 5.6. Алгоритм формування псевдовипадкових<br>послідовностей з поліпшеними взаємокореляційними властивостями ..                                                                                         | 219 |
| 5.7. Пропозиції щодо апаратної реалізації алгоритму<br>формування псевдовипадкових послідовностей з поліпшеними<br>взаємокореляційними властивостями .....                                             | 221 |
| 5.8. Методика оцінки статистичних характеристик<br>псевдовипадкових послідовностей .....                                                                                                               | 242 |
| 5.9. Дослідження статистичних характеристик<br>псевдовипадкових послідовностей .....                                                                                                                   | 245 |
| Розділ 6. МЕТОДИ ПОБУДОВИ СИГНАЛЬНО-КОДОВИХ КОНСТРУКЦІЙ<br>ТА ДОСЛІДЖЕННЯ ЇХ ВЛАСТИВОСТЕЙ .....                                                                                                        | 270 |
| 6.1. Алгебраїчні методи побудови сигнально-кодових<br>конструкцій з поліпшеними кореляційними, ансамблевими та<br>структурними властивостями .....                                                     | 299 |
| 6.2. Дослідження завадостійкості, імітостійкості й скритності<br>цифрових систем зв'язку з використанням запропонованих<br>сигнально-кодових конструкцій.....                                          | 292 |
| ВИСНОВКИ.....                                                                                                                                                                                          | 313 |
| Додаток А. Конструктивні характеристики деяких двійкових кодів<br>БЧХ примітивної й непримітивної довжини .....                                                                                        | 314 |
| Додаток Б. Конструктивні характеристики деяких недвійкових<br>кодів БЧХ примітивної довжини .....                                                                                                      | 325 |
| Додаток В. Конструктивні характеристики алгеброгеометричних<br>кодів, побудованих за проєктивними кривими (коди Ріда-Соломона),<br>еліптичними кривими, кривими Гурвіца, Ерміта, Ферма та Сузуки ..... | 347 |

|                                                                                                                                                  |     |
|--------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Додаток Г. Порівняння кодових характеристик не примітивних недвійкових кодів БЧХ і алгеброгеометричних кодів, побудованих за кривими Ерміта..... | 351 |
| ЛІТЕРАТУРА .....                                                                                                                                 | 354 |

## ВСТУП

Системи управління та зв'язку є, як правило, складовими частинами сучасних комплексів управління технічними об'єктами та людьми. Такі комплекси отримали розвиток завдяки прогресу в області комп'ютерної техніки, автоматизації управління й технологічних процесів.

Прагнення забезпечити високу перешкодозахищеність, множинний безконфліктний доступ до каналу, а також енергетичний та інформаційний захист повідомлень, що передаються каналами управління та зв'язку, привело до створення широкосмугових перешкодозахисних адресних систем зв'язку, які працюють в режимі вільного доступу з кодовим ущільненням каналів. Вільний доступ забезпечується тим, що загальний широкосмуговий радіотракт може використовуватися абонентами в разі необхідності, коли з'являються повідомлення, які підлягають передачі.

Теоретичною основою перешкодозахищеного зв'язку є відома теорема американського вченого Клода Шеннона щодо пропускну здатності каналу зв'язку. Вона стверджує, що при швидкості передачі інформації, меншій за пропускну здатність каналу зв'язку, існують такі засоби перетворення інформації (кодування), які дозволяють передавати цю інформацію із заданою якістю при як завгодно малому відношенні потужності сигналу до потужності перешкоди. Ця теорема не вказує на конкретні методи кодування, однак чітко формулює шлях досягнення заданої якості передачі. Дійсно, у відповідності з фундаментальною теоремою К. Шеннона пропускну здатність каналу зв'язку залежить від ширини смуги пропускання каналу та відношення потужності сигналу до потужності перешкоди. Відповідно, при значному зменшенні відношення потужності сигналу до потужності перешкоди для досягнення заданої якості передачі необхідно застосовувати такі методи кодування сигналів, які приводять до розширення спектра сигналів. Такі методи передачі інформації набули назву широкосмугових сигналів.

Серед відомих широкосмугових систем сигналів, які вже знайшли використання, значний інтерес становлять лінійні рекурентні послідовності, ортогональні послідовності, а також складені системи сигналів [10–12, 17–19, 94, 96, 122]. Це пов'язано з тим, що розпізнавання таких сигналів здійснюється з найбільш високою достовірністю.

Питанню синтезу складних сигналів, що мають необхідні властивості, присвячений великий ряд робіт [10, 26, 51, 101–105, 115, 128], в яких сформульоване завдання синтезу складних сигналів у загальному вигляді й розглянуті характерні особливості синтезу. Відзначимо, що в теперішній час існують різні напрями синтезу дискретних сигналів. Так, наприклад, у [18, 30, 31, 36–38, 107, 127] запропоновані процедури синтезу дискретних сигналів асимптотичними методами в спектральній області за періодичною

функцією автокореляції, які дозволяють одержати непогані наближення до необхідних значень функції автокореляції. Проте ці методи дозволяють синтезувати окремі сигнали, які мають необхідні періодичні функції автокореляції для двійкового алфавіту. Крім того, синтезовані в [15, 16, 40–42, 65, 93] сигнали мають східчасту структуру, що приводить до використання додаткової амплітудної модуляції. У джерелах [109, 110, 113, 116, 117] досліджуються питання синтезу недвійкових сигналів у часовій області за аперіодичною функцією автокореляції на основі розв'язання складних системи рівнянь. У більшості джерел розв'язання таких систем зводиться до простого перебору компонент, за яким визначаються граничні значення функцій кореляції. У роботах [4, 6, 8, 129, 132, 139, 149] запропоновані методи синтезу дискретних сигналів за функцією невизначеності в спектральній області. Використання цих методів дозволяє одержати, як і в разі синтезу дискретних сигналів за періодичною функцією автокореляції, двійкові сигнали східчастої форми. Метод синтезу сигналів з необхідними спектральними властивостями, викладений в [8, 31, 40], дозволяє одержувати сигнали з малим рівнем “бічних складових” амплітудного спектра. Проте в [63, 64, 94] не розглядаються ансамблі, авто- і взаємокореляційні властивості синтезованих сигналів. У [101–105, 144, 145] синтезовані дискретні сигнали з хорошими авто- і взаємокореляційними властивостями на основі розв'язання сукупності систем нелінійних нерівностей функцій авто- і взаємокореляції. Запропоновані в [12, 15, 16, 31, 46, 73] процедури синтезу дискретних сигналів дозволяють, на відміну від інших методів синтезу дискретних сигналів, синтезувати не окремі сигнали, а ансамблі сигналів, які мають необхідні авто- і взаємокореляційні властивості. Проте запропоновані в [93, 94, 100, 140–141] методи синтезу фазоманіпульованих сигналів мають ряд недоліків:

- не всі сигнали, синтезовані за допомогою відомих методів, задовольняють розв'язанню систем нерівностей, що задають потрібні авто- та взаємокореляційні властивості;

- використання більшості відомих методів призводить до великих часових витрат синтезу ансамблю сигналів;

- задача розв'язання систем нерівностей функцій авто- і взаємокореляції вирішена лише для випадку двійкових систем сигналів;

- не можна заздалегідь (до закінчення розв'язання задачі синтезу сигналів) визначити об'єм ансамблю сигналів, що синтезуються.

Таким чином, до теперішнього часу не розроблені методи синтезу великих ансамблів сигналів слабкорельованих між собою дискретних сигналів. Крім того, деякі питання перешкодозахисної передачі інформації можна вирішити ефективніше за допомогою методів перешкодостійкого



кодування рівнів дискретного каналу. Так, наприклад, при значенні ймовірності прийому одного сигналу, меншому ніж  $10^{-3}$ , використання практично будь-якого перешкодостійкого коду дозволяє отримати певний енергетичний виграш. При цьому виграш зростає при підвищенні довжини коду.

Теорія та методи побудови кодів, що корегують помилки в дискретних каналах зв'язку, найбільш повно викладені у монографіях [20, 21, 67, 69, 71, 72, 83, 85, 87, 126]. У джерелах [20, 21, 69, 71, 72, 74, 126] наводяться оригінальні ідеї з побудови алгоритмів кодування та декодування перешкодостійких кодів. Традиційно теорія перешкодостійкого кодування розвивається у двох споріднених напрямках. Перший пов'язаний із методами побудови безперервних (деревоподібних) кодів, які засновані переважно на алгоритмах випадкового пошуку. Найбільш відомим класом безперервних кодів є згортувальні коди, теорія та методи побудови яких докладно викладені у монографіях [20, 21, 70].

Другий напрямок розвитку теорії перешкодостійких кодів пов'язаний із застосуванням кодів кінцевої довжини (блоковими кодами) та оперує переважно алгебраїчними методами кодування та декодування. Алгебраїчна теорія блокових кодів найбільш докладно викладена у монографіях [20, 24, 87]. Проте найбільш відомі методи перешкодостійкого кодування мають суттєвий недолік – погіршення кодових властивостей порівняно з теоретичною межею зі зростанням довжини коду. Крім того, часова та ємкісна складність алгоритмів кодування та декодування зі зростанням довжини коду швидко зростає. Ця обставина не дозволяє досягти показників теоретично можливої перешкодостійкості при фіксованому співвідношенні енергії сигналу до спектральної щільності перешкод у каналах зв'язку. Через це проблема побудови перешкодозахисних систем управління та зв'язку є актуальною. Її вирішення пов'язано із важливими науково-прикладним завданням розробки сигнально-кодових конструкцій з покращеними кореляційними, ансамблевими та структурними властивостями на сигнальному рівні та з такими кодовими властивостями, які не погіршуються при підвищенні довжини та потужності коду. Актуальними є також розробка та дослідження алгоритмів обробки сигналів, методів та алгоритмів перешкодостійкого кодування та декодування.

У монографії наводяться нові результати, що пов'язані з розвитком алгебраїчної теорії кодів, зокрема з розробкою методів та алгоритмів кодування алгеброгеометричними кодами; з розвитком теорії сигналів, зокрема з розробкою похідних та складених систем сигналів. Досліджуються питання побудови ефективних сигнально-кодових конструкцій для поліпшення якісних характеристик систем управління та зв'язку.