Міністерство освіти і науки України
Вінницький національний технічний університет

**В. П. Семеренко**

# ТЕОРІЯ ЦИКЛІЧНИХ КОДІВ НА ОСНОВІ АВТОМАТНИХ МОДЕЛЕЙ

**Монографія**

Вінниця
ВНТУ
2015

УДК 681.3.06.(075)
ББК 32.973.26-018.1
С34

Рекомендовано до друку Вченою радою Вінницького національного технічного університету Міністерства освіти і науки України (протокол № 7 від 26.02.2015 р.)

Рецензенти:
**В. А. Лужецький**, доктор технічних наук, професор
**Л. І. Тимченко**, доктор технічних наук, професор

**Семеренко, В. П.**

С34 Теорія циклічних кодів на основі автоматних моделей : монографія / В. П. Семеренко. – Вінниця : ВНТУ, 2015. – 444 с.

ISBN 978-966-641-624-0

Запропоновані автоматні моделі циклічних кодів на основі теорії лінійних послідовнісних схем (ЛПС). Розглянуто систематичне і несистематичне кодування циклічних кодів за допомогою рекурсивних, нерекурсивних і комбінованих ЛПС. Наведені автоматно-графові методи декодування лінійної і поліноміальної складності для різних типів помилок: випадкових, пакетів помилок, стирань. Показані резерви підвищення продуктивності процедур кодування і декодування на основі паралельної обробки даних. Запропоновані нові оцінки здатності циклічних кодів виявляти та виправляти помилки на основі графового представлення коду. Розглянуті особливості кодів БЧХ, Ріда–Соломона, Файра, Абрамсона, і запропоновані паралельні циклічні коди.

**УДК 681.3.06.(075)**
**ББК 32.973.26-018.1**

**ISBN 978-966-641-624-0**

**ЗМІСТ**

## ПЕРЕЛІК СКОРОЧЕНЬ

АБГШ – канал з адитивним білим гаусівським шумом
БЧХ-код – код Боуза–Чоудхурі–Хоквінгема
ВОЛЗ – волоконно-оптична лінія зв’язку
ВПВ – «вертикальна» пов’язуюча вершина
ВПС – «вертикальний» пов’язуючий стан
ГПВП – генератор псевдовипадкової послідовності
ДКБП – дискретний канал без пам’яті
ДКС – двійковий канал зі стиранням
ДП – діаграма переходів
ДСК – двійковий симетричний канал
КЛ-код – квадратично-лишковий код
КДКС – комбінований двійковий канал зі стиранням
ЛПС – лінійна послідовнісна схема
ЛПМ – лінійна послідовнісна машина
М-послідовність – послідовність максимального періоду
МДВ-код – код з максимально досягнутою відстанню
НСК – найменше спільне кратне
НЦ – нульовий цикл
ОНЦ – основний нульовий цикл
ОЦ – одиничний цикл
ООЦ – основний одиничний цикл
ПВП – псевдовипадкова послідовність
ПНЦ – периферійний нульовий цикл
РД – решіткова діаграма
РЗЛОЗ – регістр зсуву з лінійним оберненим зв’язком
РС-код – код Ріда–Соломона
СА – сигнатурний аналізатор
ТОЦ – тривіальний одиничний цикл
ТНЦ – тривіальний нульовий цикл
ФГ – фактор-граф
ЦС – цифрова схема
CRC (Cyclic Redundancy Code) – циклічний надлишковий код

# ПЕРЕДМОВА

Датою народження сучасного завадостійкого кодування прийнято вважати появу у 1948 році знаменитої статті К. Шеннона [1], в якій було доведено таке твердження (теорема Шеннона–Хартлі): при будь-якій продуктивності джерела повідомлень, що не перевищує пропускної здатності каналу, існує такий спосіб кодування, який дозволяє передати всю інформацію від джерела з довільно малою ймовірністю помилки.

Теорема не дає конкретних рекомендацій про способи побудови конкретних кодів для забезпечення ідеальної передачі інформації, однак саме ця обставина і стала початковим поштовхом до розвитку завадостійкого кодування.

Як і більшість інших фундаментальних відкриттів, роботи зарубіжних [2, 3] і вітчизняних [4, 5] піонерів в цій сфері науки з’явились у відповідь на практичні потреби. В 50-х і 60-х роках XX століття людство стало освоювати космічний простір і виникла необхідність в безпомилковій передачі даних від супутників та космічних кораблів [6].

Космічний зв'язок в ті роки мав свої особливості. По-перше, характер спотворень в таких каналах дуже точно описувався моделлю адитивного білого гаусового шуму, що спричинило вивчення саме таких теоретичних моделей каналів. Внаслідок великих відстаней для передачі даних були необхідні потужні коректувальні коди зі складними алгоритмами декодування, хоча платою за це була низька швидкість передачі корисних даних. Надлишок смуги пропуску дозволяв використовувати коди з низькою спектральною густиною.

Теорія завадостійкого кодування почала бурхливо розвиватися і поступово впроваджуватися в інші сфери: цифровий аудіо- та відеозв’язок, мобільний зв’язок і передачу даних в комп’ютерах. З кожним роком ставало все більш зрозумілим, що старі моделі вже не могли коректно описувати процеси в інших системах. Необхідність врахування різних системних і технологічних компромісів сприяла появі нових критеріїв оптимальності кодів.

Практичні потреби знову стали каталізатором подальшого розвитку завадостійкого кодування, яке продовжується і в наші дні. Значний внесок в розвиток теорії кодування внесли також і вчені України [7–13].

Не применшуючи значення численних відомих сьогодні кодів, все ж варто відзначити величезну роль завадостійких кодів, які входять до класу циклічних кодів. Вперше ці коди були запропоновані Прейнджем [14], а потім розвинуті в роботах учених, чиї імена увічнені в назвах досліджених ними кодів – Хемінга [2], Голея [3], Боуза і Рой-Чоудхурі [15], Хоквінгема [16], Файра [17], Ріда і Соломона [18].

Головними перевагами циклічних кодів є їх висока коректувальна здатність і прості схеми кодування–декодування. Саме тому вони мають дуже широку сферу використання: системи передачі даних, цифрове телебачення, магнітні і оптичні носії інформації. Прикладом одного з нових напрямків практичного застосування може служити організація захисту інформації в двовимірних матричних штрих-кодах за допомогою кодів Ріда–Соломона (РС) [19]. На основі циклічних кодів були розроблені коди Кердока, Препарати, Юстесена, Гоппи, альтернантні коди, алгеброгеометричні коди та інші.

В 60–80 роки з’явилися класичні роботи по кодуванню: У. Пітерсона, Ф. Мак-Вільямса, Н. Слоена, Е. Берлекемпа та інших зарубіжних та вітчизняних дослідників [20–29]. За останні два десятиріччя кращим виданням в цій області можна вважати енциклопедичну роботу Б. Скляра [30].

В кожній із зазначених книг є декілька розділів про циклічні коди. На жаль, практично відсутні серйозні роботи, які стосувалися б тільки циклічних кодів. Винятком може служити опублікована більше 40 років тому відома книга В. Д. Колесника і Е. Т. Мирончикова [31]. Недавно вийшла з друку нова книга В. Д. Колесника [32], де головну увагу приділено різноманітним підкласам циклічних кодів.

За минулий період з’явилося багато нових матеріалів, в яких досліджуються як традиційні циклічні коди, так і різні варіанти їх об’єднання з іншими кодами.

Тому давно з’явилась необхідність в узагальненні отриманих результатів і публікації нових книг, темою яких стали ці чудові коди. Запропонована монографія направлена на ліквідацію вказаної прогалини.

Головною тенденцією в розвитку сучасних систем зв’язку є постійне збільшення швидкості передавання, практичне освоєння терабайтного діапазону. Основні досягнення останніх років пов’язані з широким використанням оптичних систем зв’язку [33]. Як і для попередніх технологій в системах передачі даних, основним резервом в підвищенні швидкості передавання є використання завадостійкого кодування. Використання кодів, що виправляють помилки (error correcting codes – ECC), дозволяє не тільки покращити якість передачі, але і зменшити кількість оптичних підсилювачів та збільшити довжину між регенераційними ділянками волоконно-оптичних ліній зв’язку (ВОЛЗ). [34]. Знаменним є те, що для наддалеких ВОЛЗ для швидкостей передавання 40 Гбіт/сек і вище вибір знову було зроблено на користь кодів РС. При високих відношеннях сигнал/шум послідовно з’єднані коди Боуза–Чоудхурі–Хоквінгема (БЧХ) і РС переважають недавно винайдені турбо-коди [35].

Однак, в оптичних системах передачі даних ще залишаються вузли електронної обробки і тому необхідна елементна база з граничними частотами, які щонайменше в п’ять разів перевищують швидкість передавання даних. Найкращим вирішенням цієї проблеми стане перехід до широкого використання паралельної обробки даних при кодуванні та декодуванні повідомлень.

Сучасні досягнення мікро- та наноелектроніки дозволяють апаратно й програмно реалізовувати складні алгоритми завадостійкого кодування й декодування з використанням кодів з великою коректувальною здатністю. Але швидке та ефективне виконання операцій кодоперетворення можливе тільки на основі принципів паралелізму. Завдяки паралельній обробці можна не тільки прискорити виконання традиційних процедур кодування–декодування, а також реалізувати нові підходи, наприклад, одночасний пошук помилок різних типів. Такі задачі актуальні для

нестаціонарних каналів, в яких швидко змінюються параметри передачі даних.

Ще одним важливим резервом в підвищенні продуктивності при передачі даних є використання багатоканальних систем. Як багатоканальні лінії зв’язку використовуються не тільки безпровідні, але і провідні лінії зв’язку (кабельний зв'язок). Найбільша сфера використання багатоканальних систем передачі даних – в комп’ютерах і комп’ютерних мережах [36, 37]. Їх головні особливості – інша модель помилок та словоорієнтована архітектура. Тому актуальною є розробка теоретичних основ паралельних циклічних кодів та ефективних методів їх кодування і декодування.

Для розв’язання нових задач необхідні розробка нових математичних моделей, нових методів обробки кодових сигналів, використання сучасних досягнень комп’ютерної архітектури з врахуванням специфіки паралельних обчислень.

Звичайно, автор не претендує на повноту викладення всіх аспектів, що пов’язані з циклічними кодами. Ця книга не є енциклопедією з циклічних кодів, в ній лише коротко наведені основні відомості про ці коди, а головна увага приділена новим результатам, які отримані автором: методам кодування й декодування циклічних кодів на основі їх автоматного представлення, розробці паралельних циклічних кодів в двійкових і недвійкових полях Галуа, а також використання методів паралельної обробки при програмній і апаратній реалізації кодерів–декодерів циклічних кодів.

# Розділ 1
# ВСТУП ДО ТЕОРІЇ ЗАВАДОСТІЙКОГО КОДУВАННЯ

## 1.1 Загальні відомості про систему передачі даних

Розглянемо коротко процес перетворення інформації в узагальненій системі передачі даних. Структурна схема передачі даних наведена на рис. 1.1.

Інформаційне повідомлення, які поступає від джерела повідомлень, спочатку обробляється *кодером джерела* з метою його більш компактного представлення, використовуючи різні способи ущільнення даних. Далі *кодер каналу* додає деяку надлишковість в кодове слово джерела і формує кодове слово каналу, яке має більшу послідовність символів, ніж у слові джерела. Кожний символ кодового слова каналу може бути представлений одним або кількома бітами. Передавач перетворює кодове слово каналу в форму, зручну для передавання по каналах зв'язку. Одним з головних вузлів передавача є *модулятор*, який перетворює цифрові символи в аналоговий сигнал.

*Канал зв'язку* – це фізичне середовище, по якому відбувається передавання сигналів від передавача до приймача. Оскільки в каналі зв'язку можливі шуми та спотворення, тому сигнали на його виході можуть відрізнятись від вхідних сигналів.

Далі сигнали в приймачі за допомогою *демодулятор*а знову перетворюються в цифрову форму, придатну для подальшої обробки.

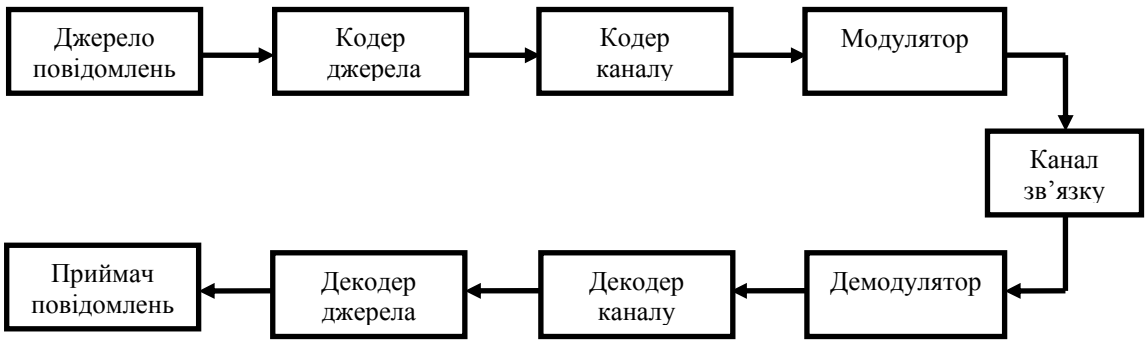



Рисунок 1.1 – Структурна схема передачі даних

Частину тракту передачі від входу модулятора до виходу демодулятора часто називають дискретним каналом, оскільки входом і виходом каналу є символи кінцевого алфавіту.

*Декодер каналу* спочатку оцінює прийняте кодове слово. Якщо в ньому відсутні спотворення, тоді в ньому відразу виділяється кодове слово джерела. В протилежному випадку декодер каналу, використовуючи надлишковість кодового слова каналу, виправляє наявні помилки (коректувальна здатність залежить від ступеня надлишковості кодового слова) і видає виправлене кодове слово джерела.

*Декодер джерела* виконує операцію, яка є оберненою до операції кодера джерела, результат якої вже поступає до користувача.

В монографії кодер і декодер джерела не розглядаються, тому в подальшому викладенні під операціями кодування і декодування розуміються тільки кодування і декодування каналу. Саме таке кодування і називають *завадостійким*.

Якщо в перші десятиріччя розвитку систем передачі даних операції канального кодування і модуляції розглядались як окремі та незалежні операції, то зараз вони використовуються одночасно як єдиний процес обробки сигналів [30, 38].

Відзначимо також, що канал використовується не тільки в традиційній системі зв'язку, наприклад, в системі передачі сигналів із супутника на приймальну антену. Процес збереження або запису даних на зовнішніх носіях також може розглядатися як своєрідний канал передачі даних.

## 1.2 Завади й помилки в каналах передачі даних

При передачі по каналу інформація піддається впливу різноманітних завад (шумів), в результаті можна отримати повідомлення від відправника з деякими помилками [39].

За місцем появи завади в каналі можна розділити на декілька груп: природного походження, промислові та ті, що виникають в апаратурі.

До перешкод природного походження належать завади від атмосфери, сонця, різних галактичних об'єктів. Джерелом промислових завад можуть бути лінії електропередач, різноманітні електроустановки,

електротранспорт. Свій вклад в загальну картину перешкод вносить і сама апаратура зв'язку.

В залежності від характеру змін в часі розрізняють флуктуаційні, гармонічні та імпульсні перешкоди, а також замирання.

*Флуктуаціями* у фізиці називають випадкові відхилення деяких фізичних величин від їх середніх значень. Прикладом таких явищ може служити тепловий шум апаратури. Математично тепловий шум можна описати як гаусівський випадковий процес. Потужність цього шуму характеризується постійною спектральною густиною потужності для всіх частот, і тому його називають «білим». Таким чином, флуктуаційні завади найкраще описувати як *білий гаусівський шум.*

*Гармонічна завада* описується синусоїдальним коливанням.

Флуктуаційні та гармонічні завади діють безперервно протягом тривалих інтервалів часу.

*Імпульсні завади* діють тільки в окремі моменти часу, зазвичай вони з'являються групами. Пікове значення імпульсної завади співмірне з амплітудою корисного сигналу і може його перевищувати.

*Замирання* (fadihg) – це завади, які виникають в безпровідному зв'язку і обумовлені наявністю багатократних шляхів проходження сигналів і відбиттям радіохвиль від природних і штучних перешкод.

Завади можуть або підсумовуватись з корисним сигналом (адитивні завади), або помножуватися з ним (мультиплікативні завади).

Вплив різних типів завад проявляється в тому, що замість переданих символів можуть бути прийняті зовсім інші. Таку подію називають *помилкою*.

Розрізняють *інверсні* помилки (зміна правильних значень на інші із заданого алфавіту значень) і *стирання* (помилки, в яких невідомі значення, але відоме їх розташування). Інверсні помилки можуть бути або *випадковими* (тобто рознесеними по всій довжині повідомлення), або *пакетними* (зосередженими в обмеженій області повідомлення) (рис. 1.2). Далі будуть наведені більш строгі визначення типів помилок. В поточному розділі розглядаються, як правило, інверсні випадкові помилки, які далі коротко будуть йменуватись просто помилками.

В [40] наведена статистика помилок в мережах АТМ в умовах експлуатації з використанням волоконно-оптичних ліній зв'язку: 65 %

складають поодинокі помилки, 23 % складають дво- і трикратні помилки, 12 % – пакетні помилки кратністю від 5 і більше.

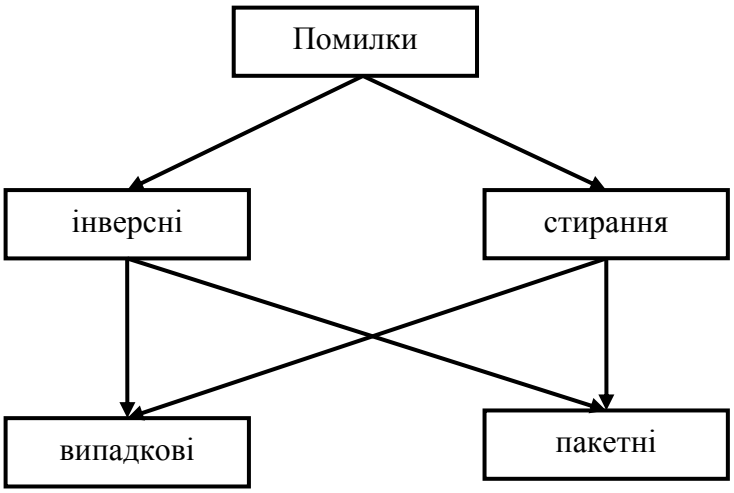



Рисунок 1.2 – Спрощена класифікація помилок
в каналах передачі даних

Як і завади, помилки є випадковими подіями, тому для них також будуть використовуватись ймовірнісні характеристики.

## 1.3 Теоретичні моделі каналів

Для оцінки ймовірності помилки, які забезпечує завадостійкий код, необхідно мати математичний опис каналу зв'язку, по якому відбувається передача повідомлень. Модель каналу повинна відображати статистику помилок у фізичному каналі і не вимагати складних математичних розрахунків. Коротко розглянемо дві групи теоретичних моделей каналів: канали без пам'яті та канали з пам'яттю. Нехай $X = \{0, 1, \ldots, q-1\}$ – вхідний алфавіт (на вході каналу зв'язку), з якого формуються кодові слова, і $Y = \{0, 1, \ldots, q-1\}$ – вихідний алфавіт (на виході каналу зв'язку).

### 1.3.1 Моделі каналів без пам'яті

Найпростішою моделлю каналу без пам'яті є *двійковий симетричний канал* (ДСК, binary symmetric channel – BSC). У цього каналу вхі-

дний $X$ і вихідний $Y$ алфавіти складаються лише з двійкових елементів: $X = \{0,1\}, Y = \{0,1\}$. В результаті дії завад з ймовірністю $p$ може відбутися спотворення переданої інформації: замість переданого 0(1) буде отримано 1(0). Відповідно, ймовірність отримання правильної інформації визначається ймовірністю $(1-p)$:

$$p(Y=0 \mid X=1) = p(Y=1 \mid X=0) = p;$$

$$p(Y=1 \mid X=1) = p(Y=0 \mid X=0) = 1-p,$$

де $p(j \mid i)$ – умовна ймовірність прийому символу $j$ при переданому символі $i$.

Схема ДСК наведена на рис. 1.3.

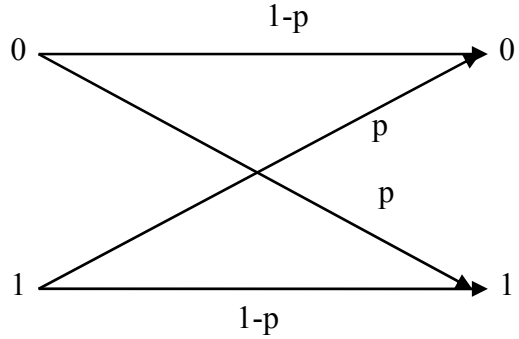



Рисунок 1.3 – Схема двійкового симетричного каналу

*Дискретний канал без пам'яті* (ДКБП, discrete memoryless channel – DMC) є узагальненням ДСК і характеризується $m$-значним вхідним алфавітом $X$ і $m$-значним вихідним алфавітом $Y$:

$$X = (0, 1, \ldots, m-1);\ Y = (0, 1, \ldots, m-1).$$

Для задання дії завад в такому каналі використовують набори умовних ймовірностей $p(j \mid i)$, $(0 \le j \le m-1, 0 \le i \le m-1)$.

ДКБП ще називають *біноміальним.*

Схема ДКБП наведена на рис. 1.4.

*Двійковий канал зі стиранням* (ДКС, binary erasure channel – BEC) – це канал з двозначним вхідним $X$ алфавітом і тризначним вихідним $Y$ алфавітом: $X = \{0,1\}, Y = \{0,1,x\}$. Символ «$x$» тут позначає відсутність будь-якої інформації, тобто її стирання. Схема ДКС наведена на рис. 1.5.

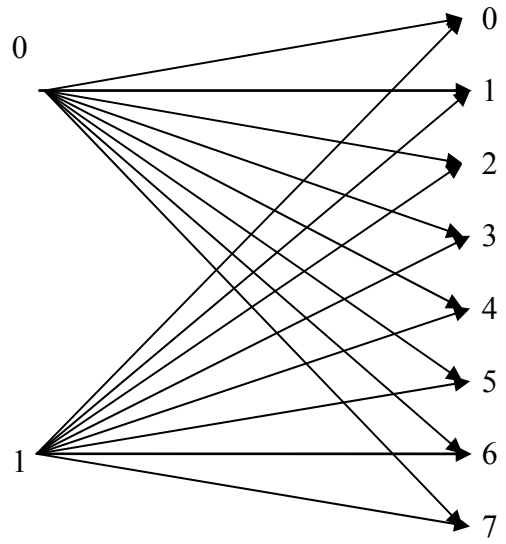



Рисунок 1.4 – Схема дискретного каналу без пам’яті для $m = 8$

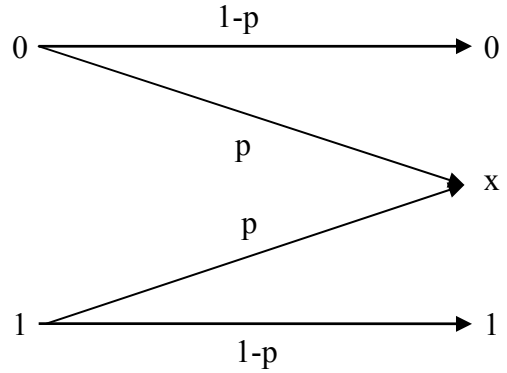



Рисунок 1.5 – Схема двійкового каналу зі стиранням

На практиці стирання часто поєднується з помилками інверсії вхідних сигналів. Схема *комбінованого двійкового каналу зі стиранням* (КДКС) наведена на рис. 1.6.

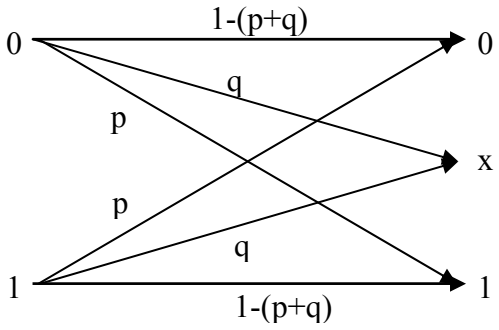



Рисунок 1.6 – Схема комбінованого двійкового каналу зі стиранням

*Гаусівський канал* (Gaussian channel) – це канал з дискретним вхідним алфавітом $X$ і неперервним вихідним алфавітом $Y$:

$$X = (0, 1, \ldots, m-1);\ Y = \{-\infty, +\infty\}.$$

Найважливішим різновидом каналом цього типу є *канал з адитивним білим гаусівським шумом* (АБГШ, additive white Gaussian noise – AWGN). Термін «адитивний» означає, що шум просто накладається на сигнал.

Демодулятор гаусового каналу приймає м'яке рішення – видає декодеру каналу додаткову інформацію про надійність прийому даних, яка може бути використана для точнішого декодування. Якщо демодулятор не зміг точно відрізнити нульовий сигнал від одиничного, тоді у відповідному розряді прийнятого кодового слова буде записаний невизначений символ $x$.

### 1.3.2 Моделі каналів з пам'яттю

Переважна більшість каналів, які зустрічаються в техніці зв'язку, це канали з пам'яттю. Для коректного опису функціонування таких каналів недостатньо знання тільки одного параметра, яким в каналах без пам'яті є ймовірність помилки $p$ [30]. Необхідно ще знати ймовірності будь-яких сполучень помилок в межах блоку даних, який передається.

Якщо в каналі без пам'яті умовна ймовірність помилкового прийому $(i+1)$-го символу при умові, що $i$-й символ прийнято помилково, рівна безумовній ймовірності помилки

$$p(i+1 \mid i) = p,$$

тоді в каналі з пам'яттю вона може бути більшою або меншою цієї величини. Найчастіше виконується умова

$$p(i+m \mid i) \geq p,$$

яка означає, що в каналі помилки мають тенденцію до групування. Причиною таких помилок можуть бути флуктуаційні завади і замирання, які мають тривалий часовий інтервал дії.

Рідше зустрічаються канали із розосередженими помилками, в яких

$$p(i+m \mid i) < p.$$

Причиною таких помилок можуть бути імпульсні завади, які з'являються рідко і представляють собою випадкову послідовність коротких сигналів.

Найбільш прийнятними теоретичними моделями каналів з пам'яттю є модель Гільберта та її різноманітні модифікації (Эліота–Гільберта, Беннета–Фройліха, Фрічмана та інших) [41].

Згідно з базовою моделлю Гільберта канал може знаходитись в одному з двох станів:

– хорошому стані $S_g$, в якому помилки відсутні;

– поганому стані $S_b$, в якому помилки з'являються випадково з ймовірністю $p_{ош}$ (найчастіше приймають $p_{ош} = 0{,}5$).

Якщо при передаванні символу $x_i$ канал знаходиться в стані $S_g$, тоді при передаванні наступного символу $x_{i+1}$ канал буде знаходитись в тому ж стані з ймовірністю $p_{gg}$ і в стані $S_b$ – з ймовірністю $p_{gb} = 1 - p_{gg}$. Якщо ж при передаванні символу $x_i$ канал знаходився в стані $S_b$, тоді при передаванні наступного символу $x_{i+1}$ канал буде знаходитись в тому ж стані з ймовірністю $p_{bb}$ і в стані $S_g$ – з ймовірністю $p_{bg} = 1 - p_{bb}$. Матрицю з ймовірностями переходів між станами можна записати таким чином:

$$P = \begin{bmatrix} p_{gg} & p_{gb} \\ p_{bg} & p_{bb} \end{bmatrix}.$$

Граф станів моделі Гільберта показаний на рис. 1.7.

Параметри моделі Гільберта визначають середню ймовірність $P_g$ знаходження каналу в хорошому стані і середню ймовірність $P_b$ знаходження в поганому стані:

$$P_g = \frac{p_{bg}}{p_{bg} + p_{gb}}; \qquad P_b = \frac{p_{gb}}{p_{bg} + p_{gb}}. \tag{1.1}$$

Із (1.1) можна знайти середні довжини хорошого $D_g$ і поганого $D_b$ станів каналу і на їх основі визначити ймовірну довжину пакету помилок:

$$D_g = \frac{1}{p_{gb}} \; ; \qquad D_b = \frac{1}{p_{bg}}.$$

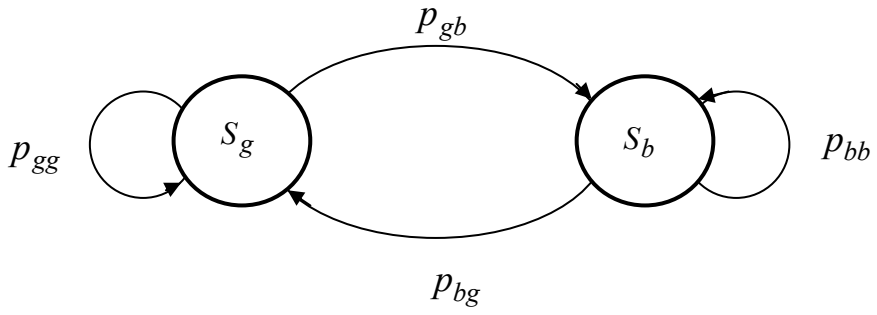



Рисунок 1.7 – Граф станів моделі Гільберта

Різновидом каналів з пам'яттю є *канали із замираннями* (fading channels). Такі моделі каналів, на відміну від моделі Гільберта, є складнішими, проте дозволяють більш адекватно представити сучасні системи зв'язку, зокрема системи безпровідного зв'язку [30].

### 1.4 Основні принципи виявлення та виправлення помилок

Розглянемо, яким чином використання завадостійкого кодування дозволяє збільшити надійність передавання по цифрових каналах.

Як вже відзначалося, процес перетворення повідомлень в комбінацію різних символів називається кодуванням, а отримана послідовність символів – *кодовим словом*. Максимальна кількість різних комбінацій, які можна отримати із $n$-розрядного кодового слова, визначається відомою формулою з комбінаторики:

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \quad \ldots \quad + \binom{n}{n} = 2^n,$$

де $\binom{n}{i}$ – число комбінацій із $n$ по $i$.

Якщо при побудові коду будуть дозволені будь-які комбінації з $2^n$ можливих, тоді такий код не зможе встановити навіть наявність спо-

творень, оскільки будь-яке прийняте кодове слово буде інтерпретовано як допустиме, тобто правильне. Кажуть, що в цьому випадку мінімальна кодова відстань дорівнює одиниці. Зазначимо, що тут ми розглядаємо тільки модель помилок каналу ДСК, коли можливі лише інверсні помилки.

Основним способом виявлення і виправлення помилок (не тільки інверсних, але про інші типи помилок детальніше в наступних розділах) служить введення надлишковості в повідомлення, що передаються. В цьому випадку кодовим словам будуть відповідати тільки дозволені кодові комбінації, число $N_p$ яких складає тільки частину із всіх можливих комбінацій $N$:

$$N_p = 2^k, \quad N_p < N.$$

Величину $k$ прийнято називати *розмірністю* завадостійкого $(n, k)$-коду.

Серед різних $(n, k)$-кодів будемо розглядати лише блокові $(n, k)$-коди, в яких кожному інформаційному повідомленню відповідає блок із $n$ символів, причому блоки кодуються й декодуються окремо один від одного. Обмежимось лінійними кодами, тобто кодами з визначеною лінійною структурою (більш строге означення лінійних кодів буде дано в другому розділі). Саме до такої різновидності кодів належать циклічні коди.

Ступінь надлишковості $(n, k)$-коду визначається кількістю перевірочних символів $r$ ($r = n - k$). Співвідношення параметрів $k$ і $n$ йменують *швидкістю коду* $\theta$:

$$\theta = \frac{k}{n}.$$

В систематичному циклічному коді слово довжини $k$ називають *інформаційним словом*, слово довжини $r = n - k$ *– контрольним словом*. В несистематичному коді не можна явно виділити інформаційне і контрольне слова, надлишковість ніби рівномірно розподілена по кодовому слову.

ОЗНАЧЕННЯ 1.1. Помилкою кратністю $\tau$ в кодовому слові $Z$ називається така зміна $\tau$ його розрядів, коли нове слово $Z_{err}$ не є кодовим ($\tau \le \tau_{\min}$).

Помилка хоча б в одному розряді кодового слова призводить до появи забороненого слова. Кількість виявлених та виправлених помилок в заданому коді залежить від взаємного розташування в кодовому просторі дозволених і заборонених слів.

ОЗНАЧЕННЯ 1.2. Вагою $w(y)$ слова $y$ називається кількість його ненульових компонентів.

Наприклад, вага кодового слова $y = 1\,1\,0\,0\,1\,0$ дорівнює $w(y) = 3$.

С поняттям ваги слова тісно пов'язане поняття *кодової відстані*. Розрізняють три види кодової відстані: Хемінга, Лі та матричне. В теорії кодування найчастіше використовується перша з них.

ОЗНАЧЕННЯ 1.3. Відстанню за Хемінгом $d(Z_1, Z_2)$ між двома кодовими словами $Z_1$ і $Z_2$ довжини $n$ називається число розрядів (позицій), в яких вони відрізняються.

Для знаходження відстані за Хемінгом двох двійкових кодових слів необхідно знайти їх суму по модулю два і потім підрахувати число ненульових компонентів, тобто визначити вагу цієї суми.

Наприклад, для слів $Z_1 = 1\,1\,0\,0\,1\,0$ и $Z_2 = 0\,1\,0\,1\,1\,0$ їх сума $Z = Z_1 \oplus Z_2$ по модулю два рівна $1\,0\,0\,1\,0\,0$, тому вага дорівнює $w(Z) = 2$ і, відповідно, відстань між ними за Хемінгом дорівнює $d(Z_1, Z_2) = 2$.

Завдяки лінійним властивостям циклічних кодів ніякі два кодових слова не розташовані в кодовому просторі поруч, тобто на одиничній відстані за Хемінгом. Між ними завжди є хоча б одне некодове слово.

ОЗНАЧЕННЯ 1.4. Мінімальна кодова відстань $d_{\min}$ лінійного блокового коду $\Omega$ дорівнює найменшій із всіх відстаней за Хемінгом $d(Z_1, Z_2)$ між різними парами кодових слів:

$$d_{\min} = \min d(Z_i, Z_j), \quad Z_i, Z_j \in \Omega, \quad i \neq j .$$

При надходженні на вхід декодера некодового слова задача декодера полягає у виборі такого кодового слова, яке знаходиться на найближчій відстані за Хемінгом від прийнятого слова.

Якщо між кодовими словами розташовано лише одне некодове слово, тоді декодер не зможе вибрати одне правильне з двох можли-

вих, тобто помилка в коді з $d_{\min} = 2$ не може бути виправлена, тільки виявлена.

Виправлення поодинокої інверсної помилки можливе лише для коду з $d_{\min} \geq 3$, коли між будь-якими кодовими словами є не менше двох некодових слів.

В загальному випадку повинно виконуватись таке співвідношення між $d_{\min}$ та мінімальним числом $\tau_c$ помилок, що виправляються, і числом $\tau_d$ помилок, що виявляються:

$$d_{\min} \geq \tau_d + \tau_c + 1 = 2\tau_c + 1 = \tau_d + 1. \qquad (1.2)$$

Нерівність (1.2) для $(n,k)$-коду можна записати, використовуючи параметри коду:

$$d_{\min} \leq n - k + 1 \quad \text{або} \quad d_{\min} \leq r + 1. \qquad (1.3)$$

Нерівність (1.3) називається границею Сінглтона [24]. Із (1.2) та (1.3) випливає, що для виправлення $\tau_c$ помилок необхідно мати не менше $2\tau_c$ перевірочних символів $r$:

$$\tau_c \leq \frac{d_{\min} - 1}{2} = \frac{n-k}{2} = \frac{r}{2}.$$

Код, для якого виконується рівність

$$d_{\min} = n - k + 1 = r + 1,$$

називається кодом з *максимально досягнутою відстанню* (МДВ-кодом).

Можна також дати просторово-геометричну інтерпретацію *коректувальної здатності* коду. Для коду, який дозволяє виправляти $\tau_c$ помилок, навколо кожного кодового слова можна описати сфери декодування радіуса $\tau_c$, що взаємно не перетинаються. Мінімальна відстань між центрами сфер дорівнює $d_{\min}$. Прийняті декодером слова з помилками кратністю менше $\tau_c$ будуть знаходитись всередині однієї із сфер і будуть декодовані як кодове слово, яке є центром відповідної сфери, тобто помилка буде виправлена. Якщо ж стануться помилки кратністю більше $\tau_c$, тоді прийняте слово може потрапити в іншу сферу і виправлення відбудеться неправильно. Однак, якщо нас ціка-

вить лише факт наявності помилки, тоді можна виявити будь-яку кількість помилок, аби лише прийняте кодове слово з помилками не потрапило в центр якої-небудь сфери. Виявляються всі помилки кратністю не більше, ніж $d_{\min} - 1$, а також багато помилок більшої кратності.

ПРИКЛАД 1.1. Розглянемо код, який складається з двох трирозрядних кодових слів: 000 и 111. За допомогою трьох розрядів можна отримати вісім слів, отже шість з них не будуть кодовими. Параметри такого коду такі: $n = 3, k = 1, d_{\min} = 3$. Для кодового слова 000 в сферу 1 декодування потрапляють три слова (100, 010, 001), які відрізняються від нього тільки в одному розряді. Аналогічним чином для кодового слова 111 в сферу 2 декодування потрапляють останні три слова (рис. 1.8).

ОЗНАЧЕННЯ 1.5. Досконалим кодом називається код, для якого сфери однакового радіуса навколо кодових слів, не перетинаючись, покривають весь простір.

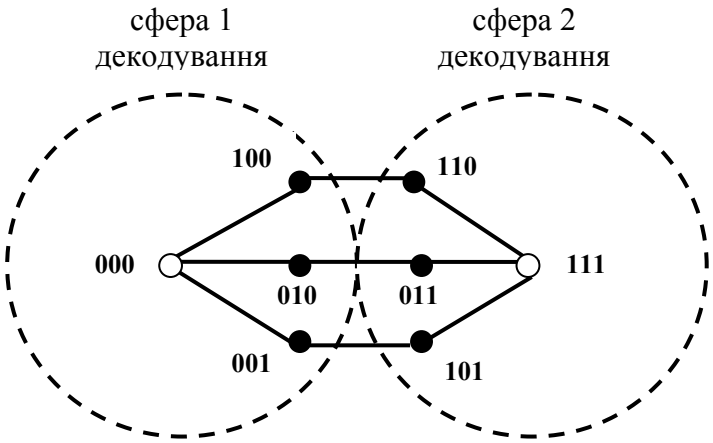



Рисунок 1.8 – Сфери декодування

Розглянутий в прикладі 1.1 код є досконалим. Відомо мало досконалих кодів, більшість складають недосконалі коди. В подальших розділах будуть розглянуті інші досконалі коди, які мають практичне значення.

Для недосконалих кодів сфери декодування не покривають весь простір, деякі слова лежать за межами цих сфер. Можливо, з позицій математичної естетики таке представлення є «недосконалим» (що і спричинило появу такого терміну), однак недосконалі коди (насамперед, циклічні недосконалі коди) дозволяють виправляти додаткову кількість помилок. В таких випадках кажуть про декодування за межами кодової відстані.

Для кодів невеликих розмірів можна легко знайти відстані між всіма кодовими словами і визначити з них значення мінімальної відстані $d_{\min}$ – найважливішого параметра завадостійких кодів. Для великих кодів повний перебір стає дуже складною обчислювальною задачею і способи зменшення трудомісткості цієї задачі належить до однієї з ключових проблем теорії кодування.

Традиційними способами вирішення проблеми оцінки коректувальної здатності кодів є знаходження спектра коду (спектра ваг) і визначення верхніх та нижніх границь. В дев'ятому розділі зроблено детальний аналіз коректувальної здатності циклічних кодів і наведені нові способи її оцінки на основі автоматних моделей цих кодів.

Іноді може виникнути дилема інтерпретації помилок, що виникли в процесі передавання по лінії зв'язку: чи то стались помилки кратністю $\tau_c$, які можна виправити, чи стались помилки кратністю більше за $\tau_c$, які лише виявляються? Зазвичай, приймається перший варіант, оскільки вважається, що помилки меншої кратності більш ймовірні, ніж помилки більшої кратності. Декодер, який притримується такого правила декодування, називається *декодером максимальної правдоподібності*.

Відомі також інші принципи декодування [25]:

– за мінімумом відстані за Хемінгом;

– за максимумом апостеріорної ймовірності;

– за мінімумом узагальненої відстані;

– на основі списків кодових слів.

Іноді декодер не може прийняти рішення про те, що було передано якесь визначене повідомлення через нечітке значення деяких символів

цього повідомлення. Тоді такі символи стираються, і повідомлення в такому вигляді передається отримувачу для подальшої обробки.

Задача побудови коду із заданою коректувальною здатністю полягає у внесенні в нього такої мінімальної надлишковості, яка б забезпечила відстань між будь-якими двома дозволеними кодовими векторами не менше $d_{\min}$. В загальному випадку ця задача поки ще не розв'язана, існують лише верхні та нижні оцінки (границі), про що детальніше буде розглянуто в розділі 9. Тільки для кодів з $d_{\min} = 3$ отримано точне співвідношення між довжиною $n$ коду і кількістю перевірочних розрядів $r$:

$$r \geq \log_2(n+1).$$

В інженерній практиці кількість перевірочних розрядів $r$ коду вибирається із спеціальних наперед обчислених таблиць [42].

## 1.5 Виграш від завадостійкого кодування

Розглянемо оцінки систем зв'язку для основних моделей каналів.

Для ДСК процедура декодування полягає у виборі кодового слова, найближчого до прийнятого слова в сенсі відстані за Хемінгом. Ймовірність $P_{err}$ невиявлення кодового слова з помилкою кратністю $\tau$ для лінійного блокового $(n,k)$-коду визначається співвідношенням [35]

$$P_{err} = \sum_{i=\tau+1}^{n} n_i p^i (1-p)^{n-i}, \qquad (1.4)$$

де $p$ – ймовірність помилки символу в слові, $n_i$ – число кодових слів ваги $i$.

Формула (1.4) дає дуже точну оцінку тільки при знанні спектра коду. При відсутності таких даних можна скористатись верхньою границею:

$$P_{err} \leq \sum_{i=\tau+1}^{n} \binom{n}{i} p^i (1-p)^{n-i}.$$

При $p \to 0.5$ і великих значеннях різниці $(n-k)$ можна використати наближену формулу:

$$P_{err} = (2^k - 1)2^{-n} \approx 2^{-(n-k)}. \qquad (1.5)$$

Як випливає з (1.5), ймовірність невиявленого помилкового слова може бути зроблена як завгодно малою при достатньо великій кількості перевірочних символів в кодових словах. Відзначимо, що такий критерій якості канального кодування є достатньо наближеним і одностороннім.

Для моделі каналу з АБГШ найважливішою характеристикою систем зв'язку є відношення енергії біта $E_b$ в переданому повідомленні до спектральної густини потужності шуму $N_0$: $E_b / N_0$. Вимірюється це відношення у децибелах.

Графік залежності ймовірності $p_b$ появи помилкового біта в кодовому слові від відношення $E_b/N_0$ наведений на рис. 1.9а. Хоча цей графік буде мати деякі відмінності для різних видів модуляції і канального кодування, в ньому можна виділити деякі важливі області. Всі криві будуть знаходитись правіше вертикальної ординати зі значенням –1,6 дБ, яка позначає *межу Шеннона*. Для забезпечення ймовірності помилки $p_b = 10^{-5}$ в системі з ідеальною фазовою модуляцією без кодування необхідно мати 9,6 дБ.

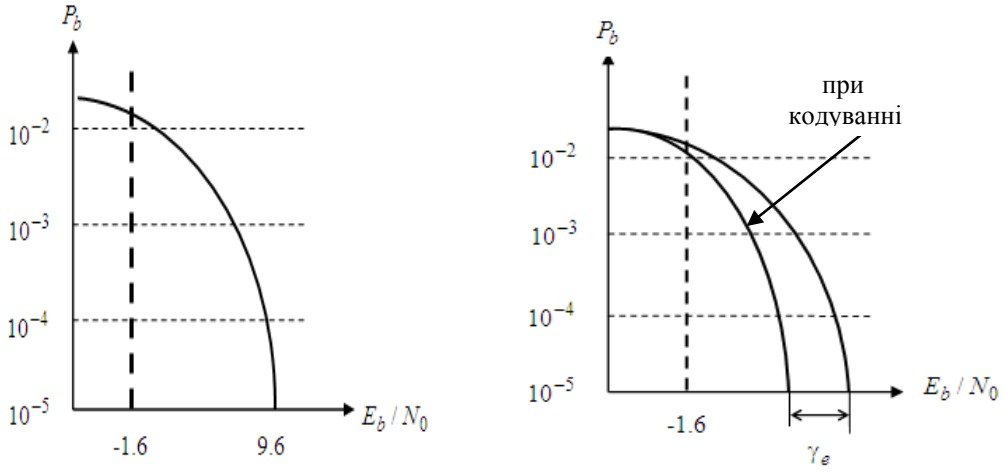
При кодуванні криві на цьому графіку зсовуються вліво, наближаючись до межі Шеннона. Різниця між двома точками на кривій без кодування і кривою з кодуванням для однакового значення ймовірності $p_b$ (наприклад, при $p_b = 10^{-5}$) складає *виграш від кодування* $\gamma_e$ (рис. 1.9б). Такий виграш ще називають *енергетичним* і зазвичай він вказується в децибелах.

Розглянемо аналітичний метод розрахунку виграшу від кодування для лінійного блокового коду, який складається тільки з $k$ інформаційних символів [30]. Обмежимось когерентним детектуванням сигналу при використанні бінарної фазової модуляції (BPSK). В цьому випадку символьна помилка рівнозначна бітовій помилці. Ймовірність $p_b$ бітової помилки в каналі з АБГШ без кодування складає

$$p_b = Q\left(\sqrt{\frac{2E_b}{N_0}}\right). \qquad (1.6)$$

Функція $Q(x)$, яку називають *гаусовим інтегралом помилок*, визначається таким чином:

$$Q(x)=\frac{1}{\sqrt{2\pi}}\int_x^{\infty}\exp\left(-\frac{u^2}{2}\right)du,\ \text{або}\ Q(x)=\frac{1}{\sqrt{2\pi}}\int_x^{\infty}\exp\left(-\frac{x^2}{2}\right)\ \text{для}\ x>3.$$




а) б)

Рисунок 1.9 – Графік залежності $p_b$ від відношення $E_b/N_0$:
а) – без завадостійкого кодування,
б) – при завадостійкому кодуванні

Функцію $Q(x)$ не можна обчислити в аналітичному вигляді, як правило, вона представлена табличними даними.

Ймовірність $P_{not}$ того, що $k$-символьне некодоване слово буде прийнято з помилкою, дорівнює 1 мінус добуток ймовірностей того, що кожний символ (тобто біт при BPSK) буде детектовано правильно:

$$P_{not}=1-(1-p_b)^k.$$

Введемо тепер в такий код $r$ перевірочних символів, які дозволять виправити $\tau$ помилок. Така коректувальна здатність коду викликає збільшення символів до $n$ і відповідне зменшення швидкості коду до $k/n$. Ймовірність $p_{b,c}$ символьної помилки в каналі з АБГШ з кодуванням складає

$$p_{b,c}=Q\left(\sqrt{\frac{2kE_b}{nN_0}}\right). \qquad (1.7)$$

Порівнюючи вирази (1.6) и (1.7) можна бачити, що в результаті внесення надлишковості ймовірність $p_{b,c}$ символьної помилки зменшилась.

Тепер можна визначити ймовірність $P_{cod}$ того, що $n$-символьне кодове слово лінійного блокового $(n, k)$-коду буде прийнято з помилкою:

$$P_{cod} \le \sum_{i=\tau+1}^{n} \binom{n}{i} p_{b,c}^{i} (1 - p_{b,c})^{n-i} . \qquad (1.8)$$

Вираз (1.8) можна також записати у вигляді, яке потребує менше обчислень:

$$P_{cod} \le 1 - \sum_{i=0}^{\tau} \binom{n}{i} p_{b,c}^{i} (1 - p_{b,c})^{n-i} . \qquad (1.9)$$

В (1.8) і (1.9) знак рівності використовується для досконалих лінійних блокових кодів.

Таким чином, завадостійке кодування приводить до збільшення кількості символів, які потрібно обробляти і передавати за той же інтервал часу і з тією ж потужністю передавача. Однак можливість виявлення і виправлення помилок компенсує ці додаткові витрати і дає додатковий виграш, який можна оцінити на рівні ймовірнісних параметрів: величина $P_{cod}$ може бути на декілька порядків меншою, ніж $P_{not}$.

Для порівняльної оцінки різних $(n,k)$-кодів з мінімальною відстанню $d_{\min}$ можна скористатись і точною характеристикою $\gamma_n$, яку називають *номінальним виграшем від кодування* [43]:

$$\gamma_n = \frac{k}{n} d_{\min} .$$

## 1.6 Критерії якості передачі дискретних повідомлень

Якість переданої інформації оцінюється ступенем відповідності прийнятого повідомлення переданому.

Згідно з рекомендаціями Міжнародного союзу електрозв'язку (МСЕ, International Telecommunication Union – ITU) виміряється низка параметрів для оцінки числових характеристик бінарного цифрового каналу.

Найбільш відомим таким параметром є *частота бітових помилок* (bit error rate – BER) – відношення числа прийнятих з помилками біт $N_{err}$ до числу посланих біт $N_{all}$ за визначений період часу:

$$\frac{N_{err}}{N_{all}}.$$

Цей параметр зазвичай вимірюється в режимі тестування при виключеному основному сервісі (Out of Service – OoS). Спеціальний пристрій (BER-тестер) передає по каналу спеціальну псевдовипадкову послідовність (ПВП) максимальної довжини (в наступних розділах будуть розглянуті властивості таких послідовностей), а потім приймає її, порівнюючи початкову ПВП з прийнятою.

Різноманітні типи фізичних каналів зв'язку мають свої мінімальні значення BER, при яких передача даних вважається нормальною (табл. 1.1). Варто відзначити, що реальні канали зв'язку на шляху від джерела повідомлень і до споживача майже завжди складаються з різнотипних сегментів, тому BER не може служити безпосередньо як експлуатаційна норма [44].

Таблиця 1.1 – Значення для основних типів цифрових каналів зв'язку

| **Тип цифрового каналу зв'язку** | **Нормальне значення BER** |
|---|---|
| Радіорелейний зв'язок | $10^{-6}$ |
| Радіозв'язок | $10^{-3}$ |
| Тропосферний зв'язок | $10^{-5}$ |
| Супутниковий зв'язок | $10^{-7}$ |
| Волоконно-оптичні лінії зв'язку | $10^{-10}...10^{-15}$ |

Якщо при тестуванні цифрового каналу зв'язку використовується великий інтервал часу, тоді параметр BER наближається до ймовірності помилкового прийому двійкового символу, тобто до ймовірності помилки на біт $P_{BER}$:

$$P_{BER} = \underbrace{\lim}_{N_{all} \to \infty} \frac{N_{err}}{N_{all}}.$$

Величина $P_{BER}$ статистично коливається навколо значення середньої кількості бітових помилок в переданих даних, а це означає, що вона по суті дорівнює раніше розглянутій теоретичній величині $p_b$. Тому можна отримати графічну інтерпретацію параметра BER.

З цією метою міжнародні стандарти ITU-R S.1062 і S.614 [44] рекомендують використовувати не єдиний обчислений показник BER, а *ймовірнісний показник помилок* BEP (Bit Error Probability), який має вигляд функції від часу вимірювання. За допомогою того ж BER-тестера вимірюють і обчислюють значення BER на чотирьох інтервалах в точках 0,2 %T, 2 %T, 10 %T і 100 %T (де T – стандартний часовий інтервал вимірювання). Далі будується графік BEP(T), який називають маскою BEP, способом кусково-лінійної апроксимації вказаних точок. Якщо фактична маска BEP збігається з еталонною маскою BEP, тоді вважається, що рівень помилок в каналі, що досліджується, задовольняє вимоги стандарту.

Вид експериментального графіка BEP(T) дуже схожий на теоретичний графік залежності ймовірності $p_b$ від відношення $E_b/N_0$ для тих же початкових даних.

Точна побудова як теоретичного, так і експериментального графіків представляє собою складну обчислювальну задачу. Тому часто звертаються до спеціальних математичних пакетів, наприклад, до Matlab [45]. Після задання початкових даних (типу каналу, способу модуляції та інших даних) можна отримати залежність BER від відношення $E_b/N_0$. Саме в такому вигляді ймовірність бітових помилок в цифрових каналах найчастіше і зустрічається на сторінках статей і книг з теорії зв'язку. Оцінка якості цифрових каналів на основі параметра BER була закладена ще в рекомендаціях МСЭ-Т G.821 [46]. Протягом тривалого часу ці рекомендації були міжнародним стандартом при проектуванні і експлуатації цифрових мереж, в 1996 році з'явилась вже четверта її версія.

З часом ставали очевидними недоліки методу вимірювання помилок за бітами. Дійсно, при появі хоча б одного біта з помилкою, помилковими ставали і весь символ, а також кодове слово і блок, в який він входить. Тому нові міжнародні стандарти роблять акцент на використанні блокових, а не бітових помилок. Ще однією причиною такої переорієнтації стали збільшення швидкостей передавання даних і розвиток техніки тестування каналів в процесі їх роботи (In Service Monitoring – ISM). Після великої підготовчої роботи були прийняті рекомендації МСЭ-Т G.826 [47], де були введені нові показники помилок для цифрових ліній передачі. Ці показники базуються на нових поняттях, які йменуються подіями помилок для трактів: EB, ES, SES і BBE.

EB (Errored Block) – *блок з помилками* – блок, в якому один або більше біт помилкові (блок – сукупність послідовних біт, що передаються цифровим трактом).

ES (Errored Second) – *секунда з помилками* – односекундний інтервал часу з одним або більше блоків з помилками (EB).

SES (Severely Errored Second) – *секунда із серйозними помилками* – односекундний інтервал часу, протягом якого сталось більше 30 % блоків з помилками (EB). SES – частина ES.

BBE (Background Block Error) – *блок з фоновою помилкою* – блок з помилками, які не є частиною SES.

На основі приведених понять введені такі параметри помилок:

ESR – *коефіцієнт секунд з помилками* – відношення числа ES до всієї кількості секунд протягом інтервалу вимірювання.

SESR – *коефіцієнт секунд із серйозними помилками* – відношення числа SES до всієї кількості секунд протягом інтервалу вимірювання.

BBER – *коефіцієнт блоків з фоновою помилкою* – відношення числа блоків BBE до всієї кількості блоків протягом інтервалу.

Показники помилок підраховуються, тільки коли тракт знаходиться в стані готовності. В рекомендаціях МСЭ-Т G.826 наведені норми на значення вказаних параметрів в залежності від швидкості передавання в Мбіт/сек.

Бурхливий розвиток волоконно-оптичної технології привів до встановлення більш жорстких норм на показники помилок в рамках

рекомендації МСЭ-Т G.828 [48]. Цей стандарт вперше вводить диференціацію помилок за степенем їх важливості. В останні роки з'явились нові міжнародні стандарти з оцінки якості цифрових каналів (G.8201 [49], M.21xx та інші).

Наостанок відзначимо, що для оцінки якості завадостійких кодів не можна обмежуватись лише тими показниками, які характеризують сам канал зв'язку і процес передавання повідомлень. Дуже важливі також інші параметри: тривалість і складність процедури декодування, вартість апаратури кодування і декодування, швидкість коду. Детальніше це питання буде розглянуто в розділі 9.

## 1.7 Висновки до розділу 1

При передаванні даних в каналах зв'язку виникають численні завади, багато з яких неможливо усунути. Як випливає з теореми Шеннона–Хартлі, завади в каналі не накладають обмежень на точність передачі інформації. Обмеження накладаються тільки на швидкість передавання, за якої можна досягти як завгодно високої достовірності. Рішенням цієї проблеми на практиці може бути введення в повідомлення, що передаються, додаткових контрольних символів, які дозволяють відрізнити правильні повідомлення від помилкових.

Введення надлишковості означає зменшення швидкості передавання, зменшення енергії, яка приходиться на канальний символ, та збільшення числа помилок за межами демодулятора. Однак декодер дозволяє не тільки компенсувати зменшення продуктивності демодулятора, але і давати додатковий виграш. При цьому варто також пам'ятати, що виграш по кодуванню представляє собою лише одну з характеристик завадостійких кодів.

Задачу побудови оптимальних завадостійких кодів не можна розв'язати для всіх випадків відразу. В різноманітних сферах, де зараз використовується кодування, є свої особливості, свої критерії якості. Тому створені різні теоретичні моделі каналів і всі розробки в завадостійкому кодуванні необхідно завжди розглядати з позицій відповідних каналів.

# Розділ 2
# АНАЛІТИЧНІ ПРЕДСТАВЛЕННЯ ЦИКЛІЧНИХ КОДІВ

## 2.1 Математичні основи циклічних кодів

Розглянемо основні алгебраїчні структури, які використовуються в теорії завадостійкого кодування: групи, кільця, поля і векторні простори [50–52].

### 2.1.1 Групи

Множина $G$ називається *групою*, якщо для будь-якої пари елементів $a$ і $b$ із цієї множини визначена деяка операція (позначається $*$) і виконуються 4 аксіоми:

– *замкнутості*: для будь-якої пари елементів $a$ і $b$ з множини $G$ елемент $c = a * b$ також належить цій множині;

– *асоціативності*: для будь-якої пари елементів $a$, $b$ і $c$ з множини $G$ справедлива рівність:

$$a * (b * c) = (a * b) * c;$$

– *існування одиниці*: множина $G$ містить єдиний елемент $e$, який називається одиничним, такий, що

$$a * e = e * a = a$$

для будь-якого елемента $a$ із $G$;

– *існування оберненого елемента*: для будь-якого елемента $a$ з множини $G$ існує єдиний елемент $b$ з $G$, який *називається* оберненим елементу $a$, і такий, що

$$a * b = e \quad \text{і} \quad b * a = e.$$

Група $G$ називається *абелевою*, якщо виконується також аксіома *комутативності*: для будь-яких елементів $a$ і $b$ з $G$ справедлива рівність:

$$a * b = b * a.$$

Абелева група може бути комутативною або мультиплікативною. В комутативній абелевій групі групова операція називається додаванням (позначається +), одиничний елемент називається нулем (позначається 0), а обернений до елемента $a$ елемент записується як $-a$, так, що

$$a + (-a) = (-a) + a = 0.$$

В мультиплікативній абелевій групі групова операція називається множенням (позначається $\bullet$), одиничний елемент називається одиницею (позначається 1), а обернений до елемента $a$ елемент записується як $a^{-1}$, так, що

$$a \bullet a^{-1} = a^{-1} \bullet a = 1.$$

Приклади груп: цілі числа відносно операції додавання, додатні раціональні числа відносно операції множення.

### 2.1.2 Кільця

*Кільцем* $R$ називається комутативна абелева група, в якій визначені операція додавання (позначається +) і операція множення (позначається сусіднім розташуванням) для будь-якої пари елементів і виконуються такі аксіоми:

– *замкнутості*: для будь-якої пари елементів $a$ і $b$ з $R$ елемент $c = ab$ також належить $R$;

– *асоціативності*: для будь-яких елементів $a$ і $b$ з $R$ справедлива рівність:

$$a(bc) = (ab)c;$$

– *дистрибутивності*: для будь-яких елементів $a$, $b$ і $c$ з $R$ справедливі рівності:

$$a(b + c) = ab + bc;$$

$$(b + c)a = ba + ca.$$

Кільце $R$ називається комутативним, якщо виконується також аксіома *комутативності*: для будь-яких елементів $a$ і $b$ з $R$ справедлива рівність

$$ab = ba.$$

Операція додавання в кільці $R$ має одиничний елемент, який називається нулем (позначається 0).

Якщо кільце $R$ має одиничний елемент відносно операції множення, тоді воно називається кільцем з одиницею. Такий одиничний елемент називається одиницею (позначається 1) і для будь-якого елемента з $R$ справедливі рівності

$$1a = a1 = a.$$

Відносно операції додавання кожний елемент кільця $R$ завжди має обернений йому елемент. Обернений елемент відносно операції множення не обов'язково існує.

Приклади кілець: цілі числа відносно операцій додавання і множення, дійсні числа відносно операцій додавання і множення.

Варто згадати ще один приклад кільця, яке в подальшому буде часто використовуватись. Спочатку дамо означення.

Вираз виду

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-2} x^{n-2} + a_{n-1} x^{n-1} \ , \qquad (2.1)$$

де $x$ – невизначена змінна, $a_0, a_1, a_2, \ldots, a_{n-2}, a_{n-1}$ – цілі числа, називається багаточленом $f(x)$ від $x$ степені $n-1$ з цілочисельними коефіцієнтами.

Сумою $h(x) = f(x) + g(x)$ багаточлена (2.1) і багаточлена

$$g(x) = b_0 + b_1 x + b_2 x^2 + \ldots + b_{n-2} x^{n-2} + b_{n-1} x^{n-1} \ , \qquad (2.2)$$

де $b_0, b_1, b_2, \ldots, b_{n-2}, b_{n-1}$ – цілі числа, називається багаточлен

$$h(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \ldots .$$

$$\ldots + (a_{n-2} + b_{n-2})x^{n-2} + (a_{n-1} + b_{n-1})x^{n-1} \ .$$

Добутком $h(x) = f(x)g(x)$ багаточленів (2.1) і (2.2) називається багаточлен

$$h(x) = (a_0 b_0) + (a_1 b_1)x + (a_2 b_2)x^2 + \ldots .$$

$$\ldots + (a_{n-2} b_{n-2})x^{n-2} + (a_{n-1} b_{n-1})x^{n-1} \ .$$

Можна довести, що розглянуті раніше багаточлени з цілочисельними коефіцієнтами утворюють комутативне кільце [51].

### 2.1.3 Поля

*Полем* $F$ називається комутативне кільце, в якому для будь-якого елемента $a$ поля:

– завжди існує обернений йому елемент відносно додавання $-a$ і обернений йому елемент відносно множення $a^{-1}$, такі, що

$$a + (-a) = 0; \quad a a^{-1} = 1;$$

– завжди існує одиничний елемент відносно додавання, який називається нулем (позначається 0), і одиничний елемент відносно множення, який називається одиницею (позначається 1), такі, що

$$a + 0 = 0 + a = a,$$

$$a1 = 1a = a.$$

Можна дати нестрогі означення розглянутих раніше алгебраїчних структур відносно елементарних арифметичних операцій: абелевою групою називається множина, в якій можна додавати і віднімати; кільцем – множина, в якій можна додавати, віднімати і множити; полем – множина, в якій можна додавати, віднімати, множити і ділити.

В полі $F$ під відніманням $(a-b)$ розуміється $a+(-b)$, а під діленням $(a/b)$ розуміється $(b^{-1}a)$. Реалізацією ділення в полі $F$ є також операція скорочення, яка означає, що якщо $ab = ac$, то $b = c$.

Багаточленом над полем $F$ називається вираз

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-2} x^{n-2} + a_{n-1} x^{n-1},$$

коефіцієнти $a_i$ якого належать полю.

В полі $F$, крім раніше розглянутих операцій додавання і множення багаточленів, визначена також операція їх ділення. Для будь-яких багаточленів $f(x)$ і $h(x)$ в полі справедлива рівність

$$h(x) = f(x)s(x) + r(x).$$

В цьому випадку кажуть, що багаточлени $f(x)$ и $h(x)$ порівнянні:

$$h(x) \equiv f(x) \pmod{s(x)}.$$

Якщо $r(x) = 0$, тоді багаточлен $f(x)$ ділить $h(x)$ або є дільником $h(x)$, а багаточлен $h(x)$ є кратним $f(x)$.

Серед різних видів полів нас будуть цікавити поля зі скінченим числом елементів. Поле з $q$ елементами називається скінченим полем, або *полем Галуа* и позначається $GF(q)$.

Найменше поле Галуа – це поле $GF(2)$ з двох елементів, які одночасно є одиничними елементами відносно операції додавання (елемент 0) і операції множення (елемент 1). Операції додавання і множення в полі $GF(2)$ можна знайти, наприклад, в [24].

Для будь-якого простого числа $q$ існує поле Галуа $GF(q)$ і тільки одне поле. Це поле можна узагальнити на поле із $q^m$ елементів, які йменуються *полем розширення* $GF(q^m)$, де $m$ – додатне ціле число.

Відзначимо, що поле $GF(q^m)$ містить всі елементи поля $GF(q)$, тобто поле $GF(q)$ є підполем поля $GF(q^m)$. Наприклад, поле $GF(2^m)$ є полем розширення для поля $GF(2)$ і містить елементи $0, 1, 2, \ldots, (2^m - 1)$.

Якщо $q$ є степенем простого числа $p$ $(q = p^m)$, то елементами поля є всі багаточлени степеня $m-1$ або менше, коефіцієнти якого лежать в простому полі $GF(p)$. Позначимо кожний ненулевий елемент $\alpha_i$ із $GF(2^m)$ багаточленом $\alpha_i(x)$:

$$\alpha = \alpha_i(x) = \alpha_{i,0} + \alpha_{i,1}x + \alpha_{i,2}x^2 + \ldots + \alpha_{i,m-1}x^{m-1}.$$

Правила додавання й множення таких багаточленів отримуються із раніше розглянутих операцій з багаточленами і подальшого приведення результату по модулю до деякого спеціального багаточлена $p(x)$ степеня $m$. Цей багаточлен має важливу властивість – його не можна розкласти на більш прості множники, використовуючи тільки багаточлени із поля $GF(p)$. Такі багаточлени називаються *незвідними*.

Відзначимо, що незвідні багаточлени аналогічні простим числам в арифметиці в тому сенсі, що вони також знаходяться способом простого перебору; таблиці незвідних багаточленів є в багатьох книгах [20, 53].

Розглянемо відмінність між двома різновидами незвідних багаточленів: тими, які належать максимальному покажчику, і тими, що не належить до нього.

Якщо незвідний багаточлен степені $n-k$ входить в розкладання бінома $x^n + 1$ і при цьому $n = 2^{n-k} - 1$, тоді такий багаточлен належить максимальному покажчику і називається також *примітивним*. Цінність примітивних багаточленів полягає в тому, що з їх допомогою можна представити елементи полів розширення і всі операції в полі, тобто фактично побудувати ці поля. Важливе практичне значення ма-

ють примітивні багаточлени поля $GF(2)$, які визначають поля Галуа $GF(2^m)$, що використовуються в кодах БЧХ і Ріда–Соломона.

Якщо ж $n < 2^{n-k} - 1$, то такий незвідний багаточлен не належить максимальному покажчику і є *неприміти́вним*.

### 2.1.4 Векторні простори

Нехай $F$ – деяке поле, а $W$– адитивна абелева група. Назвемо елементи поля $F$ скалярами, а елементи групи $W$– векторами.

Група $W$ називається *векторним простором*, якщо виконуються такі аксіоми:

– *замкнутості*: для будь-якого скаляра $a$ із поля $F$ і будь-якого вектора $w$ із $W$ є визначеним елемент $aw$, який належить $W$;

– *асоціативності*: для будь-яких скалярів $a$ і $b$ із поля $F$ і будь-якого $w$ із $W$ виконується рівність:

$$ab(w) = a(bw);$$

– *дистрибутивності*: для будь-яких скалярів $a$ і $b$ із поля $F$ і будь-яких векторів $u$ і $w$ із $W$ виконуються рівності:

$$(a+b)w = aw + bw;$$

$$a(u+w) = au + aw.$$

Прикладом векторного простору може служити множина багаточленів від $x$ з коефіцієнтами із поля $GF(q)$. Векторами цього простору служать багаточлени.

У векторному просторі $W$ сума виду

$$u = a_1 w_1 + a_2 w_2 + \ldots + a_k w_k,$$

де $a_i$ – скаляри,

називається лінійною комбінацією векторів $w_1, w_2, \ldots, w_k$.

Множина векторів $w_1, w_2, \ldots w_k$ називається лінійно незалежною, якщо є ненульові скаляри $a_1, a_2, \ldots a_k$, такі, що

$$a_1 w_1 + a_2 w_2 + \ldots + a_k w_k = 0.$$

Якщо ж згадана множина векторів не є лінійно залежною, тоді вона називається лінійно незалежною. В цьому випадку ніякий вектор із цієї множини не може бути представлений у вигляді лінійної комбіна-

ції інших векторів. Відзначимо, що нульовий вектор 0 не може належати лінійно незалежній множині.

Множина векторів $w_1, w_2, \ldots w_k$ породжує векторний простір $W$, якщо будь-який вектор із $W$ є лінійною комбінацією векторів цієї множини. Число лінійно незалежних векторів, які породжують простір $W$, називається розмірністю простору $W$. Сукупність $k$ лінійно незалежних векторів, які породжують $k$-мірний простір $W$, називається базисом простору $W$.

Один й той ж векторний простір може породжувати різні множини лінійно незалежних векторів, але всі вони містять однакову кількість векторів, тобто мають однакову розмірність. Будь-яка сукупність, яка містить більше ніж $k$ векторів $k$-вимірного векторного простору, лінійно залежна.

З позицій лінійної алгебри множина всіх $n$-розрядних векторів утворює векторний простір, а його підпростором є множина кодових векторів.

ОЗНАЧЕННЯ 2.1. Лінійний $(n,k)$-код є векторним підпростором, який породжений $2^k$ кодовими векторами у векторному просторі, яке породжено $2^n$ векторами.

Інші властивості векторних просторів достатньо повно представлені в класичних підручниках з кодування [24].

### 2.1.5 Циклічні коди і алгебра багаточленів

Основна властивість циклічних кодів полягає в наступному. Якщо кодове слово

$$Z = (z_0, z_1, \ldots, z_{n-2}, z_{n-1})$$

належить $(n,k)$-коду $\Omega$ довжини $n$ і розмірності $k$, тоді будь-яке слово

$$Z'' = (z_{n-j}, \ldots, z_{n-1}, z_0, z_1, \ldots, z_{n-j-1}),$$

яке отримане циклічним зсувом на $j$ позицій всіх компонент цього коду, також буде належать коду $\Omega$ ($j = 1 \ldots n-2$).

Оскільки циклічний код є різновидом лінійних блокових кодів, тому кодові слова циклічного коду утворюють векторний підпростір відносно простору лінійних блокових кодів.

## ЛІТЕРАТУРА

1. Shannon C. E. A mathematical theory of communication / C. E Shannon. – Bell Syst. Tech. J., 1948. – Vol. 27. – P. 379–423 (Part 1), P. 623–656 (Part 2). [Є переклад : Шеннон К. Работы по теории информации и кибернетике / К. Шеннон – М. : Изд-во иностр. лит., 1963. – 829 с.]

2. Hamming R. S. Error detecting and error correcting codes / R. S. Hamming. – Bell Syst. Tech. J. – 1950. – Vol. 29. – P. 147–160.

3. Goley M. J. T. Notes on digital codes / M. J. T. Goley // Proc. IRE, 1949. – Vol. 37. – P. 657.

4. Котельников В. А. Теория потенциальной помехоустойчивости / В. А. Котельников. – М. : Госэнергоиздат, 1956. – 152 с.

5. Харкевич А. А. Очерки общей теории связи / А. А. Харкевич. – М. : Гостехиздат, 1955. – 270 с.

6. Applications of Error-Control Coding / [D. J. Costello, Jr., J. Hagenauer, H. Imai, S. B. Wicker]. // IEEE Trans. Inform. Theory. – 1998. – Vol. 44. – No. 6, – P. 2531–2560.

7. Кузьмин И. В. Основы теории информации и кодирования / И. В. Кузьмин, В. А. Кедрус. – 2-е изд. – К. : Вища школа, 1986. – 238 с.

8. Банкет В. Л. Цифровые методы в цифровой связи / В. Л. Банкет, В. М. Дорофеев. – М. : Радио и связь, 1988. – 240 с.

9. Белецкий А. Я. Преобразования Грея. Т. 1: Основы теории / А. Я. Белецкий, А. А. Белецкий, Е. А. Белецкий. – К. : НАУ, 2007. – 412 с.

10. Борисенко А. А. Биномиальное кодирование : монография / А. А. Борисенко, И. А. Кулик ; Сум. гос. ун-т. – Сумы : СумГУ, 2010. – 205 с.

11. Жураковський Ю. П. Теорія інформації та кодування: підручник / Ю. П. Жураковський, В. П. Полторак. – К. : Вища школа, 2001. – 255 с.

12. Лужецький В. А. Високонадійні математичні Фібоначчі-процесори: монографія / В. А. Лужецький. – Вінниця : УНІВЕРСУМ–Вінниця, 2000 р. – 248 с.

13. Стахов А. П. Коды золотой пропорции / А. П. Стахов. – М. : Радио и связь, 1984. – 152 с.

14. Prange E. Cyclic error-correcting codes in two symbols / E. Prange. – AFCRC-TN-57-103, Air Force Cambridge Research Center. Cambridge, Sept. 1957.

15. Bose R. C. On a class of error-correcting binary group codes / R. C. Bose, D. K. Ray-Chaudhuri. // Inf. Contr. – 1960. – Vol. 3. – P. 68–79.

16. Hocquenghem A. Codes correcteurs d'erreurs / A. Hocquenghem. – Chiffres, 1959. – T. 2. – P. 147–156

17. Fire P. A class of multiple-error correcting binary codes for nonindependent errors / P. Fire. – Sylvania Report RSL E-2, Sylvania Reconnaissance Systems Lab., Mountain View, Calif., 1959.

18. Reed I. S. Polynomial codes over certain finite fields / I. S. Reed, G. Solomon. – J. Soc. Indust. Appl. Math. – 1960. – Vol. 8. – P. 300–304.

19. ISO/IEC 18004 : 2006 Information technology – Automatic identification and data capture techniques – QR Code 2005 bar code symbology specification.

20. Питерсон У. Коды, исправляющие ошибки / У. Питерсон ; пер. с англ. – М. : Мир, 1964. – 340 с.

21. Берлекэмп Э. Алгебраическая теория кодирования / Э. Берлекэмп ; пер. с англ. – М. : Мир, 1971. – 477 с.

22. Мак-Вильямс Ф. Дж. Теория кодов, исправляющих ошибки / Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн ; пер. с англ. – М. : Связь, 1979. – 744 с.

23. Касами Т. Теория кодирования / Т. Касами, Н. Токура, Ё. Ивадари, Я. Инагаки ; пер. с япон. – М. : Мир, 1978. – 576 с.

24. Блейхут Р. Теория и практика кодов, контролирующих ошибки / Р. Блейхут ; пер. с англ. – М. : Мир, 1986. – 576 с.

25. Кларк Дж., мл. Кодирование с исправлением ошибок в системах цифровой связи / Дж. Кларк мл., Дж. Кейн; пер. с англ. – М. : Радио и связь, 1987. – 392 с.

26. Галлагер Р. Теория информации и надежная связь / Р. Галлагер; пер. с англ. – М. : Сов. радио, 1974. – 719 с.

27. Кловский Д. Д. Передача дискретных сообщений по радиоканалам / Д. Д. Кловский – М. : Связь, 1969. – 375 с.

28. Финк Л. М. Теория передачи дискретных сообщений / Л. М. Финк. Изд. 2-е – М. : Советское радио, 1970. – 728 с.

29. Самойленко С. И. Помехоустойчивое кодирование / С. И. Самойленко. – М. : Наука, 1966. – 310 с.

30. Скляр Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр. ; Изд. 2-е, испр. ; Пер. с англ. – М. : Издательский дом «Вильямс», 2004. – 1104 с.

31. Колесник В. Д. Декодирование циклических кодов / В. Д. Колесник, Е. Т. Мирончиков. – М. : Связь, 1968. – 252 с.

32. Колесник В. Д. Кодирование при передаче и хранении информации (Алгебраическая теория блоковых кодов) / В. Д. Колесник. – М. : Высш. школа, 2009. – 550 с.

33. Слепов Н. Н. Современные технологии цифровых оптоволоконных сетей связи / Н. Н. Слепов. – Изд. 2-е, испр. – М. : Радио и связь, 2003. – 468 с.

34. Слепов Н. Н. Волоконные системы дальней связи. Перспективы развития / Н. Н. Слепов. // ЭЛЕКТРОНИКА: Наука, Технология, Бизнес. – 2005. – № 6 – С. 70–75.

35. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение / Р. Морелос-Сарагоса ; пер. с англ. – М. : Техносфера, 2006. – 320 с.

36. Rao T. R. N. Error-Control Coding for Computer Systems / T. R. N. Rao, E. Fujiware. – Prentice Hall, Englewood Cliffs, N.Y., 1989.

37. Varsamou M. A new data allocation method for parallel probe-based storage devices / M. Varsamou, T. Antonakopoulos // IEEE Transactions on Magnetics. – 2008. – Vol. 44. – No. 4. – P. 547–554.

38. Прокис Дж. Цифровая связь / Дж. Прокис; пер. с англ. – М. : Радио и связь, 2000. – 800 с.

39. Блох Э. Л. Модели источники ошибок в каналах передачи цифровой информации / Э. Л. Блох, О. В. Попов, В. Я. Турин. – М. : Связь, 1971. – 312 с.

40. Богданов В. Н. Защита от ошибок в сетях АТМ / В. Н. Богданов, П. С. Вихлянцев, М. В. Симонов. // ИНФОРМОСТ. – 2002. – № 3 – С. 20–24.

41. Мелентьев О. Г. Теоретические аспекты передачи данных по каналам с группирующимися ошибками / О. Г. Мелентьев. – М. : Горячая линия-Телеком, 2007. – 232 с.

42. Березюк Н. Т. Кодирование информации (двоичные коды) / [Н. Т. Березюк, А. Г. Андрущенко, С. С. Мощицкий и др. ]. – Харьков: Вища щкола, 1978. – 252 с.

43. G. D. Forney, Jr. Modulation and Coding for Linear Gaussian Channels / G. D. Forney, Jr., G. Ungerboeck. // IEEE Trans. Inform. Theory. – October, 1998. – Vol. 44. – No. 6. – P. 2384–2434.

44. Слепов Н. Н. Оценка показателей ошибок цифровых линий передачи / Н. Н. Слепов // ЭЛЕКТРОНИКА: Наука, Технология, Бизнес. – 2002. – № 5 – С. 22–28.

45. Васильев А. Н. Matlab. Самоучитель. Практический подход / А. Н. Васильев. – СПб. : Наука и техника, 2012. – 448 с.

46. Рекомендации МСЭ-Т G.821 (12/02). Показатели ошибок международного цифрового соединения, работающего на скорости передачи ниже первичной и образующего часть сети с интеграцией услуг.

47. Рекомендации МСЭ-Т G.826 (12/02). Параметры показателей ошибок и нормы между оконечными пунктами для международных цифровых трактов и соединений с постоянной скоростью передач.

48. Рекомендации МСЭ-Т G.828 (03/00). Параметры показателей ошибок и нормы для международных синхронных цифровых трактов с постоянной скоростью передач.

49. Рекомендации МСЭ-Т G.8201 (09/03). Параметры показателей ошибок и нормы между оконечными пунктами для международных трактов многих операторов в оптической транспортной сети многих операторов.

50. Лидл Р. Конечные поля. / Р. Лидл, Г. Нидеррайтер; в 2 т., Т. 1 – М. : Мир, 1988. – 430 с.

51. Фрид Э. Элементарное введение в абстрактную алгебру / Э. Фрид ; пер. с венг. – М. : Мир, 1979. – 260 с.

52. Курош А. Г. Курс высшей алгебры / А. Г. Курош. ; Изд. 9-е. – М. : Наука, 1968. – 431 с.

53. Гилл А. Линейные последовательностные машины / А. Гилл ; пер. с англ. – М. : Наука, 1974. – 288 с.

54. Айчифер Э. С. Цифровая обработка сигналов: практический подход / Э. С. Айчифер, Б. У. Джервис. ; Изд. 2-е, испр. : пер. с англ. – М. : Издательский дом «Вильямс», 1992. – 992 с.

55. Кун С. Матричные процессоры на СБИС / С. Кун ; пер. с англ. – М. : Мир, 1991. – 672 с.

56. Friedland B. Linear Modular Sequential Circuits / B. Friedland // IRE Trans. – 1959. – Vol. 6. – P. 61–68.

57. Huffman D. A. The Syntsesis of Linear Sequential Coding Networks / D. A. Huffman. // Information Theory, Acad. Press Inc., N. Y., – 1956. – P. 77–95.

58. Huffman D. A. A Linear Circuit Viewpoint on Error-Correcting Codes / D. A. Huffman. // IRE Trans. – 1956. – Vol. IT-2. – P. 20–28.

59. Глушков В. М. Синтез цифровых автоматов / В. М. Глушков. – М. : Наука, 1966. – 476 с.

60. Кузнецов О. П. Дискретная математика для инженера / О. П. Кузнецов, Г. М. Адельсон-Вельский. ; Изд. 2-е. – М. : Энергоатомиздат, 1988. – 480 с.

61. Фараджев Р. Г. Линейные последовательностные машины / Р. Г. Фараджев. – М. : Сов. радио, 1975. – 288 с.

62. Элспас Б. Теория автономных линейных последовательностных сетей / Б. Элспас // Киб. сборник.– М. : ИЛ., 1963. – Вып. 7. – С. 90–128.

63. Vardy A. Trellis Structure of Codes / A. Vardy, V. Pless, W. C. Huffman. Handbook of Coding Theory. – Eds, Amsterdam, The Netherlands : Elsevier, 1998.

64. Schlegel C. Trellis Coding / C. Schlegel. – New York : IEEE Press, 1997. – P. 274.

65. Tanner R. M. A Recursive Approach to Low Complexity Codes / R. M. Tanner // IEEE Trans. Inform. Theory. – Sep. 1981. – Vol. 27. – P. 533–547.

66. Gallager R. G. Low-Density Parity-Check Codes / R. G. Gallager. – Cambridge MA : MIT Press, 1963. – P. 90.

67. Wiberg N. Codes and Iterative Decoding on General Graphs / N. Wiberg, H. A. Loeliger, R. Kotter // Eur. Trans.Telecomm. – Sep./Oc. 1995. – Vol. 6. – P. 513–525.

68. Forney G. D. Codes on the graphs: Normal Realizations / G. D. Forney // IEEE Trans. Inform. Theory. – Fab. 2001. – Vol. 47. – P. 520–548.

69. Соловьева Ф. И. Введение в теорию кодирования: Учебное пособие / Ф. И. Соловьева. – Новосибирск : Новосибирский гос. ун-т, 2005. – 130 с.

70. Семеренко В.П. Разработка универсального кодера-декодера циклических кодов / В. П. Семеренко // Электронное моделирование. – 1995. – № 4. – С. 26–31.

71. Meggitt J. E. Error-correcting codes and their implementation / J. E. Meggitt // IRE Trans. Inf. Theory. – 1961. – Vol. IT-7. – P. 232–244.

72. Касами Т. Теория кодирования / Т. Кассами, Н. Токура, Е. Ивадари, Я. Инагаки ; пер. с япон. – М. : Мир, 1978. – 576 с.

73. Peterson W. W. Encoding and error-correction procedures for the Bose-Chaudhuri codes. / W. W Peterson // IEEE Trans. Inform. Theory. – 1960. – Vol. IT-6. – P. 459–470.

74. Gorenstein D. C. A class of error-correcting codes in $p^m$ symbols. / D. C. Gorenstein, N. Zierler // J. Soc. Indust. Appl. Math. – 1961. – Vol. 9. – P. 207–214.

75. Massey J. L. Shift-register syntesis and BCH codes / J. L. Massey // IEEE Trans. Inform. Theory. – 1969. – Vol. IT-15. – P. 122–127.

76. Chien R. T. Cyclic decoding procedures for Bose-Chaudhuri-Hocquenghem codes. / R. T. Chien // IEEE Trans. Inform. Theory. – 1964. – Vol. 10. – P. 357–363.

77. Forney G. D., Jr. On decoding BCH codes. / G. D. Forney, Jr. // IEEE Trans. Inform. Theory. – 1965. – Vol. IT-11. – P. 549–557.

78. Coding Theory and Cryptography. The Essentials / [D. R. Hankerson, D. G. Hoffman, D. A. Leonard, C. C. Lindner, and others] Wall. Second Edition, Revised and Expanded. – New York : CRC Press. – 2000. – 350 p.

79. Золотарёв В. В. Теория и алгоритмы многопорогового декодирования / В. В. Золотарёв. – М. : Горячая линия-Телеком, 2006. – 270 с.

80. Omura J. K. A Probabilistic Decoding Algorithm for Binary Group Codes / J. K. Omura // Stanford Research Institute. Menlo Park, California, March 1969.

81. Семеренко В. П. Высокопроизводительные алгоритмы для исправления независимых ошибок в циклических кодах / В. П. Семеренко // Системи обробки інформації: зб. наук. пр. – Харків: ХУПС, 2010. – Вип. 3(84), – С. 80–89.

82. Prange E. The use of information sets in decoding cyclic codes / E. Prange // IRE Trans. Inf. Theory. – 1962. – Vol. IT-8.– P. 5–9.

83. Когновицкий О. С. Двойственный базис и его применение в телекоммуникациях / О. С. Когновицкий. – СПб. : Линк, 2009. – 411 с.

84. Конопелько В. К. Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов. Изд. 3/ В. К. Конопелько, В. А. Липницкий. – М. : Едиториал УРСС, 2012. – 176 с.

85. Миллер Р. Последовательные и параллельные алгоритмы: Общий подход / Р. Миллер, Л. Боксер ; пер. с англ. – М. : БИНОМ. Лаборатория знаний, 2006. – 406 с.

86. Коричнев Л. П. Статистический контроль каналов связи / Л. П. Коричнев, В. Д. Королев. – М. : Радио и связь, 1989. – 240 с.

87. Abramson N. M. A class of Systematic Codes for Non-Independent Errors / N. M. Abramson // IRE Trans. Inf. Theory. – 1959. – Vol. IT-5. – No. 12. – P. 150–157.

88. Столлингс В. Компьютерные системы передачи данных / В. Столингс. ; Изд. 6-е; пер. с англ. – М., Издательский дом «Вильямс», 2002. – 928 с.

89. Вернер М. Основы кодирования. Учебник для вузов / М. Вернер ; пер. с англ. – М. : Техносфера, 2004. – 288 с.

90. Koopman P. Cyclic Redundancy Code (CRC) Polynomial Selection For Embedded Networks / P. Koopman, T. Chakravarty // The International Conference on Dependable Systems and Networks (DSN-2004). – June 2002. – P. 1–10.

91. Горяшко А. П. Синтез диагностируемых схем вычислительных устройств / А. П. Горяшко. – М. : Наука, 1987. – 288 с.

92. Reiger S. H. Codes for the correction of «clustered» errors / S. H. Reiger // IRE Trans. Inf. Theory, – Vol. 6. – Mar. 1960. – P. 16–21.

93. Семеренко В. П. Декодирование пакетов ошибок в цикличес-ких кодах / В. П. Семеренко // Математические машины и системы. – 1999. №1. – С. 30–48.

94. Semerenko V. P. Burst-Error Correction for Cyclic Codes / V. P. Semerenko // Proceeding of International IEEE Conference EUROCON2009, S. Petersburg, Russia. – P. 1646–1651.

95. Закревский А. Д. Логические уравнения / А. Д. Закревский ; Изд. 2-е. – М. : УРСС, 2003. – 95 с.

96. Fossorier M. Universal burst error correction / M. Fossorier // Proc. IEEE Int. Symp. Information Theory, Seatle, WA, Jul. 2006. – P. 1969–1973.

97. Berlecamp E. On the inherent intractability of certain coding problems / E. Berlecamp, R. J. McEliece, H. C. van Tilborg // IEEE Trans. Inform. Theory. – May, 1978. – Vol. 24. – No. 5. – P. 384–386.

98. Vardy A. The Intractability of Computing the Minimum Distance of a Code / A. Vardy // IEEE Trans. Inform. Theory. – November, 1997. – Vol. 43. – No. 1. – P. 1757–1766.

99. Dumer I. Hardness of Approximating the Minimum Distance of a Linear Code / I. Dumer, D. Micciancio, M. Sudan // IEEE Trans. Inform. Theory. – January, 2003. – Vol. 49. – No. 1. – P. 22–37.

100. Hartmann C. Generalizations of the BCH Bound / C. Hartmann, K. Tzeng // Information and Control. – 1972. – Vol. 20. – No. 5. – P. 489–498.

101. Roos C. A Generalization of the BCH Bound for Cyclic Codes, Including the Hartmann-Tzeng Bound Journal of Combinatorial Theory / C. Roos // Journal of Combinatorial Theory, Series A. – 1982. – Vol. 33. – No. 2. – P. 229–232.

102. Boston N. Bounding Minimum Distances of Cyclic Codes Using Algebraic Geometry / N. Boston // Electronic Notes in Discrete Mathematics. – 2001. –Vol. 6. – No. 5. – P. 384–386.

103. van Lint, J. H. On The Minimum Distance of Cyclic Codes / J. H. van Lint, R. M. Wilson // IEEE Transactions on Information Theory. – 1986. – Vol. 32. – No. 1. – P. 23–40.

104. Семеренко В. П. Оценка корректирующей способности ци-клических кодов на основе автоматных моделей / В. П. Семеренко //

Східно-європейський журнал передових технологій. – 2015. – № 2. – С. 16–24.

105. Конопелько В. К. Анализ возможности применения БЧХ кодов для коррекции зависимых ошибок / В. К. Конопелько, О. Г. Смолякова, А. В. Шкиленок // Доклады БГУИР. – 2007. – № 5. – С. 17–22.

106. Теория электрической связи. Учебное пособие / [К. К. Васильев, В. А. Глушков, А. В. Дермидонтов, А. Г. Нестеренко]. – Ульяновск. : УлГТУ, 2008. – 452 с.

107. Lin S. Error-Control Coding: Fundamentals and Applications / S. Lin, D. J. Costello ; 2nd. ed. – Upper Saddle River, NJ : Prentice-Hall, 2004.

108. Форни Д. Каскадные коды / Д. Форни ; пер. с англ. – М. : Мир, 1970. – 207 с.

109. Шахнович И. DVB-T2 – новый стандарт цифрового телевизионного вещания/ И. Шахнович // Электроника: НТБ. – 2009. – № 6. – С. 30–35.

110. Блох Э. Л. Обобщенные каскадные коды / Э. Л. Блох, В. В. Зяблов. – М. : Связь, 1976. – 240 с.

111. Guruswami V. Maximum-likelihood decoding of Reed-Solomon codes is NP-hard ECCC / V. Guruswami, A. Vardy. – Rep. TR 04-40. – Apr. 2004.

112. Jiang Gross J. Algebraic soft-decision decoding of Reed-Solomon codes using bit-level soft information / J. Jiang Gross, K. R. Narayanan // IEEE Trans. Inform. Theory. – Sep. 2008. – Vol. 54. – No. 9. – P. 3907–3928.

113. Welch L. R. Error Correction for Algebraic Block Codes / L. R. Welch, E. R. Berlecamp, U.S.A. – No. 4 633 470. Dec., 30, 1986.

114. Sudan M. Decoding of Reed-Solomon beyond the error-correction bound / M. Sudan, // J. Complexity. – Sep. 1997. – Vol. 13. – P. 180–193.

115. Guruswami V. Improved decoding of Reed-Solomon and algebraic-geometry codes / V. Guruswami, M. Sudan // IEEE Trans. Inform. Theory. – Sep. 1999 Vol. 45. – No. 6. – P. 1757–1767.

116. Wu Y. New list decoding algorithms for Reed-Solomon and BCH Codes / Y. Wu // IEEE Trans. Inform. Theory. – Aug. 2008. – Vol. 54. – No.8. – P. 3611–3630.

117. Семеренко В. П. Декодирование кодов Рида–Соломона на основе графовой и автоматной моделей / В. П. Семеренко // Электронное моделирование. – 2011. – № 1. – С. 57–72.

118. Chen G. A Burst-error Algorithm for Reed-Solomon Codes / G. Chen, P. Owsley // IEEE Trans. Inform. Theory. – Nov. 1992. – Vol. 38. – No. 6. – P.1807–1812.

119. Metzner J. J. On Correcting Bursts (and Random Errors) in Vector Symbol $(n, k)$ Cyclic Codes / J. J. Metzner // IEEE Trans. Inform. Theory. – April, 2008. – Vol. 54. – No. 4. – P. 1795–1807.

120. Semerenko V. P. On Correcting of the Full Burst Errors for Reed–Solomon Codes / V. P. Semerenko // STATISTICAL METHODS OF SIGNAL AND DATA PROCESSING (SMSDP-2010) : Proceedings. Kiev, Ukraine, October 13–14. – 2010. – P. 169–171.

121. Семеренко В. П. Параллельное декодирование укороченных циклических кодов / В. П. Семеренко // Оптико-электронные информационно-энергетические технологии. – 2012. – № 1. – С. 30–41.

122. Казаков М. А. Разработка логики визуализаторов алгоритмов на основе конечных автоматов: / М. А. Казаков, Г. А. Корнеев, А. А. Шалыто. Телекоммуникации и информатизация образования. – 2003. – № 6. – С. 27–58.

123. Семеренко В. П. Паралельні алгоритми завадостійкого кодування / В. П. Семеренко // European Conference on Innovations in Technical and Natural Sciences. Proceedings of the 1st International scientific conference (February 17, 2014). «East West» Association for Advanced Studies and Higher Education GmbH. Vienna. 2014. – P. 82–88.

124. Хокинг С. Краткая история времени: От Большого взрыва до черных дыр / С. Хокинг ; пер. с англ. – СПб. : Амфора, 2008. – 231 с.

125. Пригожин И. Время, хаос, квант / И. Пригожин, И. Стенгерс. – М. : Издат. группа Прогресс, 1994. – 272 с.

126. Логика. Автоматы. Алгоритмы / [М. А. Айзерман, Л. А. Гусев, Л. И. Розоноэр, И. М. Смирнова, А. А. Таль]. – М. : Физматгиз, 1963. – 556 с.

127. Семеренко В. П. Темпоральні моделі паралельних обчислень / В. П. Семеренко // Austrian Journal of Technical and Natural Sciences. – January-February, 2014. – № 1. – P. 13–25.

128. Габидулин Э. М. Кодирование в радиоэлектронике / Э. М. Габидулин, В. Б. Афанасьев. – М. : Радио и связь, 1986. – 176 с.

129. Viswanath P. Opportunistic Beam Forming Using Dumb Antennas / P. Viswanath, N. David C. Tse, R. Laroia // IEEE Trans. Inform. Theory. – Juny 2002. – Vol. 52. – P. 1277–1294.

130. Конопелько В. К. Надежное хранение информации в полупроводниковых запоминающих устройствах: / В. К. Конопелько, В. В. Лосев. – М. : Радио и связь, 1986. – 240 с.

131. Hsiao M. Y. Single-Channel Error Correction in an f-Channel System / M. Y. Hsiao // IEEE Trans. On Computers. – Oct. 1968. – Vol. 17. – P. 935–943.

132. Ahlswede R. Multi–way communication channels / R. Ahlswede // 2nd Int. Symp. Inform. Theory, 23–52, Publishing House of the Hungarian Academy of Sciences. Tsahkadzor, Armenian SSR, 1973.

133. Fujiwara E. Parallel Decoding for Burst Error Control Codes / E. Fujiwara, K. Namba, M. Kitakami // Electronics and Comm. in Japan. – Jan. 2004. – Vol. 87. – No. 1. – P. 38–48.

134. Семеренко В. П. Паралельні циклічні коди / В. П. Семеренко // Вісник ВПІ. – 2014. – № 6. – С. 65–72.

135. Патент на корисну модель «Пристрій для виправлення помилок в циклічних (n, k)-кодах» / Семеренко В. П. – № 93798; заявл. 29.05.2014 ; опубл. 10.10. 2014, Бюл. № 19.

136. McEliece R. J. A Public-Key Criptosystem Based on Algebraic Theory / R. J. McEliece // DGN Progres Report 42–44, Jet Propulsi on Lab. Pasadena, CA. January – February, 1978. – P. 114–116.

137. Niederreiter H. Knapsack-Type Cryptosystems and Algebraic Coding Theory / H. Niederreiter // Probl. Control and Inform. Theory. – 1986. – Vol. 15. – P. 19–34.

138. Конопелько В. К. Защита информации кодовыми криптосистемами на основе теории норм синдромов и свойств циклотомической перестановки чисел / В. К. Конопелько, О. Г. Смолякова. // Технические средства защиты информации. Материалы докл. 6-й Белорусско-российской научно-техн. конф. (Минск 19–23 мая 2008 г.). – Минск. – С. 65.

139. Сидельников В. М. Открытое шифрование на основе двоичных кодов Рида–Маллера / В. М. Сидельников // Дискретная математика. – М., 1994. – Том 6, Вып. 3. – С. 3–20.

140. Стасев Ю. В. Несимметричные теоретико-кодовые схемы с использованием алгеброгеометрических кодов / Ю. В. Стасев, А. А. Кузнецов // Кибернетика и системный анализ. – 2005. – № 3. – С. 47–57.

141. Осмоловский С. А. Стохастические методы защиты информации / С. А. Осмоловский. – М. : Радио и связь, 2003. – 320 с.

*Наукове видання*

**Семеренко Василь Петрович**

# ТЕОРІЯ ЦИКЛІЧНИХ КОДІВ НА ОСНОВІ АВТОМАТНИХ МОДЕЛЕЙ

Монографія

Редактор Н. Мазур

Оригінал-макет підготовлено В. Семеренко

Підписано до друку 9.07.2015 р.
Формат 29,7×42¼. Папір офсетний.
Гарнітура Times New Roman.
Друк різографічний. Ум. др. арк. 25,64
Наклад 300 (1-й запуск 1–75) пр. Зам № В2015-24

Вінницький національний технічний університет,
КІВЦ ВНТУ,
21021, м. Вінниця, Хмельницьке шосе, 95,
ВНТУ, ГНК, к. 114.
Тел. (0432) 59-85-32.
Свідоцтво суб'єкта видавничої справи
серія ДК № 3516 від 01.07.2009 р.

Віддруковано ФОП Барановська Т. П.
21021, м. Вінниця, вул. Порика, 7.
Свідоцтво суб'єкта видавничої справи
серія ДК № 4377 від 31.07.2012 р.