УДК 004.056:004.627
УКПП
№ державної реєстрації 0116U005238
Інв. №

Міністерство освіти і науки України
Сумський державний університет (СумДУ)
40007, м. Суми, вул. Римського-Корсакова, 2; тел. 33-02-25

ЗАТВЕРДЖУЮ
Проректор з наукової роботи
д-р фіз.-мат. наук, професор

_____ А. М. Чорноус

ЗВІТ
ПРО НАУКОВО-ДОСЛІДНУ РОБОТУ

ЗАСОБИ КОДУВАННЯ І ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

(остаточний)

Керівник НДР
д.т.н, професор О.А. Борисенко

2021

Рукопис закінчений 15 червня 2021 року

Результати роботи розглянуто науковою радою СумДУ, протокол від __.__.2021 р. № __

СПИСОК АВТОРІВ

Керівник НДР		
професор д.т.н., професор	_____ ___.06.2021	О.А. Борисеко (вступ, розділ 1,2, висновки)
Виконавці:		
доцент к.т.н., доцент	_____ ___.06.2021	І.А. Кулик (розділ 3,4)
доцент к.т.н., доцент	_____ ___.06.2021	О.В. Бережна (розділ 1,2)
доцент к.т.н., доцент	_____ ___.06.2021	А.І. Новгородцев (розділ 3,4)
доцент к.т.н., доцент	_____ ___.06.2021	О.М. Кобяков (розділ 3,4)
ст.викладач к.т.н.	_____ ___.06.2021	О.Є. Горячев (розділ _)
ст.викладач	_____ ___.06.2021	Т.О. Протасова (розділ _)
аспірант	_____ ___.06.2021	В.В. Сердюк (розділ _)
аспірант	_____ ___.06.2021	М.С. Шевченко (розділ _)
аспірант	_____ ___.06.2021	А.О. Горішняк (розділ _)

РЕФЕРАТ

Звіт про НДР: _60_ с., _4_ табл., _6_ рис., _35_ джерел.

БІНОМІАЛЬНІ СИСТЕМИ ЧИСЛЕННЯ, БІНОМІНАЛЬНІ ЧИСЛА, ЗАХИСТ ІНФОРМАЦІЇ, КВАЗІРІВНОВАЖНИЙ КОД, РІВНОВАЖНІ КОМБІНАЦІЇ, СТИСНЕННЯ ДАНИХ

В роботі розглянуті питання завадостійкого кодування із захистом інформації від несанкціонованого доступу для числових даних. Використовуються як звичайні двійкові коди, так і завадостійкі коди. В якості останніх використовуються біноміальні і отримані на їх основі рівноважні коди. Крім того використовувались квазірівноважні біноміальні коди, які дозволяли стискати інформацію. Це дозволило значно підняти завадостійкість інформації, що передається. Вибір цих кодів викликаний ще тим, що вони крім завадостійкості мають просту і гнучку структуру і є нероздільними. Це дозволяє поряд з захистом від помилок використовувати їх ще і для захисту від небажаного до них доступу. Особливо це важливо при передачі даних телекомунікаційними системами від датчиків тепла, води, електроенергії і тому подібних задач. В випадку, що досліджувався, в якості даних використовувались цифри. Вони особливо чутливі до завад, але з другого боку у них досить важко виявити розподіл ймовірності. Це дозволяє захищати їх від доступу досить простими методами, що і було зроблено в даній роботі.

Була запропонована телекомунікаційна система яка успішно вирішила вказані задачі. Вона мала буферну пам'ять, пристрій відображення, пристрої одночасного кодування від завад і несанкціонованого доступу. Сумісно вони створювали системи як передачі, так і прийому інформації. Важливо також було оцінити ступінь завадостійкості кодів, що використовувались в цій системі. Для цього було проведено комп’ютерне моделювання і отримані позитивні оцінки ефективності розробленої телекомунікаційної системи.

Поряд із захистом інформації важливо також підвищувати швидкість передачі інформації при її передачі, що потребує її стиснення. Ця задача вирішувалась на основі використання біноміальних чисел. Для цього підраховувалась кількість одиниць в двійковій кодовій комбінації і цим самим вони перетворювались в біноміальні комбінації. Далі вони стискувались відповідно до форму біноміальних систем числення.

ЗМІСТ

стор.

ВСТУП

На сьогодні, як ніколи раніше, виросла роль інформаційних систем, які зберігають, передають і обробляють інформацію. В цьому процесі важливу роль мають способи і системи кодування інформації. Від них залежить швидкість передачі і обробки інформації, а також її надійність. Тому кодування інформації було і залишається основним фактором, який підвищує ефективність інформаційних систем і особливо систем телекомунікації. Відповідно існує багато наукових робіт на цю тему.

В даній праці кодуванню теж приділяється особлива увага. Треба було розробити такі коди, які б одночасно захищали інформацію від завад і несанкціонованого доступу і в той же час могли відображатися на пристроях відображення, забезпечуючи тим самим ефективний контроль роботи системи оператором. В якості таких кодів в даній праці були взяті рівноважні, квазірівноважні, біноміальні і квазібіноміальні коди. В сукупності вони забезпечівували найбільш ефективну роботу інформаційної системи і особливо телекомунікаційної.

Важливою задачею при цьому є задача оцінки ефективності вибрангих кодів. Для цього потрібно розробити відповідний математичний апарат і програми, які його реалізують. Тут важливою задачею буде ймовірність помилок, що знаходяться і помилок, що не знаходяться. Перші зявляються пр. появі заборонених кодових комбінацій, а другі дозволених. Відповідна робота по розробленому математичному апарату оцінок кодів буде надана нижче в пояснювальній записці до даної роботи.

1 СИСТЕМА ПЕРЕДАЧІ ТА ВІДОБРАЖЕННЯ ІНФОРМАЦІЇ ІЗ ЗАХИСТОМ ЧИСЛОВИХ ДАНИХ

1.1 Актуальність дослідження

Дослідження направлено на вирішення практичної задачі, побудови цифрової системи передачі та відображення інформації із захистом числових даних від несанкціонованого доступу та помилок. Практично немає жодного виробничого процесу, де б не застосовувалися системи передачі інформації, які поряд з загальною інформацією, не передавали б ще і інформацію в вигляді числових даних. Вони часто подаються багато розрядними десятковими числами, цифри яких мають двійково-десяткову форму і тому кодуються 4 бітами. Числа після передачі, як правило, ще і відображаються на індикаторах для того, щоб оператор міг отримати та прийняти відповідне керуюче рішення.

Такі 4-розрядні двійково-десяткові числа використовуються, наприклад, в системах збору даних з датчиків тепла, електроенергії, води. В більш складних сферах виробництва вони можуть використовуватися в далекомірах, частотомірах, фазометрах і тому подібних пристроях. Передача та відображення числових даних відбувається навіть при вимірюванні цифровими пристроями тривалості одиночних імпульсів, їх фронтів і зрізів, або зрушень між ними. Точність і швидкість таких вимірювань значно вища, ніж при використанні осцилографів з каліброваними розгортками, розтяжками, мітками та іншими подібними аналоговими пристроями, які використовуються для підвищення точності вимірювання [1].

При цьому досить часто ставиться задача не тільки передачі та відображення багато розрядної числової інформації, а і підвищення її секретності, тому що ця інформація може визивати також інтерес і для сторонніх осіб. Відповідно потрібен її захист від несанкціонованого доступу до неї, в тому числі і за допомогою шифрування. При цьому для підвищення стійкості шифру можна використовувати для кожного розряду десяткового

багато розрядного числа свій шифр. При цьому часто вимагається, щоб система передачі цифрових даних була захищена не тільки від несанкціонованого доступу, а і від завад, тому що числова інформація за своєю природою має мало надлишкової інформації, а тому є найменш захищена та відповідно найбільш вразлива від їх дії [2-7].

Побудова такої системи, яка передає і відображає багато розрядну числову інформацію та одночасно захищає її від несанкціонованого доступу і завад і є задачею даної роботи.

1.2 Ідея рішення

В основу рішення захисту від несанкціонованого доступу, що пропонується, покладені шифрувальні таблиці, які перетворюють набір з 10 двійково-десяткових вихідних цифр довжиною 4 біта у взяті випадково довільні перестановки цих же цифр, тобто реалізують широко розповсюджений стандар-тний шифр підстановок [8-10]. При цьому деякі з цих двійково-десяткових цифр можуть переходити в такі ж самі цифри. Перестановки беруться тому, що кожна цифра одного розряду, що передається, повинна відрізнятися від інших цифр, які можуть бути передані в цьому розряді. Якщо, наприклад, дві різні цифри кодуються одною двійково-десятковою комбінацією, то на приймальному кінці буде незрозуміло, яка з цих двох цифр передається.

Шифрувальна таблиця шифрує двійково-десяткові цифри одного розряду і тим самим створює його шифр і одночасно ключ. Кількість таких таблиць очевидно буде дорівнювати факторіалу $10! = 10 \times 9 \times 8 \times \ldots \times 1 = 3628800$. Три з них в якості прикладу наведені нижче в таблиці 1.1.

Всі вони можуть бути використані як шифри – ключі для 3 розрядів багато розрядного двійково-десяткового числа. Права сторона з кожної з цих таблиць являє собою ключ довжиною в 40 біт.

Якщо вона становиться відомою, то отримати вихідні цифри з них є досить простою задачею, яка вирішується переходом кодових зображень двійково-десяткових цифр з правої сторони таблиці на ліву.

Таблиця 1.1 – Варіанти шифрувальних таблиць

Варіант 1			Варіант 2			Варіант 3		
№	$x_1x_2x_3x_4$	$f_1f_2f_3f_4$	№	$x_1x_2x_3x_4$	$f_1f_2f_3f_4$	№	$x_1x_2x_3x_4$	$f_1f_2f_3f_4$
0	0000	0011	0	0000	0000	0	0000	0000
1	0001	0101	1	0001	0001	1	0001	0001
2	0010	0000	2	0010	0010	2	0010	0010
3	0011	1000	3	0011	0011	3	0011	0011
4	0100	0110	4	0100	0100	4	0100	0111
5	0101	0010	5	0101	1001	5	0101	1000
6	0110	0010	6	0110	1000	6	0110	1001
7	0111	0001	7	0111	0101	7	0111	0100
8	1000	1001	8	1000	0110	8	1000	0110
9	1001	0111	9	1001	0111	9	1001	0101

Однак для того, щоб їх знайти необхідно для кожного кодового зображення реальної двійково-десяткової цифри з 10 можливих цифр знайти одну. Для цього потрібно при аналізі отриманого кодового зображення двійково-десяткової цифри, яке декодується, знайти її реальне значення. Наприклад, в варіанті 1 таблиці 1.1 реальній цифрі 0000 відповідає зображення 0011. Треба довести, що реально запис 0011 передає значення 0000 десяткової цифри 0, або довести зворотне. Якраз ця задача для цифрових даних складає основну трудність, тому що, як правило, для них нема явних тестів, які б її вирішували, і тому для рішення цієї задачі треба шукати більш складні шляхи. Якщо б вдалося встановити в таблиці 1 кодування цифри 0000 комбінацією 0011, то тоді можна переходити до

декодування другої цифри, яка передається по каналу зв'язку, наприклад 1000, і так далі, поки не буде встановлена відповідність значень всіх $f_1f_2f_3f_4$ комбінаціям $x_1x_2x_3x_4$. Тільки в такому випадку можна вважати, що ключ до шифру знайдено. Можна в принципі 10 двійково-десяткових цифр для шифрування брати не з 10, а з їх загальної кількості 16, але це не міняє суть шифрування. Він залишається незмінним.

1.3 Ефективність захисту

Ефективність захисту розряду двійково-десяткового числа напряму залежить від наявності тесту, який би розпізнавав за невеликий час дійсне значення перехопленої двійково-десяткової комбінації цифри, що передається. Якщо б такий тест був, то тоді для 10 цифр потрібно було б зробити 10 розпізнавань, і на цьому завершити дешифрування одного розряду числа. Потім аналогічно можна було б розшифрувати цифри наступного розряду числа, якщо там використовується своя шифрувальна таблиця, і так далі. Якщо розрядів, наприклад, 5, то тоді знадобиться 50 кроків дешифрування. Це невелике число і захист, що розглядається, не мав би сенсу. Однак в реальності таких тестів розпізнавання цифр або нема, або вони досить складні, і тоді захист з допомогою шифрувальних таблиць, що розглядаються, може дати потрібні результати, особливо якщо інформація швидко старіє.

Крім того, є можливість зашифрувати порядок передачі цифр розрядів в десятковому числі. Зазвичай вони йдуть від старших розрядів до молодших. Але можна цей порядок і поміняти. Якщо, наприклад, передаються 5-розрядні двійково-десяткові десяткові числа, то порядок розрядів може змінюватися $5! = 120$ варіантами. Можна також два 5-розрядні двійково-десяткові числа передати одночасно змішаними і тоді буде отримано $10! = 3628800$ варіантів, або три таких числа, що збільшить кількість варіантів дешифрування до 15!. Тобто відомим методом шифрування

підстановок і перестановок можна отри-мати для даної задачі передачі числової інформації досить стійкий шифр [8-10].

1.4 Завадостійкість шифру

Підвищення завадостійкості цифр, що передаються, може відбуватися за рахунок використання 6 надлишкових станів в двійковій-десяткових числах, а також додаткового завадостійкого кодування, наприклад на парність, або непарність. Але є ще одна можливість отримати завадостійкий шифр – це використати рівноважний код з 2 одиницями та довжиною 5, в якому є 10 кодових комбінацій. В такому випадку таблиці 1.1 для варіанта 1 прийме наступний вигляд (таблиця 1.2).

Таблиця 1.2 – Завадостійке кодування

Завадостійкий код			Завадостійкий код		
№	$x_1x_2x_3x_4$	$f_1f_2f_3f_4$	№	$x_1x_2x_3x_4$	$f_1f_2f_3f_4$
0	0000	00011	5	0101	01100
1	0001	00101	6	0110	10001
2	0010	00110	7	0111	10010
3	0011	01001	8	1000	10100
4	0100	01010	9	1001	11000

Даний рівноважний код легко знаходить помилки підсумовуванням кількості одиниць в кодових словах. Якщо їх більше або менше 2, то це є ознакою помилки, а якщо 2, то це ознака відсутності помилки. Крім того, наявність шифрування в вигляді перестановок дозволяє зберігати та передавати ключі в системі з надійним їх захистом інформації від завад, що теж важливо, коли ключі часто змінюються. Перестановки по своїй природі мають досить значну надлишковість і відповідно можуть не тільки виявляти помилки, а і виправляти деякі з них [5,6]. Тому вони мають достатньо високу

ефективність при їх використанні в телекомунікаційних системах, особливо, якщо взяти до уваги можливість їх побудови з допомогою факторіальних чисел [5,6,11,12].

1.5 Система передачі та відображення двійково-десяткових цифр

В даному дослідженні розробляється система передачі та відображення однієї двійково-десяткової цифри. Передача та відображення інших двійково-десяткових цифр, які створюють додаткові розряди в десятковому числі, для кожної з них проходить паралельно за схемою, яка розроблена для одного розряду десяткового числа. Відповідно можна організувати паралельну передачу та відображення будь-якої кількості двійково-десяткових цифр з одночасним їх висвітленням на індикаторах. Хоча не виключається передача двійково-десяткових цифр, які належать багато розрядному числу, послідовно одна за другою з їх висвітленням на одному індикаторі. Такий варіант системи більш економний, але потребує додаткового запам’ятовування цифр, які відображаються.

Структурна схема системи передачі та відображення однієї двійково-десяткової цифри надана на рисунку 1.1.

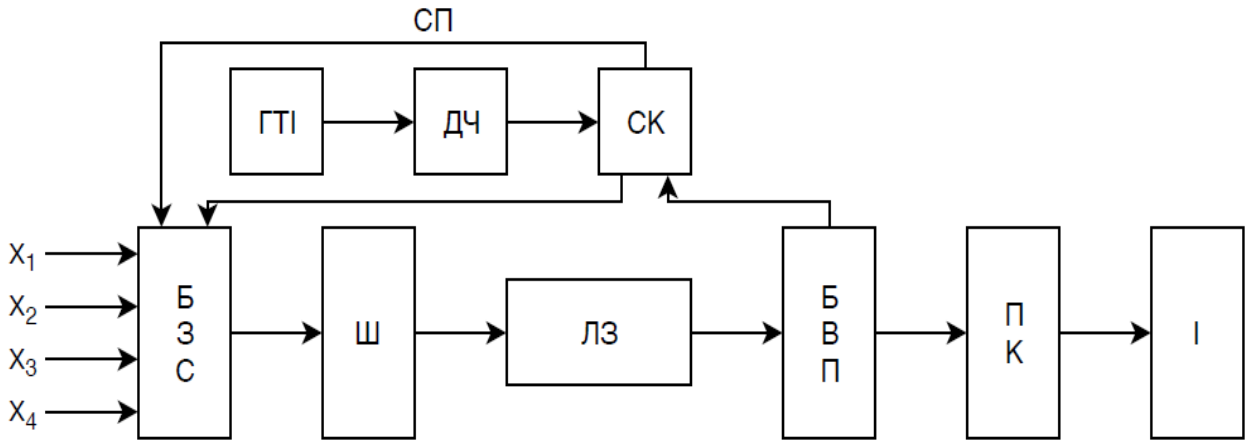

Рисунок 1.1 – Система передачі та відображення однієї двійково-десяткової цифри

Її блоки поділяються на блоки сторони, що передає дані, та блоки сторони, що сприймає ці дані. Відповідно до наведених позначень система, що розглядається, містить на стороні, яка передає дані, генератор тактових імпульсів (ГТІ), дільник частоти (ДЧ), систему керування (СК), буферну запам’ятовуючу схему (БЗС), шифратор (Ш), лінію зв’язку (ЛЗ). На прийомній стороні знаходиться: блок виправлення помилок (БВП), перетворювач кодів (ПК) чотирьох розрядних кодових комбінацій в семи розрядні кодові комбінації, індикатор (І).

Система працює наступним чином. На вхід буферної запам'ятовуючої схеми (БЗС) приходить і запам’ятовується двійково-десяткова цифра X_1, X_2, X_3, X_4, яка складається з 4-х розрядів. Вона відповідає десятковій цифрі, яка повинна бути передана по ЛЗ і відображена на індикаторі.

Ці цифри в шифрувальних таблицях обираються випадково, шляхом довільних перестановок 10 вихідних цифр. Таким чином, чотирьох розрядна двійково-десяткова цифра з БЗС в незмінному вигляді подається на шифратор, який перетворює її в чотирьох розрядне двійкове слово, яке, як правило, не відповідає вхідній цифрі. Після цього отримане на виході шифратора слово подається на лінію зв’язку (ЛЗ), де воно може спотворюватися під дією завад, перетворюючись в інше чотирьох розрядне слово. Якщо, це спотворене чотирьох розрядне слово по своєму числовому значенню не буде відноситися до слів, які зазначені в таблиці шифру, то воно визначається блоком виправлення помилок (БВП) як заборонене.

Відповідно цей блок видає сигнал на схему керування (СК) про те, що виникла помилка. З схеми керування надходить сигнал на БЗС і відбувається повторна відправка вхідної цифри в лінію зв’язку (ЛЗ). Якщо знову виникає помилка, то знову відбувається відправка вхідної цифри. Це може продовжуватися до трьох повторів передачі кодової комбінації по ЛЗ. Якщо після третього повтору знову з’являється помилка, то СК виробляє сигнал "Аварія", і система зупиняється.

Після того, як БВП сприйняв сигнал як правильний, він по сигналу зі СК відправляє його на перетворювач кодів (ПК), який замість чотирьох двійкових розрядів виробляє сім, які потім надходять на індикатор, для того, щоб висвітити його сегменти і тим самим відобразити відповідну цифру. Цифра, яка відображається на індикаторі повинна відповідати двійково–десятковій цифрі, яка знімається з БЗС. Цю відповідність реалізує ПК. Він може бути реалізований на постійному запам’ятовуючому пристрої, на адресні входи якого подаються зашифровані слова, а з комірок пам’яті знімаються дешифровані семи розрядні кодові слова, які перетворюються індикатором в зображення відповідних цифр. Подача на БЗС символів для індикації відбувається із заданою частотою, тобто вони періодично змінюються.

Система, що розглядається, може бути на практиці реалізована на одній мікросхемі ПЛІС і тому має невеликі габарити і відносно дешева та надійна. Її використання може швидко дати бажаний ефект і тому швидко окупитися.

1.6 Висновки дослідження

Система, що пропонується, має практичну направленість для задач передачі та відображення числової інформації, які є практично на кожному виробництві. Тому вона досить поширена. Введення в цю систему захисту інформації від несанкціонованого доступу і завад робить її більш прийнятною для сьогоденних умов, коли скритність і завадостійкість інформації є важливо вимогою сучасного виробництва. Запропонована система захисту десяткових чисел в вигляді двійково-десяткових шифрувальних таблиць проста, швидкодіюча та недорога, але в той же час може бути досить надійною. Її використання забезпечить надійну скритність і завадостійкість при передачі та відображенні числової інформації для багатьох випадків її впровадження в практику.

2 ОЦІНКА ЗАВАДОСТІЙКОСТІ КОДУВАННЯ ДЕСЯТКОВИХ ЦИФР РІВНОВАЖНИМИ КОМБІНАЦІЯМИ

2.1 Актуальність і мета дослідження

Кодування інформації все більше застосовується в різних галузях промисловості та господарства. Рівень завдань, покладених на електронні циф-рові пристрої та системи, в ряді випадків досить високий. Наслідки в результаті відмов технічних засобів через вплив перешкод можуть становити суттєві матеріальні втрати, нести загрозу безпеці та життю користувача. Дослідження питань оцінки завадостійкості засобів передачі інформації є необхідним та актуальним аспектом їх розвитку. Особливо це важливо з появою нових методів кодування та захисту інформації при порівнянні їх між собою [2-4, 13].

На практиці широко використовуються системи передачі двійково-десяткових цифр, які, наприклад, знімаються з вимірювальних пристроїв води, електрики і т.д. Однак при цьому виникає потреба їх захисту від завад. В роботі пропонується для цього використовувати кодування цих цифр рівноважними комбінаціями, як найбільш просте за апаратурною реалізацією, швидкодією і досить високою завадостійкістю [14-15].

Однак оцінка завадостійкості двійково-десяткових рівноважних кодів не має закінченого вигляду і тому потребує подальших досліджень. Дана робота спрямована на проведення такої оцінки. Вона дозволить в кінцевому підсумку оцінити ефективність роботи системи передачі числових даних, яка використовує двійково-десяткові рівноважні коди.

Рівноважний код – це двійковий код, в якому комбінації містять k одиниць та $(n - k)$ нулів, де n – довжина кодових комбінацій. Перевагою рівноважних кодів є можливість швидко та ефективно знаходити помилки під час обробки інформації. Оскільки рівноважний код складається з двійкових комбінацій, які містять k одиниць та $(n - k)$ нулів, можна легко

знайти помилку в них. Ознакою помилки є не співпадіння числа нулів (n - k) чи одиниць k в кодовій комбінації.

Так, наприклад в роботах [14-15] використовується завадостійкий код, в основу якого покладені рівноважні коди, які складаються з 2 одиниць та 3 нулів. Вони допомагають зашифрувати двійково-десяткові цифри від 0 до 9. Кожна кодова комбінація характеризується параметрами $k = 2$ та $n = 5$. Наприклад, для цифри 0 була застосована рівноважна кодова комбінація 00011. Отже, якщо після передачі цієї комбінації по каналу зв'язку кількість одиниць в ній буде відрізнятись від параметра $k = 2$, то це буде ознакою помилки.

Основними задачами дослідження є:

– оцінка завадостійкості рівноважних кодів, які кодують двійково-десяткові цифри;

– програмне моделювання системи передачі двійково-десяткових цифр.

2.2 Вихідний матеріал до дослідження

В роботах [16-17] була запропонована оцінка завадостійкості системи передачі даних за допомогою рівноважних кодів, кількість комбінацій в яких дорівнює M. Суть її полягає в тому що кожна кодова комбінація, яка буде передаватися по каналу зв'язку, може перейти, крім переходу в правильну комбінацію, в клас із $M - 1$ дозволених помилкових комбінацій, які не виявляються, або в клас із $(N - M)$ заборонених комбінацій, які можна виявити, де N – загальна кількість кодових комбінацій.

Для оцінки завадостійкості рівноважних кодів запропоновано використати формули імовірностей переходів кодових комбінацій в ці класи [7].

Правильний перехід рівноважної комбінації в саму себе при передачі оцінює ймовірність

$$П = \sum_{i=1}^{M} P_i p_i^i ,$$

де P_i – імовірність генерування джерелом інформації i-ї кодової комбінації;

p_i^j – імовірність переходу i-ї кодової комбінації в i-у.

Імовірність помилкових переходів рівноважних комбінацій, які не виявляються

$$V = \sum_{i=1}^{M} P_i p_i^H ,$$

де p_i^H – імовірність помилкового переходу i-ї комбінації в клас комбінацій, які не виявляються.

Вона визначається за формулою

$$p_i^H = \sum_{j=1, j\neq i}^{M} p_{i,j}^H ,$$

де – імовірність помилкового переходу i-ї комбінації, що передається, в j-у дозволену.

Імовірність помилкових переходів, які можна виявити

$$Z = \sum_{i=1}^{M} P_i p_i^0 ,$$

де p_i^0 – імовірність помилкового переходу i-ї комбінації, що передається, в клас комбінацій, які можна виявити.

Її можна визначити за формулою

$$p_i^0 = \sum_{j=M+1}^{N} p_{i,j}^0 ,$$

де – імовірність помилкового переходу для *i*-ї кодової комбінації.

Для оцінки завадостійкості рівноважних кодів також використаємо наступні теореми [16].

Теорема 2.1 Рівноважна кодова комбінація довжини n з k одиницями переходить в $C_k^r C_{n-k}^r$ комбінацій з r помилками, які не виявляються.

Для помилкового переходу, який не виявляється, від однієї рівноважної комбінації до іншої необхідно щоб перехід r одиниць в нулі супроводжувався б таким же самим переходом r нулів в одиниці. В іншому випадку помилку можна легко виявити простим підрахунком одиниць у кодовій комбінації.

Теорема 2.2 Кількість можливих переходів з помилками, які не виявляються, при $k \le n/2$ визначається за формулою

$$Y = \sum_{r=1}^{k} C_k^r C_{n-k}^r = C_n^k - 1.$$

Будь-яка рівноважна кодова комбінація із заданими k та n може перейти в будь-яку іншу з такими самими k та n. Кількість таких комбінацій буде дорівнювати $\mathrm{C_n^k}$. Але, оскільки одна з них є вихідною (базовою) то загальна кількість помилкових переходів буде дорівнювати $\mathrm{C_n^k}$-1.

Якщо відомі імовірності переходів нуля в нуль $\mathrm{p_{00}}$ та одиниці в одиницю $\mathrm{p_{11}}$, то імовірності переходів нуля в одиницю та одиниці в нуль можна визначити наступним чином: $p_{01} = 1 - p_{00}, p_{10} = 1 - p_{11}$.

Теорема 2.3 Імовірність переходу рівноважної кодової комбінації довжини n з $\mathrm{k \le n/2}$ одиницями в будь-яку дозволену комбінацію з помилками, які не виявляються, визначається за формулою

$$V_i = \sum_{r=1}^{k} C_k^r C_{n-k}^r p_{01}^r p_{10}^r p_{11}^{k-r} p_{00}^{n-k-r} .$$

Теорема 2.4 Імовірність помилкових переходів рівноважних комбінацій, які не виявляються

$$V = V_i,$$

де $V_i = p_i^H$.

Тому у випадку якщо $k \le n/2$ імовірність переходів рівноважних комбінацій в дозволені помилкові комбінації дорівнює

$$V = \sum_{i=1}^{M} P_i p_i^H = \sum_{i=1}^{M} P_i V_i = \sum_{i=1}^{M} \sum_{r=1}^{k} P_i C_k^r C_{n-k}^r p_{01}^r p_{10}^r p_{11}^{k-r} p_{00}^{n-k-r} .$$

Оскільки у всіх M рівноважних кодових комбінаціях, які генеруються джерелом інформації, кількість одиниць та нулів є сталими, то й імовірності V_i рівні між собою. Це означає, що будь-яке згенероване i має ту саму ймовірність V_i переходу в кодову комбінацію з помилкою, яка не виявляється:

$$V = \sum_{i=1}^{M} P_i V_i = V_i \sum_{i=1}^{M} P_i = V_i .$$

Після визначення значень ймовірності V помилкових переходів, які не виявляються та ймовірності $П$ правильного переходу, імовірність помилкових переходів, які можна виявити знаходиться наступним чином

$$Z = 1 - П - V .$$

2.3 Основний матеріал дослідження

Закодуємо двійково-десяткові цифри від 0 до 9 рівноважними кодовими комбінаціями довжини $n = 5$ з кількістю одиниць $k = 2$. Для цього використаємо таблицю 2.1.

Таблиця 2.1 – Кодування двійково-десяткових цифр рівноважним кодом

№	*x*1*x*2*x*3*x*4	*f*1*f*2*f*3*f*4*f*5
0	0 0 0 0	0 0 0 1 1
1	0 0 0 1	0 0 1 0 1
2	0 0 1 0	0 0 1 1 0
3	0 0 1 1	0 1 0 0 1
4	0 1 0 0	0 1 0 1 0
5	0 1 0 1	0 1 1 0 0
6	0 1 1 0	1 0 0 0 1
7	0 1 1 1	1 0 0 1 0
8	1 0 0 0	1 0 1 0 0
9	1 0 0 1	1 1 0 0 0

Проведемо аналіз завадостійкості досліджуваного коду. Для цього потрібно:

– визначити загальну *N* та дозволену *M* кількість кодових комбінацій;

– визначити значення ймовірності *V* помилкових переходів, які не виявляються, ймовірності *П* правильного переходу та ймовірності *Z* помилкових переходів, які можна виявити, для двійково-десяткових рівноважних кодових комбінацій при різних станах каналу зв’язку;

– оцінити ефективність методу захисту інформації від завад на базі рівноважних кодів.

Спочатку визначимо загальну (*N*) та дозволену (*M*) кількість кодових комбінацій.

Загальна кількість двійкових кодових комбінацій довжиною $n = 5$:

$$N = 2^n = 2^5 = 32.$$

Кількість дозволених кодових комбінацій для рівноважного коду з параметрами $n = 5$ та $k = 2$:

$$M = C_n^k = C_5^2 = 10.$$

Відповідно до наведеної вище математичної моделі обчислені значення ймовірностей V помилкових переходів кодових комбінаій в дозволені помилкові комбінації для симетричного каналу зв'язку. Також для цього каналу знайдені ймовірності $П$ правильного переходу та ймовірності Z помилкових переходів, які виявляються. Вони обчислюються для різних значень ймовірностей збою одного біту інформації. По результатам обчислення вказаних формул побудовані відповідні графіки на рисунках 2.1, 2.2, 2.3.

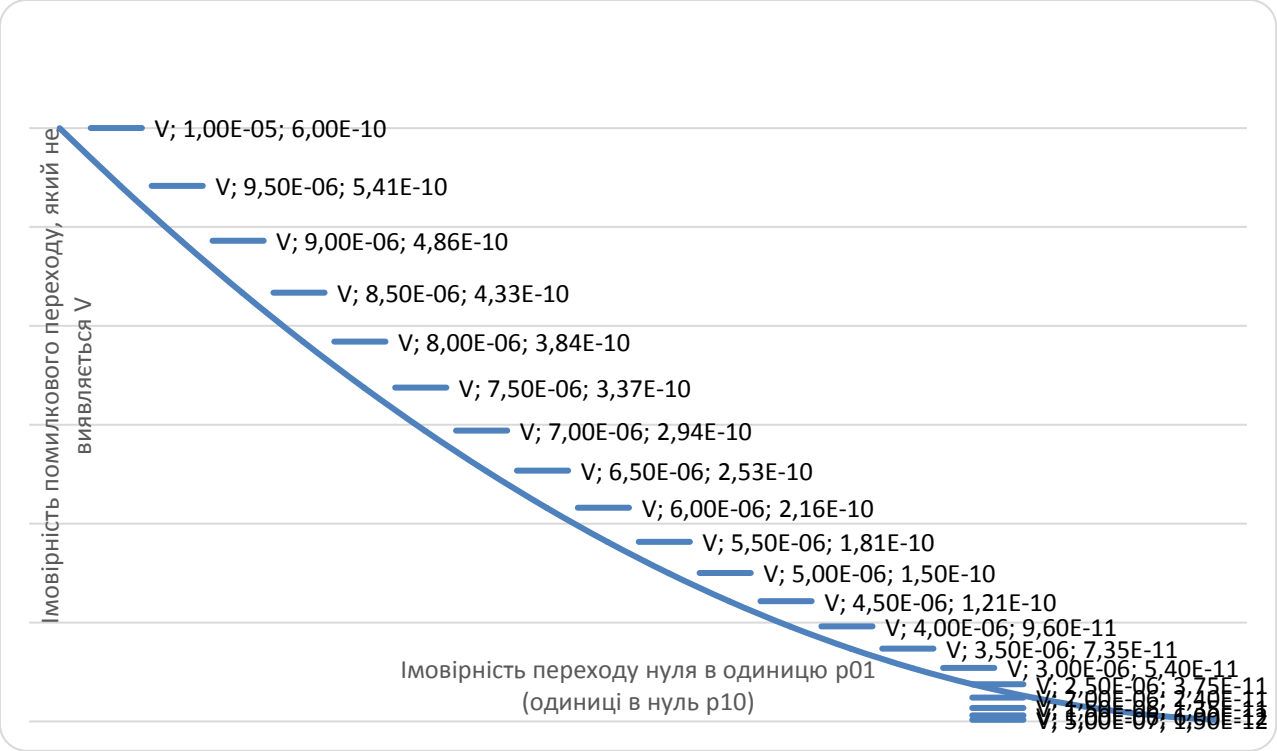

Рисунок 2.1 – Графік залежності ймовірності V помилкового переходу, який не виявляється, від ймовірності збою одного біта інформації

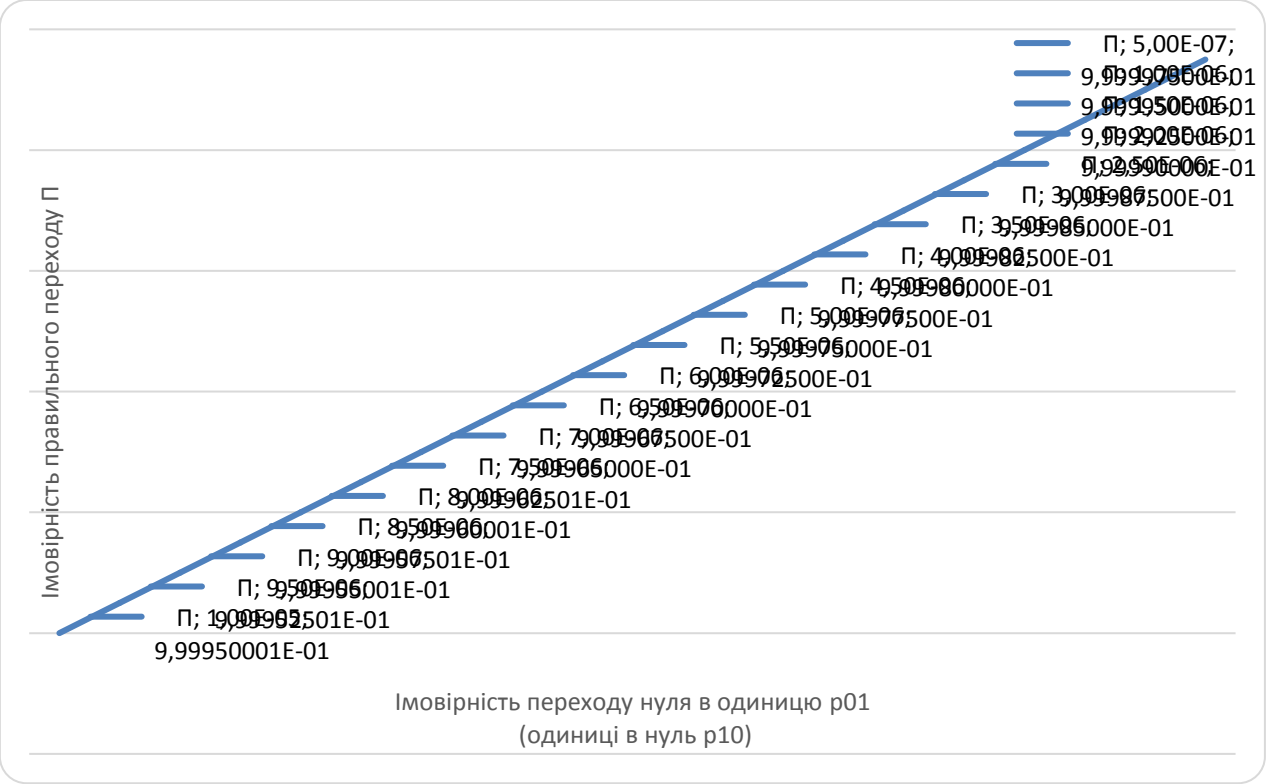

Рисунок 2.2 – Графік залежності ймовірності *П* правильного переходу від ймовірності збою одного біта інформації

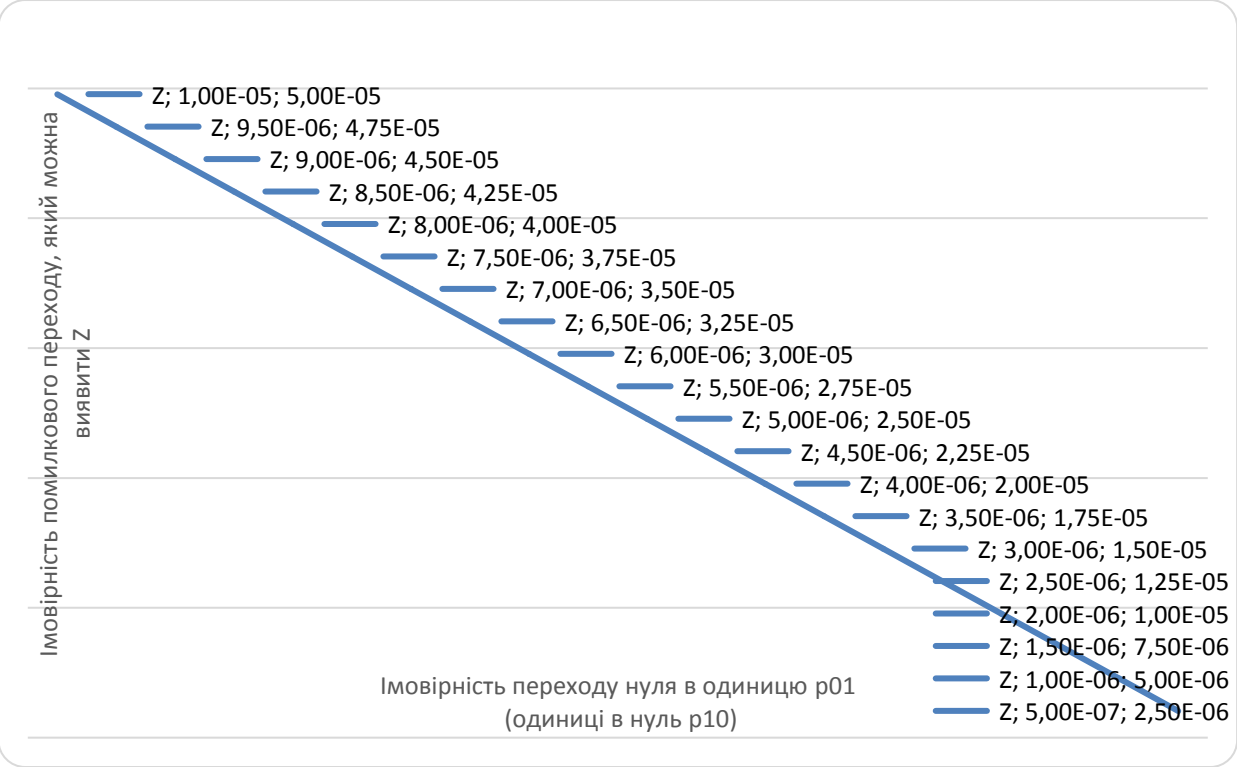

Рисунок 2.3 – Графік залежності ймовірності *Z* помилкового переходу, який можна виявити, від ймовірності збою одного біта інформації

Ці графіки дозволяють для кожного значення p_{01} (або p_{10}), виявити ймовірністі *П* правильної передачі двійково-десяткових рівноважних комбінацій і *Z* помилкової, які можна виявити, а отже і виправити. Це дозволяє прийняти рішення про експлуатаційну надійність системи передачі вимірювальної інформації і оцінити її ефективність.

Для встановлення кількісних вимог до достовірності передачі даних в автоматизованих розподілених системах та в системах телемеханіки у міжнародному стандарті IEC 870-5-1-95 визначені три класи достовірності даних I1, I2 та I3. Використання того чи іншого класу залежить від характеру даних, що передаються, наприклад, текстова інформація, вимірювальні дані та команди керування технологічними об'єктами. При проектуванні автоматизованих систем вважається достатнім при передачі текстової інформа-ції забезпечити значення *V* не гірше ніж 10^{-3}, при передачі вимірювальної інформації не гірше ніж 10^{-8}, а при передачі команд керування не гірше ніж 10^{-12}. Дотримання таких вимог необхідно здійснювати для встановленого рівня ймовірності збою одного біта інформації у каналах зв'язку не більше 10^{-4}, але не гірше ніж вимоги відповідного класу достовірності. Особливо важливо знати значення ймовірностей *V*, тому що ці помилки не виявляються, а значить можуть нанести шкоду, наслідки якої важко передбачити.

Результати досліджень значень ймовірностей *V* при застосуванні наведеного методу для захисту вимірювальної інформації від помилок наведені на рисунку 2.4. Там же показана відповідність *V* класам достовірності.

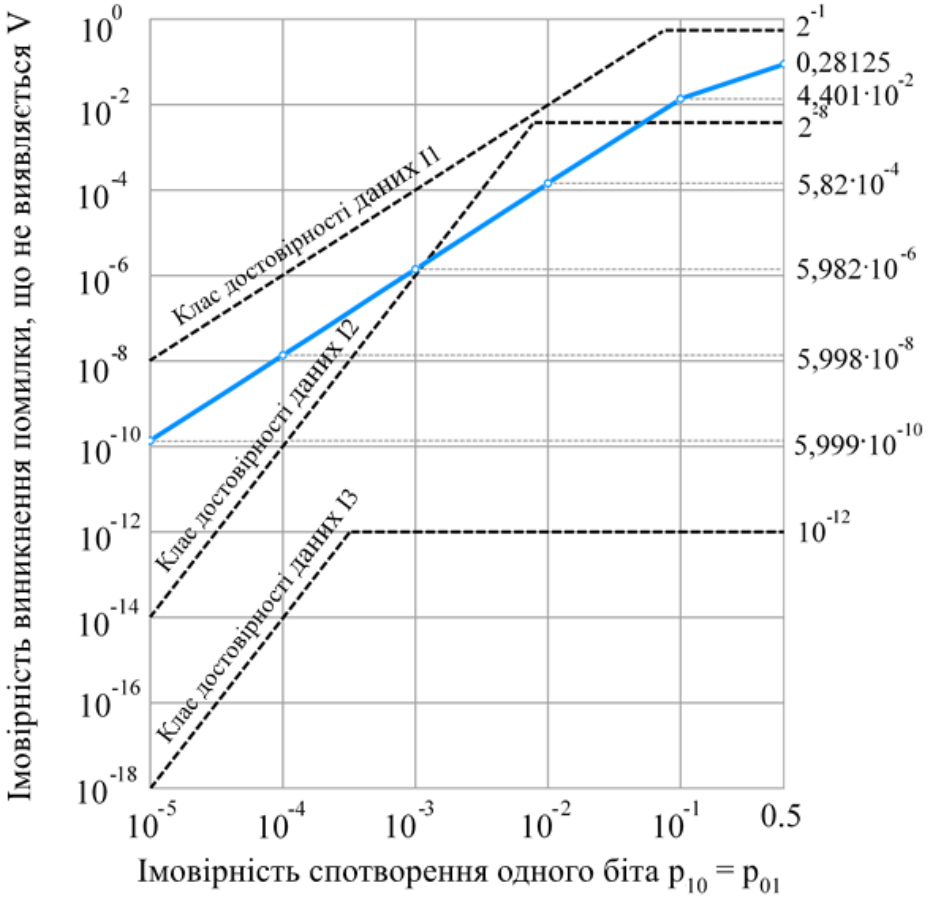

Рисунок 2.4 – Графік залежності ймовірності *V* помилкового переходу, який не виявляється, від ймовірності збою одного біта інформації для різних класів достовірності та наведеного методу захисту вимірювальної інформації

За результатами аналізу можна зробити висновок, що застосування рівноважних кодів забезпечує вимоги класу достовірності I1 у всьому діапазоні рівнів збою одного біту інформації. Вимоги класу I2 забезпечуються тільки до рівня ймовірності 10^{-3}. Вимоги, які забезпечують захист вимірювальної інформації до значення $V=10^{-8}$ отримані при рівні ймовірності збою одного біта інформації 10^{-4}.

Застосування рівноважних кодів забезпечило необхідний рівень захисту вимірювальної інформації у відповідності до вимог стандарту IEC 870-5-1-95 при введенні мінімального рівня надлишковості у вимірювальну інформацію.

2.4 Висновки дослідження

В роботі було досліджено кодування двійково-десяткових цифр рівноважними кодами. Проведена оцінка завадостійкості двійково-десяткових рівноважних кодів та побудована її програмна модель. В результаті дослідження можна зробити висновок, що надана методика оцінки завадостійкості кодування двійково-десяткових чисел рівноважними кодами дає можливість ефективно використовувати її на практиці.

Отримані результати та рекомендації носять універсальний характер і можуть бути застосовані та використані для різних систем зв'язку, які використовують десяткові цифри. В подальшому запропонована методика оцінки завадостійкості може бути використана і для більш складних задач кодування рівноважними кодами, наприклад текстової інформації.

3 ГЕНЕРУВАННЯ КВАЗІРІВНОВАЖНИХ КОДІВ НА ОСНОВІ ДВІЙКОВИХ БІНОМІАЛЬНИМИ ЧИСЕЛ

3.1 Актуальність мети і постановка задачі дослідження

Одним з підходів до біноміальному кодування є побудова на впорядкованій множині біноміальних чисел різних кодів, що мають біноміальну структуру, тобто структуру, в основі якої лежать біноміальні коефіцієнти [18, 19]. Переймаючись правилами комбінування кодових ознак (необов'язково елементів алфавіту) на структурі множини біноміальних чисел, можна отримати безліч різних кодів.

Серед перших результатів кодування з використанням двійкових біноміальних чисел є отримання рівноважних кодів, які знаходять широке застосування в системах комбінаторної оптимізації, передачі і шифрування даних [19 20]. Рівноважні кодові комбінації з параметрами n і k являють собою сполучення k одиниць з n двійкових розрядів. Складнощі їх формування полягають в тому, що, на жаль, відсутні прості, регулярні способи отримання рівноважних кодів з заданими значеннями n і k. Застосування ж двійкових біноміальних чисел в якості основи для побудови рівноважних кодових послідовностей дозволяє істотно спростити їх генерування не тільки в систематичному (лексикографічному) порядку, а й у випадковому.

Подібними до рівноважних кодів є квазірівноважні, які допускають кілька значень числа k одиниць в n-розрядних комбінаціях. Квазірівноважні коди представляють особливий інтерес не тільки як окремий тип комбінаторних конфігурацій – сполучень зі змінним числом одиниць, а й як коди, по-перше, що володіють значно більшою потужністю в порівнянні з рівноважними, а значить є більш ефективними для передачі з точки зору інформаційної надмірності, а, по-друге, як коди, здатні адаптуватися до рівня необхідної перешкодозахищеності за рахунок зміни кількості параметрів і їх значень.

Але формування квазірівноважних комбінацій має теж саму трудність, що і формування рівноважних – відсутність регулярних способів їх генерування, що в повній мірі негативно позначається для кодів великої потужності [21]. І тут ефективне вирішення зазначеної проблеми можливе на шляху використання двійкових біноміальних чисел, оскільки квазірівноважні кодові комбінації мають також біноміальну структуру.

Таким чином, метою даного дослідження є отримання простоти апаратно-програмної реалізації і високої швидкості формування квазірівноважних комбінацій. Для досягнення зазначеної мети необхідно вирішити такі завдання:

- виділити в структурі квазірівноважного коду виконавчі біноміальні числа;
- розробити метод і алгоритм формування квазірівноважних комбінацій на основі біноміальних чисел, що використовує числову функцію двійковій біноміальної системи числення.

3.2 Двійкові біноміальні числа

Двійкові біноміальні числа $X_j = \left(x_1 x_2 ... x_i ... x_r\right)$ з параметрами n і k генеруються двійковою біноміальною системою числення, яка володіє числовою функцією виду

$$F_j = x_1 C_{n-1}^{k-q_1} + ... + x_i C_{n-i}^{k-q_i} + ... + x_{r-1} C_{n-r+1}^{k-q_{r-1}} + x_r C_{n-r}^{k-q_r} = \sum_{i=1}^{r} x_i C_{n-i}^{k-q_i}, \qquad (3.1)$$

і системами обмежень для утворення множини X біноміальних чисел X_j, $X_j \in X$, $j = \overline{0, N-1}$:

$$\begin{cases} k \le r \le n-1 \\ q = k \\ x_r = 1 \end{cases} \quad \text{і} \quad \begin{cases} n-k = r-q \\ 0 \le q \le k-1, \\ x_r = 0 \end{cases} \qquad (3.2)$$

де n і k – цілочисленні параметри двійкової біноміальної системи числения;

r – кількість розрядів (довжина) біноміального числа, $r < n$;

x_i – біноміальна двійкова цифра – 0 або 1;

q – число одиниць в біноміальному числі;

q_i – сума одиничних значень x_i, починаючи з першого розряду числа до $(i-1)$-го включно:

$$q_i = \sum_{t=1}^{i-1} x_t , \tag{3.3}$$

де $q_1 = 0$, $q_i \le k$;

N – кількість двійкових біноміальних чисел X_j або потужність множини X.

Згідно системам обмежень (3.2) числа $X_j = (x_1 x_2 ... x_i ... x_r)$ мають нерівномірну довжину $\min(k, n-k) \le r \le n-1$. Якщо біноміальні числа $X_j = (x_1 x_2 ... x_i ... x_{r-1} 1)$ задовольняють першій системі обмежень (3.2) і, отже, закінчуються розрядом $x_r = 1$, то їх відносять до першого класу біноміальних чисел. Якщо $X_j = (x_1 x_2 ... x_i ... x_{r-1} 0)$ задовольняють другий системі обмежень (3.2) і, внаслідок цього, закінчуються розрядом $x_r = 0$, то такі числа відносяться до другого класу біноміальних чисел. При цьому перший і другий класи являють собою підмножини множини X біноміальних чисел [18].

В якості вагового коефіцієнта i-го розряду двійкового біноміального числа в числовій функції (3.1) виступає біноміальний коефіцієнт $C_{n-i}^{k-q_i}$, який залежить як від позиції $i = \overline{1,r}$ розряду, що розглядається, так і від суми q_i двійкових значень цифр x_i, що передують цьому розряду. Таким чином,

структуру двійкових біноміальних чисел $X_j = (x_1 x_2 ... x_i ... x_r)$ визначає число сполучень виду $C_{n-i}^{k-q_i}$.

Оскільки кількість N двійкових біноміальних чисел X_j з параметрами n і k складає $N = C_n^k$, то при розгляді відомої формули додавання для чисел сполучень

$$C_n^k = C_{n-1}^{k-1} + C_{n-1}^k \tag{3.4}$$

можна припустити, що структура біноміальних чисел лежить в основі кодових комбінацій довжини $(n-1)$ розрядів, які містять k і $(k-1)$ двійкових одиниць, тобто квазірівноважних комбінацій з параметрами n, k і $(k-1)$. Отже, на основі двійкових біноміальних чисел X_j можливо взаємно-однозначне відображення

$$\varphi_{кр} : X[n,k] \to Y[n-1,k,k-1]$$

множини X біноміальних чисел $X_j = (x_1 x_2 ... x_i ... x_r)$ з параметрами n і k на множині $Y[n-1,k,k-1]$ квазірівноважних комбінацій Y_j довжини $(n-1)$ розрядів, які містять k і $(k-1)$ двійкових одиниць. Висловлене припущення обгрунтовується нижчеподаною теоремою.

Теорема 3.1 При додаванні з боку молодших розрядів до двійкових нерівномірних біноміальних чисел $X_j = (x_1 x_2 ... x_i ... x_{r-1} 1)$ першого класу $(n-r-1)$ двійкових нулів, а до чисел $X_j = (x_1 x_2 ... x_i ... x_{r-1} 0)$ другого класу $(n-r-1)$ двійкових одиниць, формується квазірівноважний код $Y[n-1,k,k-1]$ довжини $(n-1)$ розрядів з кількістю двійкових одиниць k і

$(k-1)$, де n і k – параметри біноміальних чисел X_j, r – число розрядів біноміальних чисел X_j, $\min(k,n-k) \le r \le n-1$.

Доказ. Як відомо, довжина двійкових нерівномірних біноміальних чисел $X_j = (x_1 x_2 ... x_i ... x_r)$ знаходиться в діапазоні $k \le r \le n-1$ для біноміальних чисел $X_j = (x_1 x_2 ... x_i ... x_{r-1} 1)$ першого класу, і $n-k \le r \le n-1$ для біноміальних чисел $X_j = (x_1 x_2 ... x_i ... x_{r-1} 0)$ другого класу.

Також з систем обмежень (3.2) випливає, що для біноміальних чисел $X_j = (x_1 x_2 ... x_i ... x_{r-1} 1)$ першого класу кількість одиниць постійно і дорівнює k, а для біноміальних чисел $X_j = (x_1 x_2 ... x_i ... x_{r-1} 0)$ другого класу кількість нулів постійно і дорівнює $l = n-k$. Таким чином, якщо числа $X_j = (x_1 x_2 ... x_i ... x_{r-1} 1)$ першого класу доповнити нулями до довжии $(n-1)$, то, очевидно, кількість одиниць в них залишиться постійною і рівною k. Тогда як, доповнюючи біноміальні числа $X_j = (x_1 x_2 ... x_i ... x_{r-1} 0)$ другого класу одиницями до довжини $(n-1)$, їх кількість буде $q = n-1-(n-k) = k-1$.

Отже, при доповненні біноміальних чисел $X_j = (x_1 x_2 ... x_i ... x_{r-1} 1)$ першого класу нулями, а біноміальні числа $X_j = (x_1 x_2 ... x_i ... x_{r-1} 0)$ другого класу одиницями до довжини $(n-1)$ отримуємо квазірівноважний код $Y[n-1,k,k-1]$ довжини $(n-1)$ розрядів з кількістю двійкових одиниць k і $(k-1)$. **Теорема доведена.**

З бієктивного відображення $\varphi_{кр}$ можна зробити висновок, що кількість N вихідних двійкових біноміальних чисел буде дорівнювати потужності $N_{кр}$ квазірівноважного коду.

Теорема 3.2 Для потужності $N_{кр}$ множини $Y[n-1,k,k-1]$ квазірівноважних комбінацій справедлива наступна рівність

$$N_{кр} = C_{n-1}^{k} + C_{n-1}^{k-1}. \qquad (3.5)$$

Доказ. Згідно бієктивного кодового відображення $\varphi_{кр} : X[n,k] \to Y[n-1,k,k-1]$ маємо $N_{кр} = N = C_n^k$. Отже, на підставі властивості додавання чисел сполучень $N_{кр} = C_n^k = C_{n-1}^k + C_{n-1}^{k-1}$. **Теорема доведена.**

Для випадку, коли вихідні біноміальні числа X_j мають параметри $n = 6$ і $k = 3$, наведемо в лексикографічному порядку всі квазірівноважні комбінації $Y_j \in Y[5,3,2]$, використовуючи обґрунтований в теоремі 3.1 метод формування квазірівноважного коду (таблиця 3.1).

Кількість $N_{кр}$ квазірівноважних комбінацій $Y_j \in Y[5,3,2]$ визначається згідно виразу (3.5):

$$N_{кр} = C_{n-1}^{k-1} + C_{n-1}^{k} = C_5^2 + C_5^3 = 10 + 10 = 20.$$

На підставі вмісту розрядів x_r біноміальных чисел $X_j = (x_1 x_2 ... x_i ... x_r)$ приймається рішення про двійкове значення $(5-r)$ додаваних кодових елементів для формування квазірівноважних комбінацій $Y_j = (y_1 y_2 y_3 y_4 y_5)$, де $3 \le r \le 5$ і $j = \overline{0,19}$. В таблиці 3.1 розряди x_r розташовуються зліва від додаткових кодових елементів, виділених темним тлом. Умовно проведена межа між світлим і темним областями таблиці буде розділяти квазірівноважні комбінації $Y_j = (y_1 y_2 y_3 y_4 y_5)$ і відповідні їм біноміальні числа $X_j = (x_1 x_2 ... x_i ... x_r)$. Крім того, на рисунку 3.1 показана деревоподібна структура квазірівноважного коду $Y[5,3,2]$, яка повторює структуру множини біноміальних чисел $X[6,3]$.

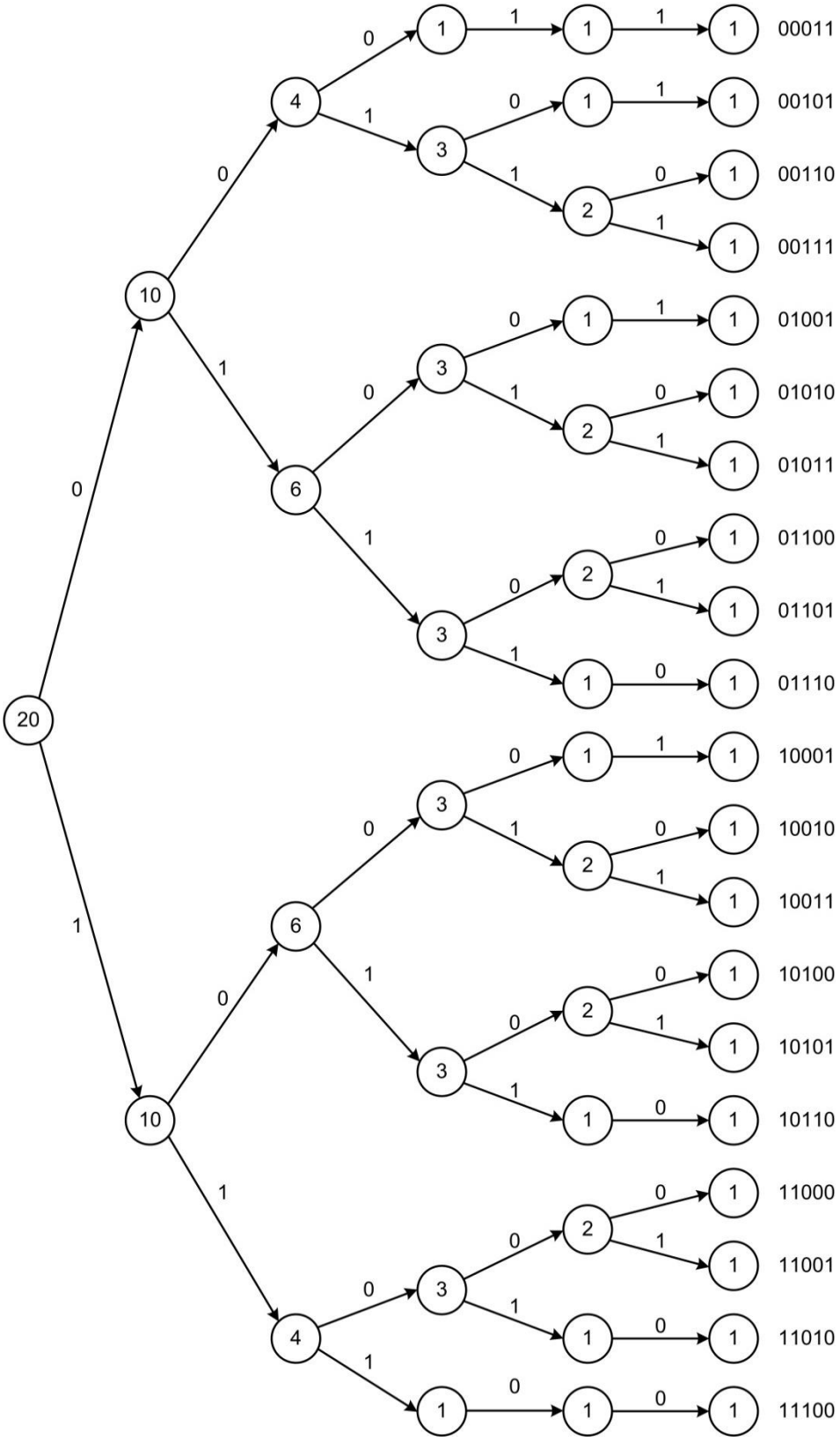

Рисунок 3.1 – Квазірівноважний код $Y[5,3,2]$ на структурі множини біноміальних чисел при $n = 6, k = 3, k = 2$

Таблиця 3.1 – Квазірівноважнй код з параметрами $n=5,\ k=3$ і $k=2$

F_j	Квазірівноважні комбінації $Y_j \in Y[5,3,2]$					F_j	Квазірівноважні комбінації $Y_j \in Y[5,3,2]$				
	y_1	y_2	y_3	y_4	y_5		y_1	y_2	y_3	y_4	y_5
0	0	0	0	**1**	**1**	10	1	0	0	0	**1**
1	0	0	1	0	**1**	11	1	0	0	1	0
2	0	0	1	1	0	12	1	0	0	1	1
3	0	0	1	1	1	13	1	0	1	0	0
4	0	1	0	0	**1**	14	1	0	1	0	1
5	0	1	0	1	0	15	1	0	1	1	**0**
6	0	1	0	1	1	16	1	1	0	0	0
7	0	1	1	0	0	17	1	1	0	0	1
8	0	1	1	0	1	18	1	1	0	1	**0**
9	0	1	1	1	**0**	19	1	1	1	**0**	**0**

3.3 Алгоритми прямого і зворотного перетворення

Відображення множини біноміальних чисел $X[n,k]$ на множині квазірівноважних комбінацій $Y[n-1,k,k-1]$, а також зворотне перетворення, можна реалізувати за допомогою алгоритмів, що використовують вельми прості операції порозрядного порівняння, підрахунку і конкатенації.

Загальний алгоритм, який реалізує пряме відображення $\varphi_{кр}$ для вихідних нерівномірних біноміальних чисел $X_j=(x_1x_2...x_i...x_r)$ з параметрами n і k виглядає наступним чином:

1. Визначення кількості r розрядів біномиального числа $X_j=(x_1x_2...x_i...x_r)$.

2. Якщо $r = n-1$, то біноміальне число $X_j = (x_1 x_2 ... x_i ... x_r)$ співпадає з відповідною квазірівноважною комбінацією $Y_j = (y_1 y_2 ... y_i ... y_{n-1})$. В іншому випадку переходимо до кроку 3.
3. Визначення значення останнього розряду x_r біноміального числа $X_j = (x_1 x_2 ... x_i ... x_r)$.
4. Якщо $x_r = 1$, то число $X_j = (x_1 x_2 ... x_i ... x_{r-1} 1)$ належить до першого класу біноміальних чисел і до нього праворуч від розряду $x_r = 1$ додаються $(n-r)$ двійкових нулів для отримання квазірівноважної комбінації виду $Y_j = (y_1 y_2 ... y_i ... y_{r-1} 100...0)$. В іншому випадку переходимо до кроку 5.
5. До числа $X_j = (x_1 x_2 ... x_i ... x_{r-1} 0)$, яке відноситься до другого класу біноміальних чисел, праворуч від розряду $x_r = 0$ додаємо $(n-r)$ двійкових одиниць для отримання квазірівноважної комбінації виду $Y_j = (y_1 y_2 ... y_i ... y_{r-1} 011...1)$.

В результаті роботи алгоритму прямого перетворення отримуємо шукані квазірівноважні комбінації $Y_j = (y_1 y_2 ... y_i ... y_{n-1})$ довжини $(n-1)$ з кількістю k або $(k-1)$ одиниць, відповідні вихідним нерівномірним біноміальним числам $X_j = (x_1 x_2 ... x_i ... x_r)$. При цьому повинні виконуватися рівності $x_1 = y_1$, $x_2 = y_2$, …, $x_{r-1} = y_{r-1}$.

Зворотне відображення

$$\varphi_{кр}^{-1} : Y[n-1, k, k-1] \to X[n, k]$$

квазірівноважних комбінацій $Y_j = (y_1 y_2 ... y_i ... y_{n-1})$ з параметрами $(n-1)$, k и $(k-1)$ на відповідні біноміальні числа $X_j = (x_1 x_2 ... x_i ... x_r)$ виконується за допомогою наступного загального алгоритму зворотного переходу:

1. Визначення значення останнього розряду y_{n-1} квазірівноважної комбінації $Y_j = (y_1 y_2 ... y_i ... y_{n-1})$.
2. Підрахунок кількості двійкових одиниць q і нулів l в вихідній квазірівноважній комбінації $Y_j = (y_1 y_2 ... y_i ... y_{n-1})$.
3. Якщо значення розряду $y_{n-1} = 1$, то переходимо до кроку 4. В іншому випадку виконується перехід до кроку 6.
4. Якщо кількість одиниць $q = k$ в комбінації $Y_j = (y_1 y_2 ... y_i ... y_{n-2} 1)$, то квазірівноважна комбінація збігається з відповідним біноміальним числом $X_j = (x_1 x_2 ... x_i ... x_{r-1} 1)$. В іншому випадку переходимо до наступного кроку.
5. В вихідній комбінації $Y_j = (y_1 y_2 ... y_i ... y_{r-1} 011...1)$ всі останні одиничні розряди відкидаються до появи першого нуля $y_r = 0$, і в результаті виходить біноміальне число виду $X_j = (x_1 x_2 ... x_i ... x_{r-1} 0)$.
6. Якщо кількість нулів $l = n - k$ в комбінації $Y_j = (y_1 y_2 ... y_i ... y_{n-2} 0)$, то квазірівноважна комбінація збігається з відповідним біноміальним числом $X_j = (x_1 x_2 ... x_i ... x_{r-1} 0)$. В іншому випадку переходимо до наступного кроку.
7. В вихідній комбінації $Y_j = (y_1 y_2 ... y_i ... y_{r-1} 100...0)$ всі останні нульові розряди відкидаються до появи першого одиниці $y_r = 1$, і в результаті виходить біноміальне число виду $X_j = (x_1 x_2 ... x_i ... x_{r-1} 1)$.

В результаті роботи алгоритму зворотного перетворення отримуємо шукані нерівномірні біноміальні числа $X_j = (x_1 x_2 ... x_i ... x_r)$ довжини r з параметрами n і k, відповідні вихідним квазірівноважним комбінаціям $Y_j = (y_1 y_2 ... y_i ... y_{n-1})$. При цьому повинні виконуватися рівності $y_1 = x_1$, $y_2 = x_2$, …, $y_{r-1} = x_{r-1}$.

3.4 Висновки дослідження

Встановлений в даній роботі факт, що квазірівноважні комбінації довжини $(n-1)$ розрядів, які містять k і $(k-1)$ двійкових одиниць, мають ту ж структуру, що і двійкові біноміальні числа з параметрами n і k, дозволив синтезувати алгоритм прямого перетворення біноміальних чисел в квазірівноважної код, а також алгоритм зворотного перетворення. Отримані алгоритми відрізняються наступними позитивними властивостями:

1) використання простих операцій, як наприклад, поразрядного порівняння, підрахунку одиниць і конкатенації кодових частин перетворюються комбінацій;
2) обмежена кількість самих операцій, що проводяться в процесі перетворень, яке змінюється тільки полиномиально зі збільшенням довжини n комбінацій.

Дані відмінні риси розроблених алгоритмів призводять до порівняно невеликого обсягу апаратно-програмних витрат при їх практичної реалізації, а також забезпечують високу швидкість їх роботи, що відповідає поставленої в роботі мети наукових досліджень.

Перспектива подальшої наукової роботи в даному напрямку полягає у вирішенні завдань перерахування і генерування квазірівноважних комбінацій, використовуючи отримані в роботі алгоритми як складові частини більш загального процесу перетворень з використанням біноміальних чисел.

4 РОЗРОБКА МЕТОДІВ СТИСКАЮЧОГО КОДУВАННЯ ДАНИХ НА ОСНОВІ ДВІЙКОВИХ БІНОМІАЛЬНИХ ЧИСЕЛ

4.1 Актуальність і постановка завдання дослідження

Застосування стискаючого кодування даних має на меті, перш за все, підвищення продуктивності інформаційних систем, до числа яких можна віднести комп'ютеризовані системи управління, системи архівування даних, розподілені бази даних і т.п. Стиснення інформації дозволяє домогтися продуктивності двома шляхами [22, 23]:

1) зменшення витрат часу на передачу інформації каналами зв'язку;

2) збільшення ємності пам'яті для зберігання інформації, яка застосовується в системі.

Підвищення продуктивності системи, згідно з першим напрямком, полягає в тому, що за той же період часу збільшується кількість інформації, яка передається по каналу зв'язку. Тим самим збільшується пропускна здатність каналу, але, умовно кажучи, «віртуально» без зміни його реальних характеристик. Таким чином, інформаційна система отримує можливість за той же період часу обробляти більшу кількість даних.

Відповідно до другого напрямку, зростання продуктивності інформаційної системи можливий за рахунок:

– збільшення кількості стислих даних в пам'яті тієї ж ємності;

– зменшення обсягу пам'яті для зберігання стислих даних з тією ж самою кількістю інформації.

Таким чином, стиснення інформації є спосіб збільшення продуктивності обробки даних в різних інформаційних системах, який характеризується незначними витратами в економічному плані. У зв'язку з цим, розробка і дослідження методів і алгоритмів стиснення є актуальною задачею, що має не тільки наукову, а й техніко-економічну цінність.

4.2 Об'єкт дослідження

Об'єкт дослідження – методи стиснення даних без втрат, призначені для усунення інформаційної надмірності повідомлень і мінімізації їх довжини, тобто скорочення розрядності їх подання.

Методи стискаючого кодування характеризуються [22–24]:

– типом стискуваних даних;

– моделями процесів стиснення і відновлення на основі аналітичних співвідношень або статистичних залежностей;

– алгоритмами (схемами пристроїв) стиснення і відновлення даних.

Використання стиснення даних в інформаційних системах дозволяє:

1) знизити вартісні витрати на їх створення за рахунок здешевлення пристроїв пам'яті і можливості застосування недорогих низькошвидкісних каналів зв'язку;

2) підвищити їх продуктивність за рахунок збільшення швидкості передачі інформації по вже існуючим каналам і збільшення кількості збережених даних у вже наявної пам'яті без істотних витрат на їх модернізацію.

При цьому особливий інтерес викликають методи, над результатами стиснення яких можна проводити обчислювальні операції без зворотного відновлення до вихідних послідовностей.

Одними з найбільш проблемних місць впровадження стиснення є високі вимоги до обчислювальних ресурсів системи, значні витрати при його реалізації і невисока швидкість кодування/декодування. Для поліпшення зазначених характеристик стиснення даних в інформаційних системах пропонуються до розгляду методи стиснення на основі двійкових біноміальних чисел.

4.3 Мета і завдання дослідження

Метою даної роботи є мінімізація часу стиснення і відновлення двійкових послідовностей при обмеженні на обсяг апаратно-програмних

витрат при практичній реалізації методів стиснення на основі двійкових біноміальних чисел.

Завдання дослідження роботи формулюються наступним чином:

1. Побудова математичної моделі методу стиснення двійкових n-розрядних рівноважних комбінацій з фіксованим числом $0 < k < n$ одиниць на основі двійкових (n,k)-біноміальних чисел.

2. Побудова математичної моделі узагальненого методу стиснення двійкових n-розрядних послідовностей зі змінним числом $0 \le k \le n$ одиниць на основі двійкових (n,k)- біноміальних чисел.

4.4 Дослідження існуючих рішень проблеми

Величезну роль, як і раніше, в інформаційних системах відіграють методи стиснення без втрат інформації, що пояснюється тим, що [24, 25]:

1) стискаюче кодування без втрат є більш універсальним рішенням з огляду на те, що воно, як правило, не орієнтується на конкретний, вузько спеціалізований тип інформації, а може працювати відразу з множиною типів даних;

2) значна кількість методів стиснення без втрат мають справу з двійковою інформацією, що додатково підкреслює універсальний характер таких методів;

3) для багатьох інформаційних систем застосування стиснення без втрат є безальтернативним з урахуванням невизначеності ціннісного критерію використовуваних даних або відсутності психофізіологічного фактора сприйняття інформації. До таких систем, наприклад, можна віднести системи автоматизації наукового експерименту, системи автоматичного управління, розподілені бази даних.

Перспективними є методи і алгоритми стиснення без втрат на основі структурних чисел [26, 27], які генеруються структурними системами числення. Основною ідеєю стискаючого перетворення інформації на основі

структурних систем числення є те, що в структурі будь-якої кодової послідовності можна виявити відповідне структурне число. Таким чином, поставивши у відповідність вихідним кодовим послідовностям їх структурні числа можна істотно зменшити інформаційну надмірність.

Особливе місце серед структурних систем числення займають двійкові біноміальні системи з параметрами n і k, які генерують двійкові (n,k)-біноміальні числа [18, 27]. Числова функція двійквої (n,k)-біноміальної системи числення, яка визначає десятковий кількісний еквівалент $F_j = \mathrm{dec}\, X_j$ двійкового біноміального числа X_j, має вид [18, 27]:

$$F_j = \mathrm{dec}\ X_j = \sum_{i=1}^{r} x_i C_{n-i}^{k-q_i},$$

де $X_j = x_1 x_2 ... x_i ... x_r$, $r < n$, $X_j \in X$, $j = 1, 2, ..., C_n^k$;

q_i – сума одиничних цифр x_i від першого розряда до (i–1)-го включно:

$$q_i = \sum_{t=1}^{i-1} x_t,\ q_i \le k.$$

(n,k)-біноміальні числа X_j, які генеруються повинні задовільняти наступним кодоутворюючим обмеженням [27, 28]:

$$\begin{cases} l = n - k, \\ x_r = 0, \end{cases} \quad \text{и} \quad \begin{cases} q = k, \\ x_r = 1, \end{cases}$$

де q і l – числа одиниць и нулів в двійковому біноміальному числі X_j.

У роботах [29, 30] наводяться способи кодування джерел інформації з використанням комбінаторної системи числення, але структурні числа при кодуванні не використовуються, а здійснюється безпосередній перехід від

стискаємої послідовності до двійкового номеру. Такий перехід характеризується складністю обчислень. Хоча в роботі [30] робиться спроба розгляду біноміальних кодів, але без системного підходу при відсутності кодоутворюючих обмежень.

У роботах [31, 32] розглядаються методи стискаючого кодування на основі нумераційних функцій, але, з одного боку, дані методи мають істотну обчислювальну складність, а, з іншого, структурні числа при розгляді цих методів не розглядаються. Крім того, стискувані послідовності характеризуються складними комбінаторними обмеженнями, що обмежує використання запропонованих методів.

В роботі [33] наводиться тезисно модель стиснення на основі двійкових біноміальних чисел, але тільки для одного типу двійкових послідовностей – рівноважних комбінацій, які мають вельми обмежене поширення.

Теоретичною і практичною основою даної роботи є той факт, що в основі будь-яких двійкових послідовностей, які стискаються, можна виявити відповідні їм структурні числа, що генеруються структурними системами числення [27]. Такий підхід до розробки методів стискаючого кодування характеризується універсальністю вирішення завдань, а також отриманням стиснутих образів, що володіють числовими характеристиками. Це дозволяє в разі потреби проводити їх обчислювальну обробку без їх відновлення.

У наведеному дослідженні в якості послідовностей, що стискаються, розглядаються двійкові рівноважні комбінації, які можна отримати з будь-якої двійкової послідовності шляхом простого підрахунку числа двійкових одиниць, які містяться в ній.

4.5 Методи дослідження

Реализація біноміального відображення $\varphi^{-1}: Y \to X$ в рамках побудови математичної моделі перерахування для вихідних двійкових n-розрядних послідовностей виду $Y_j \in Y\left[n,k\right]$ є стиснення:

$$f_b : Y[n,k] \to X[n,k], \tag{4.1}$$

рівноважних комбінацій Y_j на основі двійкових (n,k)-біноміальних чисел $X_j \in X[n,k]$ [14]. В свою чергу, реалізація біноміального відображення $\varphi : X \to Y$ в рамках побудови математичної моделі генерування для $Y_j \in Y[n,k]$ значить відновлення:

$$f_b^{-1} : X[n,k] \to Y[n,k], \tag{4.2}$$

вихідних рівноважних комбінацій Y_j на основі двійкових (n,k)-біноміальних чисел $X_j \in X[n,k]$.

Нижченаведена теорема 4.1, яку приведена без доказу, вказує властивості відображення f_b і спосіб його практичної реалізації. Домовимося операцію декатенації далі позначати символом виду «/».

Теорема 4.1 Будь-якій двійковій послідовності $Y_j = y_1 y_2 ... y_i ... y_n$, $Y_j \in Y[n,k]$, $j = \overline{1, C_n^k}$, що складається з n розрядів y_i, сума значень якихх дорівнює k, можна поставити у відповідність єдине двійкове (n,k)-біноміальне число $X_j = x_1 x_2 ... x_i ... x_r$, $X_j \in X[n,k]$, $r < n$, за допомогою функції $X_j = f_b(Y_j)$ виду:

$$X_j = x_1 x_2 ... x_i ... x_r = \begin{bmatrix} y_1 y_2 ... y_i ... y_{n-1} 0/00...0, \\ y_1 y_2 ... y_i ... y_{n-1} 1/11...1. \end{bmatrix} \tag{4.3}$$

Таким чином, відображення $f_b : Y[n,k] \to X[n,k]$, яке задається теоремою 4.1, будемо називати методом стиснення на основі двійкових (n,k) -біноміальних чисел або біноміальним стисненням.

Моделювання процесу стиснення f_b двійкових рівноважних комбінацій $Y_j = y_1 y_2 ... y_i ... y_n$ на основі двійкових (n,k)-біноміальних чисел X_j, використовуючи теорему 4.1 і функцію (4.3), складається з наступних етапів.

Eman 1. Визначається в n-розрядній рівноважній комбінації $Y_j = y_1 y_2 ... y_i ... y_n$, яка має число k одиниць, значення останнього розряду y_n.

Eman 2. Якщо $y_n = 0$, то:

$$X_j = Y_j / 00...0 = y_1 y_2 ... y_i ... y_{n-1} 0 / 00...0 = x_1 x_2 ... x_i ... x_{r-1} 1,$$

тобто від комбінації $Y_j = y_1 y_2 ... y_i ... y_{n-1} 0$ відкидаються всі нульові розряди, починаючи з $y_n = 0$, до появи першої двійкової одиниці $y_r = 1$, яка представлятиме значення останнього розряду $x_r = y_r = 1$ вихідного (n,k)-біноміального числа $X_j = x_1 x_2 ... x_i ... x_{r-1} 1$. В іншому випадку:

$$X_j = Y_j / 11...1 = y_1 y_2 ... y_i ... y_{n-1} 1 / 11...1 = x_1 x_2 ... x_i ... x_{r-1} 0,$$

тобто від комбінації $Y_j = y_1 y_2 ... y_i ... y_{n-1} 1$ відкидаються всі одиничні розряди, починаючи з $y_n = 1$, до появи першого двійкового нуля $y_r = 0$, який буде представляти значення останнього розряду $x_r = y_r = 0$ вихідного (n,k)-біноміального числа $X_j = x_1 x_2 ... x_i ... x_{r-1} 0$. При цьому в обох випадках значення інших розрядів залишаються без змін: $x_1 = y_1$, $x_2 = y_2$,…, $x_{r-1} = y_{r-1}$.

Теорема 4.2, яку наведемо без доказу, надає властивості відображення f_b^{-1} і спосіб його практичної реалізації. Введемо тепер в розгляд операцію конкатенації, яку позначимо як «++». Дана дія є зворотною по відношенню до операції декатенації.

Теорема 4.2 Будь-якому двійковому (n,k)-біноміальному числу $X_j = x_1x_2...x_i...x_r$, $X_j \in X[n,k]$, $r < n$, можна поставити у відповідність єдину двійкову рівноважну комбінацію $Y_j = y_1y_2...y_i...y_n$, $Y_j \in Y[n,k]$, $j = \overline{1,C_n^k}$, складену з n розрядів y_i, сума значень яких дорівнює k, за допомогою функції $Y_j = f_b^{-1}(X_j)$ виду:

$$Y_j = y_1y_2...y_i...y_n = \begin{bmatrix} x_1x_2...x_i...x_{r-1}0++11...1, \\ x_1x_2...x_i...x_{r-1}1++00...0. \end{bmatrix} \quad (4.4)$$

Моделювання процесу відновлення f_b^{-1} двійкових рівноважних комбінацій $Y_j = y_1y_2...y_i...y_n$ на основі двійкових (n,k)-біноміальних чисел X_j, використовуючи теорему 4.2 і функцію (4.4), складається з наступних етапів.

Етап 1. Визначається в двійковому (n,k)-біноміальному r-розрядному числі $X_j = x_1x_2...x_i...x_r$, $X_j \in X[n,k]$, $r < n$, значення останнього розряду x_r.

Етап 2. Якщо $x_r = 0$, то:

$$Y_j = X_j++11...1 = x_1x_2...x_i...x_{r-1}0++11...1 = y_1y_2...y_i...y_{n-1}1,$$

тобто до двійкового біноміального числа $X_j = x_1x_2...x_i...x_{r-1}0$ приєднуються одиничні розряди 11...1: $y_{r+1} = y_{r+2} = ... = y_n = 1$ так, щоб загальна кількість розрядів шуканої двійкової рівноважної комбінації Y_j складала n, $Y_j \in Y[n,k]$. В іншому випадку:

$$Y_j = X_j++00...0 = x_1x_2...x_i...x_{r-1}1++00...0 = y_1y_2...y_i...y_{n-1}0,$$

тобто до двійкового біноміального числа $X_j = x_1 x_2 ... x_i ... x_{r-1} 1$ приєднуються нульові розряди $00...0$: $y_{r+1} = y_{r+2} = ... = y_n = 0$ так, щоб загальна кількість розрядів шуканої двійкової рівноважної комбінації Y_j складала n, $Y_j \in Y[n,k]$. При цьому в обох випадках значення інших розрядів залишаються без змін: $x_1 = y_1$, $x_2 = y_2$, …, $y_r = x_r = 1$.

Відображення $f_b : Y[n,k] \to X[n,k]$ є бієктивним, оскільки відповідності $X_j = f_b(Y_j)$ і $Y_j = f_b^{-1}(X_j)$ є функціональні (теореми 4.1 и 4.2), тобто кожний елемент $Y_j \in Y[n,k]$ має єдиний образ $X_j \in X[n,k]$, а кожний елемент $X_j \in X[n,k]$ − єдиний прообраз $Y_j \in Y[n,k]$.

Відображення виду f_b і f_b^{-1} оперують з двійковими n-розрядними рівноважними комбінаціями $Y_j \in Y[n,k]$, тобто число k одиниць є величина постійна. При цьому слід врахувати, що, виходячи з властивостей двійкових (n,k)-біноміальних чисел [23], $k_{\min} = 1$ і $k_{\max} = n-1$. Більш загальним є випадок, коли k може приймати будь-які значення з заданого діапазону $0 \le k \le n$, а масив A, що стискається, є множина:

$$A = \bigcup_{k=0}^{n} Y[n,k] \text{ и } A_j \in A = \{0,1\}^n, \ j = \overline{1, 2^n},$$

двійкових n-розрядних послідовностей A_j, для яких відсутнє обмеження виду по числу k одиниць.

З урахуванням того, що двійкові (n,k)-біноміальніе числа X_j є префіксними тільки для постійного значення k [27], то для однозначного відновлення $A_j \in A = \{0,1\}^n$ з чисел X_j слід додатково використовувати значення k одиниць, вираженого в двійковому вигляді Bin$k$.

При стисненні A_j необхідно використовувати функцію f_w, яка ставить у відповідність вихідній послідовності A_j виборку $\left(k, Y_j\right)$, де $Y_j = A_j$. Далі, якщо отримане значення k задовольняє нерівності $0 < k < n$, то для стиснення рівноважної комбінації Y_j, відповідній A_j, використовується кодування f_b на основі двійкових біноміальних чисел. При цьому до стислих комбінацій для однозначного відновлення додається $\mathrm{Bin}k$, тобто виконується додатково кодування виду f_k. Якещо ж значення k задовольняє системі рівностей $\left(k = 0\right) \vee \left(k = n\right)$, то кодована результуюча комбінація буде складатися тільки з $\mathrm{Bin}k$, тобто використовується єдиний метод кодування f_k.

Таким чином, розглянемо відображення виду:

$$f_{bg} : A \to Z,$$

яке задається відповідною функцією:

$$Z_j = f_{bg}\left(A_j\right),$$

де $A_j = a_1 a_2 ... a_i ... a_n$, $A_j \in A = \{0,1\}^n$, $Z_j = \left(\mathrm{Bin}\, k, X_j\right)$ або $Z_j = \mathrm{Bin}\, k$, $Z_j \in Z$, $j = \overline{1, 2^n}$. Нижченаведена теорема 4.3, яку наведемо без доказу, вказує властивості відображення f_{bg} і спосіб його реалізації.

Теорема 4.3 Будь-якій двійковій послідовності $A_j = a_1 a_2 ... a_i ... a_n$, $A_j \in A = \{0,1\}^n$, $j = \overline{1, 2^n}$, можна поставити у взаємно однозначну відповідність двійкову комбінацію $Z_j \in Z$ наступного виду:

1) якщо $0 < k < n$, то:

$$Z_j = \mathrm{Bin}\, k + + X_j, \tag{4.5}$$

де $k = \sum_{i=1}^{n} a_i$ і $X_j = f_b\left(Y_j\right),\ X_j \in X\left[n,k\right],\ Y_j \in Y\left[n,k\right];$

2) в іншому випадку, якщо $\left(k=0\right) \vee \left(k=n\right)$, то:

$$Z_j = \mathrm{Bin}\, k. \tag{4.6}$$

Відображення $f_{bg} : A \to Z$ також є бієктивним, оскільки кожний елемент A_j має єдиний образ, а кожний елемент Z_j – єдиний прообраз для всіх $A_j \in A$ і $Z_j \in Z$.

Способи практичної реалізації відображень f_{bg} і f_{bg}^{-1}, вказаних в теоремі 4.3, можуть бути різними. Вибрані підходи до побудови f_{bg} і f_{bg}^{-1}, методи кодування і моделі процесів, що формуються для них, в кінцевому підсумку впливають на швидкодію й обсяг апаратно-програмних витрат при їх практичної реалізації.

Відображення $f_{bg} : A \to Z$ називається узагальненим методом стиснення на основі двійкових $\left(n,k\right)$-біноміальных чисел (або узагальненим біноміальним стисненням), яке задається наступною складною функцією виду:

$$f_{bg} = \begin{cases} f_k \circ f_w,\ \left(k=0\right) \vee \left(k=n\right), \\ f_k \circ f_b \circ f_w,\ 0 < k < n, \end{cases} \tag{4.7}$$

де Z – множина результуючих послідовностей Z_j:

$$Z = Z_o \cup Z_b,$$

$$Z_o = Q \times \varnothing = \left\{ Z_j \,/\, Z_j = \mathrm{Bin}\, k, \left(k=0\right) \vee \left(k=n\right) \right\},$$

$$Z_b = Q \times X[n,k] = \left\{ Z_j \,/\, Z_j = \left(\mathrm{Bin}\, k, X_j \right), 0 < k < n-1 \right\},$$

$$Q = \left\{ \mathrm{Bin}\, k \,/\, 0 \le k \le n \right\},\ Y_j \in Y[n,k],\ Y_j = f_w\left(A_j\right);$$

f_k – функція $Z_j = f_k\left(A_j\right)$, яка ставить у відповідність вихідній послідовності $Y_j = A_j$ двійкову запис $\mathrm{Bin}\, k$ числа k одиниць, де $\left(k=0\right) \vee \left(k=n\right)$, і яка визначає відображення виду:

$$f_k : Y[n,k] \to Z_o,$$

або функція $Z_j = f_k\left(X_j\right)$, яка ставить у відповідність двійковому (n,k)-біноміальному числу результуючу послідовність $Z_j = \mathrm{Bin}\, k + + X_j$, якщо $0 < k < n$, і яка визначає відображення виду:

$$f_k : X[n,k] \to Z_b;$$

f_w – функція $Y_j = f_w\left(A_j\right)$, яка ставить у відповідність вихідній послідовності A_j упорядковану вибірку виду $\left(k, Y_j\right)$, де $Y_j = A_j$, і визначає відображення виду:

$$f_w : A \to M,$$

$$M = \left\{ \left(k, Y_j\right) / 0 < k < n, Y_j \in Y[n,k] \right\}.$$

У свою чергу, зворотне відображення $f_{bg}^{-1} : Z \to A$, яке задається зворотною складною функцією:

$$f_{bg}^{-1} = \begin{cases} f_w^{-1} \circ f_k^{-1}, \ \left(k=0\right) \vee \left(k=n\right), \\ f_w^{-1} \circ f_b^{-1} \circ f_k^{-1}, \ 0 < k < n, \end{cases} \tag{4.8}$$

є відновлення з урахуванням наявного значення k вихідних двійкових послідовностей A_j. У випадку $0 < k < n$ відновлення A_j зійснюється на основі

$\mathrm{Bin}\,k$ і двійкових (n,k)-біноміальних чисел $X_j \in X[n,k]$, а у випадку $k=0$ або $k=n$ – на основі $\mathrm{Bin}\,k$ шляхом генерування n нулів або одиниць, відповідно.

Способи реалізації складних функцій (4.7), (4.8) на підобласті визначення $k \in \{1,2,...,n-1\}$ для стиснення f_{bg} є аналогічними як для функцій (4.3), (4.4) стиснення f_b на всій області значень k, тобто на всьому діапазоні $0<k<n$. Способи реалізації складних функцій (4.7), (4.8) на підобласті визначення $k \in \{0,n\}$ визначаються простою операцією обчислення k одиниць при стисненні f_{bg} і формуваннямм вихідної нульової або одиничної послідовності A_j при відновленні f_{bg}^{-1}.

З теорем 4.1 і 4.2, які обґрунтовують методи реалізації відповідності, формульованої теоремою 4.3, а також з самої теореми 4.3, слідують моделі процесів узагальненого біноміального стиснення f_{bg} і відновлення f_{bg}^{-1} двійкових послідовностей.

Моделювання процесу стиснення f_{bg} двійкових послідовностей $A_j = a_1a_2...a_i...a_n$, $A_j \in A = \{0,1\}^n$, $j=\overline{1,2^n}$ здійснюється на основі теорем 4.1 і 4.3, функції (4.3) і складається з наступних етапів.

Eman 1. Визначається кількість s розрядів для двійкового представлення $\mathrm{Bin}\,k$ числа k одиниць, $0 \le k \le n$, вихідної n-розрядної послідовності $A_j = a_1a_2...a_i...a_n$:

$$s = \lceil \log_2(n+1) \rceil.$$

Eman 2. Проводиться обчислення числа k двійкових одиниць у вихідній n-розрядній послідовності $A_j = a_1a_2...a_i...a_n$:

$$k = \sum_{i=1}^{n} a_i,$$

тим самим реалізуя функцію $f_w\left(A_j\right) = \left(k, Y_j\right)$ і визначаючи клас рівноважних комбінацій $Y\left[n,k\right]$, до якого відноситься A_j, $A_j = Y_j \in Y\left[n,k\right]$.

Етап 3. Виконується перетворення числа k одиниць до його двійкового виду $\mathrm{Bin}\, k$, який складається з s розрядів.

Етап 4. Якщо число k задовольняє системі рівностей $\left(k = 0\right) \vee \left(k = n\right)$, тобто $k \in \left\{0, n\right\}$, то результуючою буде комбінація виду $Z_j = \mathrm{Bin}\, k$, $Z_j \in Z_o$. У противному випадку наявне значення n і обчисленне значення k являють собою параметри двійкової (n,k)-біноміальної системи числення і здійснюється перехід до подальших етапів для реалізації кодування $f_k\left(f_b\left(Y_j\right)\right) = Z_j$.

Етап 5. Визначається в n-розрядній рівноважній комбінації $Y_j = y_1 y_2 ... y_i ... y_n$, яка має число k одиниць, значення останнього розряду y_n.

Этап 6. Якщо $y_n = 0$, то:

$$X_j = Y_j / 00...0 = y_1 y_2 ... y_i ... y_{n-1} 0 / 00...0 = x_1 x_2 ... x_i ... x_{r-1} 1,$$

тобто від комбінації $Y_j = y_1 y_2 ... y_i ... y_{n-1} 0$ відкидаються всі нульові розряди, починаючи з $y_n = 0$, до появи першої двійкової одиниці $y_r = 1$, яка представлятиме значення останнього розряду $x_r = y_r = 1$ $\left(n,k\right)$-біноміального числа $X_j = x_1 x_2 ... x_i ... x_{r-1} 1$. В іншому випадку:

$$X_j = Y_j / 11...1 = y_1 y_2 ... y_i ... y_{n-1} 1 / 11...1 = x_1 x_2 ... x_i ... x_{r-1} 0,$$

тобто від комбінації $Y_j = y_1 y_2 ... y_i ... y_{n-1} 1$ відкидаються всі одиничні розряди, починаючи з $y_n = 1$, до появи першого двійкового нуля $y_r = 0$, який буде представляти значення останнього розряд $x_r = y_r = 0$ (n,k)-біноміального числа $X_j = x_1 x_2 ... x_i ... x_{r-1} 0$. При цьому в обох випадках значення інших розрядів залишаються без змін: $x_1 = y_1$, $x_2 = y_2$, …, $x_{r-1} = y_{r-1}$.

Этап 7. Виконується конкатенація двійкових значень $\mathrm{Bin}\, k$ і (n,k)-біноміального числа X_j, тобто кодування виду $f_k(X_j) = Z_j$ для випадку $0 < k < n$ або $k \in \{1,2,...,n-1\}$:

$$Z_j = \mathrm{Bin}\, k + + X_j,$$

тим самим отримуючи результуючу комбінацію $Z_j \in Z_b$.

Моделювання процесу відновлення f_{bg}^{-1} послідовностей $A_j = a_1 a_2 ... a_i ... a_n$, $A_j \in A = \{0,1\}^n$, $j = \overline{1,2^n}$ з комбінацій-образів Z_j, $Z_j \in Z_o \cup Z_b$ здійснюється на основі теорем 4.2, 4.3 і функції (4.4). В моделі, яка реалізує f_{bg}^{-1}, в якості основних кроків використовуються етапи з моделі відновлення f_b^{-1} при відомому $\mathrm{Bin}\, k$ і вводяться кроки, які формують послідовності тільки з нулів або тільки з одиниць, коли $k = 0$ або $k = n$ відповідно.

4.6 Аналіз результатів дослідження

Перевагами методів стиснення на основі двійкових біноміальних чисел є наступні.

1. Використання двійкових біноміальних чисел для стиснення дозволяє збільшити продуктивність інформаційних систем. Це відбувається за рахунок зменшення часу передачі стислої інформації та зменшення необхідного

обсягу пам'яті для її зберігання. При цьому коефіцієнти стиснення даних в інформаційній системі є досить високими.

2. Методи стиснення на основі двійкових біноміальних чисел володіють високою швидкодією при низькому рівні апаратно-програмних витрат. Це дозволяє працювати методам в реальному часі, а витрати на їх впровадження є мінімальними.

3. Досліджені методи стиснення мають універсальний характер застосування і спрямовані на обробку поширених двійкових послідовностей, для яких необхідно обчислити тільки кількість одиниць, які містяться в них.

4. Стислі образи, одержувані при стискаючому кодуванні, мають властивості чисел, що дає додатковий позитивний ефект при застосуванні розглянутих методів стиснення. Над ними можна проводити різні арифметичні операції, операції порівняння і упорядкування без відновлення вихідних даних, що є дуже корисною якістю, наприклад, для розподілених баз даних.

Недоліками методів стиснення, які використовують двійкові біноміальні числа є наступні.

1. У разі змінного значення кількості одиниць в двійкових послідовностях необхідно використання службового слова для кожної стислої комбінації з метою її подальшого однозначного відновлення, що трохи знижує ступінь біноміального стиснення.

2. Ступінь стиснення також буде знижуватися і може бути менше одиниці при приблизно рівній кількості двійкових нулів і одиниць, а також при їх рівномірному розташуванні в розрядної сітці послідовностей, що стискаються.

Можливості та перспективи подальших досліджень стиснення на основі двійкових біноміальних чисел є наступні.

1. Виявлення та використання граничних значень числа одиниць, при яких стиснення на основі двійкових біноміальних чисел є доцільним,

дозволить істотно зменшити час кодування і поліпшити ступінь біноміального стиснення.

2. Системи кодоутворюючих обмежень для двійкових біноміальних чисел надають можливість контролювати появу помилок при стисканні двійкових послідовностей, а також при їх передачі по каналу зв'язку і зберіганні в пам'яті. Це дозволяє підвищити завадостійкість інформаційних систем.

4.7 Висновки дослідження

1. Побудовано математичну модель методу стиснення рівноважних комбінацій на основі двійкових біноміальних чисел. Основу отриманої математичної моделі складають теореми 4.1, 4.2 і розроблені моделі процесів біноміального стиснення і відновлення для послідовностей з постійним числом одиниць.

2. Побудовано математичну модель узагальненого біноміального методу стиснення двійкових послідовностей з перемінним числом одиниць. Основу отриманої математичної моделі складають теорема 4.3 і розроблена модель процесу узагальненого біноміального стиснення (модель процесу узагальненого біноміального відновлення грунтується на моделі відновлення для рівноважних комбінацій).

Розроблені моделі процесів стиснення і відновлення на основі двійкових біноміальних чисел характеризуються невеликим числом простих операцій, що забезпечує високу швидкодію кодування і декодування, а також низький обсяг апаратно-програмних витрат.

ВИСНОВКИ

Проведена робота показує, що розроблена телекомунікаційна система дозволяє підвищити всі основні характеристики сучасних телекомунікаційних систем: швидкодію за рахунок стиску інформації, завадостійкість за рахунок використання нероздільних біноміальних кодів і одночасно її скритність. Система передачі має просту структуру і може бути легко реалізована. В той же час вона може надати підвищену ефективність її роботи. Всі ці показники дають можливість рекомендувати розроблену телекомунікаційну систему в практику на підприємствах з передачею числової інформації від датчиків, а також для зняття показників лічильників в комунальній сфері обслуговування.

ПЕРЕЛІКДЖЕРЕЛ ПОСИЛАННЯ

1. Воробей Р.И. Измерительные преобразователи систем оптической диагностики с многофункциональными одноэлементными фотоприемниками / Воробей Р.И., Гусев О.К., Свистун А.И. и др. // Приборы и методы измерений 2018. – Т. 9, № 3. – С. 215–226.

2. Olexiy A. Borysenko and Vyacheslav V. Kalashnikov. Chapter 7: Description and applications of binomial numeral systems complex. – Security and noise immunity of telecommunication systems: new solutions to the codes and signals design problem. Collective monograph. Edited by Sergey G. Rassomahin and Alexandr A. Kuznetsov. – ASC Academic Publishing, Minden, Nevada, USA, 2017. – pp. 147-159.

3. Alexandr A. Kuznetsov, Roman V. Serhiienko, Dmytro I. Prokopovych-Tkachenko and Bakhytzhan S. Akhmetov. Chapter 3: Representation of cascade codes in the frequency domain. – Security and noise immunity of telecommunication systems: new solutions to the codes and signals design problem. Collective monograph. Edited by Sergey G. Rassomahin and Alexandr A. Kuznetsov. – ASC Academic Publishing, Minden, Nevada, USA, 2017. – pp. 71-101.

4. Alexandr A. Kuznetsov, Sergii V. Ksvun, and Yuriy I. Gorbenko. Chapter 4: The methodology of evaluating the energy gains from coding in channels with grouping errors. – Security and noise immunity of telecommunication systems: new solutions to the codes and signals design problem. Collective monograph. Edited by Sergey G. Rassomahin and Alexandr A. Kuznetsov. – ASC Academic Publishing, Minden, Nevada, USA, 2017. – pp. 102-119.

5. Горячев А.Е. Обнаружение ошибок в перестановках / А.Е. Горячев // Вісник СумДУ. Технічні науки. – 2009. – №3. – С. 169 – 174.

6. Борисенко А.А. Обнаружение и исправление ошибок в перестановках / А.А. Борисенко, А.Е. Горячев, Е.Л. Онанченко // Міжнародна науково-практична конференція «Інформаційні технології та комп’ютерна інженерія». – Вінниця: ВНТУ, 2010. – С. 348 – 349.

7. Alexei A. Borisenko, Vyacheslav V. Kalashnikov, Nataliya I. Kalashnykova and Alexey E. Goryachev. Chapter 11: A Generalized Criterion of Efficiency for Telecommunication Systems. – M. Favorskaya and Lakhmi Jain (Eds.), Computer Vision in Advanced Control Systems Using Conventional and Intelligent Paradigms (Springer Series: Intelligent Systems Reference Library, ISSN 1868-4394), Springer-Verlag, Alemania, 2014, vol. 1, pp. 353 – 373. http://www.springer.com/series/8578.

8. Шеннон К. Работы по теории информации и кибернетике. – М.: Иностранная литература, 1963. – 832 с.

9. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд. – М.: Вильямс, 2001. – 672 с.

10. Молдовян А.А. Криптография: скоростные шифры // А.А. Молдовян, Н.А. Молдовян, Н.Д. Гуц, Б.В. Изотов. – СПб.: БХВ-Петербург, 2002. – 244 с.

11. Borisenko A. A. Generation of Permutations Based Upon Factorial Numbers / A. A. Borisenko, V. V. Kalashnikov, I. A. Kulik, A. E. Goryachev // Eighth International Conference on Intelligent Systems Design and Applications. Kaohiung, Taiwan, 2008. – P. 57 – 61.

12. Борисенко А. Факториальные числа в задачах защиты информации / Борисенко А., Горячев А., Сердюк В., Ермаков М. // Безпека інформації, 2018. – Т. 24, № 3. – *С.* 169-174.

13. Matsenko, S., Borysenko, O., Spolitis, S., Bobrovs, V. (2019), “Noise Immunity of the Fibonacci Counter with the Fractal Decoder Device for Telecommunication Systems”, Latvian Journal of Physics and Technical Sciences, Riga, Latvia, Vol. 56, No. 5, pp. 12-21.

14. Борисенко О.А. Система передачі та відображення інформації із захистом числових даних / О.А. Борисенко, О.В. Бережна, А.І. Новгородцев, В.В. Сердюк, М.М. Яковлев // Системи обробки інформації. – 2019. – Вип. 2. – С. 103-108.

15. Про особливості шифрування в розподілених системах відображення числових даних / О.А. Борисенко, О.В. Бережна, М.М. Яковлев, О.О. Рахма-толь, М.С. Фурса // Фізика, електроніка, електротехніка (ФЕЕ-2019): матеріали та програма науково-технічної конференції. – Суми, 23-26 квітня 2019 р. / СумДУ. – Суми, 2019. – С. 90.

16. Борисенко А.А. Оценка помехоустойчивости системы передачи данных на основе равновесных кодов / А.А. Борисенко, О.В. Бережная, И.А. Кулик // Вісник Сумського державного університету. – 1999. – №1. – С. 79-82.

17. Оценка помехоустойчивости систем передачи данных на основе кодов с постоянным весом / О.А. Борисенко, О.В. Бережна, А.І. Новгородцев, В.В. Сердюк, М.М. Яковлев // Інформаційна безпека та інформаційні технології: матеріали Міжнародної науково-практичної конференції. – Харків, 24-25 квітня 2019 р. / ХНЕУ імені Семена Кузнеця. – Харків, 2019. – С. 23.

18. Борисенко А.А. Биномиальный счет. Теория и практика: Монография / А.А. Борисенко. – Сумы: ИТД "Университетская книга", 2004. – 170 с

19. Борисенко А.А. Биномиальный счет и счетчики: Монография / А.А. Борисенко. – Сумы: Изд-во СумГУ, 2008. – 152 с.

20. Рейнгольд Э., Нивергельд Ю. Комбинаторные алгоритмы. Теория и практика / Э. Рейнгольд, Ю. Нивергельд. – М.: Мир, 1980. – 476 с.

21. Цымбал В.П. Теория информации и кодирование / В.П. Цымбал. – К.: Вища шк., 1992. – 263 с.

22. Sayood Kh. Introduction to Data Compression / Kh. Sayood. – Morgan Kaufmann, 2017. 5 edition. – 790 p.

23. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео / Ватолин Д. и др. – М.: ДИАЛОГ-МИФИ, 2003. – 384 с.

24. Смирнов М.А. Обзор применения методов безущербного сжатия данных в СУБД / М.А. Смирнов. URL: http://compression.ru/download/articles/ db/smirnov_2003_ database_compression_review.pdf.

25. Sayood Kh. Lossless Compression Handbook / Kh. Sayood. – Academic Press, 2012. – 488 p.

26. Борисенко О.А. Число і системи числення в електронних цифрових система / О.А. Борисенко // Вісник СумДУ, 2007. – № 4. – С. 71–76.

27. Борисенко А.А. Биномиальное кодирование: монография / А.А. Борисенко, И.А. Кулик. – Сумы: Изд-во СумГУ, 2010. – 206 с.

28. Кулик И.А. Алгоритм генерирования двоичных биномиальных чисел на основе минимальных систем кодообразующих ограничений / И.А. Кулик, В.Б. Чередниченко, С.В. Костель // Вісник СумДУ. Серія «Технічні науки», 2008. – № 2. – С. 45–52.

29. Pieter J. An Algorithm for Source Coding / J. Pieter, M. Schalkwijk // IEEE Transact. on Information Theory. 1972. – Vol. IT-18, No. 3. – P. 395–399.

30. Cover M. Thomas. Enumerative Source Coding / Thomas M. Cover // IEEE Transactions on Information Theory. 1973. – Vol. IT-19, No. 1. – P. 73–77.

31. Амелькин В.А. Методы нумерационного кодирования / В.А. Амелькин. – Новосибирск: Наука, 1986. – 155 с.

32. Амелькин В.А. Перечислительные задачи серийных последовательностей / В.А. Амелькин. – Новосибирск: ИВМиМГ СО РАН, 2008. – 317 с.

33. Кулик И.А. Модели сжатия и восстановления данных на основе двоичных биномиальных чисел / И.А. Кулик, А.А. Борисенко, Аджири Ониуке // V Міжнар. наук.-практ. конференція «Методи та засоби кодування, захисту й ущільнення інформації», 19-21 квітня 2016 р.: тез. доп. Вінниця: Вінницький національний технічний університет, 2016. – С. 101–105.

34. Кулик И.А. Генерирование кодов-сочетаний для решения информаци-онных задач ИУС / И.А. Кулик, Е.М. Скордина, С.В. Костель // АСУ и приборы автоматики. Всеукраинский межведомственный сборник. 2011. – № 155. –С. 15–23.

35. Combinatorial Algorithms: Theory and Practice / Greenfield T. et al. // The Statistician. 1978. – Vol. 27, No. 2. – P. 138. doi: https://doi.org/10.2307/2987917.