ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ В. Н. КАРАЗІНА
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

Кошман Сергій Олександрович
(прізвище, ім'я, по батькові)

УКД 681.004.38
(індекс)

ДИСЕРТАЦІЯ

МЕТОДИ ТА ЗАСОБИ ОПЕРАТИВНОГО КОНТРОЛЮ ТА ДІАГНОСТИКИ ДАНИХ КОМПОНЕНТІВ КОМП'ЮТЕРНОЇ СИСТЕМИ У ЗАЛИШКОВИХ КЛАСАХ

(назва дисертації)

05.13.05 – Комп'ютерні системи та компоненти
(шифр, назва спеціальності)

Технічні науки
(галузь знань)

Подається на здобуття наукового
ступеня доктора технічних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____С. О. Кошман
(підпис, ініціали та прізвище здобувача)

Науковий консультант
Краснобаєв Віктор Анатолійович, доктор технічних наук, професор.

Харків – 2018

АНОТАЦІЯ

Кошман С. О. Методи та засоби оперативного контролю та діагностики даних компонентів комп'ютерної системи у залишкових класах. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.05 – Комп’ютерні системи та компоненти. – Харківський національний університет імені В.Н. Каразіна Міністерства освіти і науки України, Харків, 2018.

В ході досліджень було проведено аналіз сучасних науково-технічних областей та направлень де існує необхідність у швидких цілочислових арифметичних обчисленнях. Визначено, що зростаюча складність та обсяги обчислювальних задач вимагають необхідності істотного підвищення швидкодії реалізації арифметичних операцій. Результати досліджень методів підвищення швидкодії комп'ютерних систем і компонентів обробки цілочислових даних (КСКОЦД) показали, що в межах позиційних систем числення (ПСЧ) кардинального підвищення швидкодії досягти неможливо. Це обумовлено, в першу чергу, наявністю у ПСЧ міжрозрядних зв'язків між числами, що оброблюються. Всі перераховані обставини привели численну групу вчених таких як Акушський І. Я., Юдицький Д. І., Ніколайчук Я. М., Глушков В. М., Черв'яков Н. І., William Jenkins, Amos Omondi, Bin Yan та багатьох інших в області обчислювальної техніки, звернутися до непозиційної системи числення у залишкових класах (СЗК). На основі результатів аналізу було визначено, що на сьогоднішній день вже вирішені основні теоретичні питання СЗК і розроблено математичний апарат для створення швидкодіючих комп'ютерних систем та компонентів. Отримано ряд позитивних результатів не тільки в теоретичному плані, але і в практичному використанні СЗК. Однак результати досліджень показали, що до теперішнього часу існує невирішена проблема побудови ефективної системи оперативного контролю та діагностики даних у СЗК. Відсутність

постановки і результатів вирішення цієї проблеми стримує широкі потенційні можливості швидкої обробки даних, що закладені у властивостях СЗК. Ця обставина породжує протиріччя між високою швидкодією реалізації цілочислових арифметичних операцій і низькою оперативністю контролю і діагностики даних. Результати аналізу сучасних тенденцій розвитку комп'ютерних систем і компонентів, що функціонують у СЗК підтверджують наявність наступної конфліктної ситуації. З одного боку, між існуючою можливістю значного підвищення швидкодії виконання цілочислових арифметичних операцій, а з іншого боку, низькою оперативністю існуючих методів і засобів контролю та діагностики результатів обчислень, за рахунок значного часу реалізації перерахованих процедур. Тому розробка методів оперативного контролю та діагностики даних, що представлені у СЗК, дозволить усунути існуюче протиріччя при побудові КСКОЦД. Наукові результати розташовані наступним чином.

У першому розділі проведено дослідження областей науки, що вимагають швидку та достовірну реалізацію цілочислових обчислень, та показано, що використання СЗК, як системи числення КСКОЦД дозволяє значно підвищити ефективність їх функціонування. Приведено аналіз задач, які оперують з цілочисловими даними. Досліджено існуючі методи забезпечення оперативного контролю та діагностики даних. Результати аналізу цих методів показали, що вони не завжди задовольняють вимогам по забезпеченню високої оперативності контролю і діагностики даних. Сформульовано концепцію розвитку швидкодіючих КСКОЦД представлених у СЗК, яка полягає у розробці та застосуванні методів і засобів оперативного контролю та діагностики помилок даних.

У другому розділі роботи сформульовано та досліджено принципи побудови непозиційних кодових структур (НКС) у СЗК, виходячи з яких проведено аналіз основних властивостей СЗК. Дослідження впливу властивостей СЗК на структуру та процес функціонування КСКОЦД показали, що застосовування кодів у залишкових класах ефективне для

вирішення певного класу задач. Причому, поєднання комбінованого застосування СЗК та двійкової ПСЧ при побудові спеціалізованих комп'ютерних систем, може привести до підвищення продуктивності КСКОЦД у цілому. Тобто керування всією комп’ютерною системою може здійснюватися у двійковому коді, а обробка даних буде виконується на основі представлення чисел у коді СЗК. Виходячи з аналізу властивостей СЗК, розглянуто принципи реалізації основних арифметичних операцій над числами які представлені системою зі взаємно простими основами. При цьому використання властивостей СЗК дає можливість широкого вибору принципів, методів та варіантів системотехнічних рішень при створенні КСКОЦД. Також з аналізу основних властивостей СЗК можна зробити висновок, що КСКОЦД у СЗК, можна віднести до об'єктів, що легко контролюються та діагностуються. Тобто особливості структури та принципи функціонування КСКОЦД у СЗК дозволяють розробляти ефективні методи контролю та діагности помилок даних, що не мають аналогів у ПСЧ. Однак недостатня оперативність процедур діагностики помилок даних у СЗК, обумовлює необхідність вдосконалення існуючих та розробку нових методів контролю та діагностики помилок даних.

У третьому розділі проведено дослідження коригувальних властивостей непозиційних кодових структур у СЗК. Виходячи з аналізу основних положень теорії завадостійкого кодування даних для оцінки ефективності будь-якого коригувального коду необхідно знати зв'язок між надмірністю і можливостями виявляти і виправляти помилки. Для визначення коригувальних можливостей кодів у залишкових класах найчастіше використовують поняття мінімальної кодової відстані $d_{\min}$ між будь-якими двома векторами (числами) A_1 і A_2 з множини числа компонент M, в яких ці вектори відрізняються один від одного. Тобто двом сусіднім числам A_1 і A_2 (що відрізняється на одиницю) відповідають вектори A_1 і A_2, відстань між якими дорівнює довільній основі m_i для заданої СЗК. До тож у

СЗК інформаційна і контрольна частини векторів рівноправні щодо реалізації арифметичних операції. У даному розділі показано, що мінімальна кодова відстань коригуючого коду в СЗК залежить від кількості та величини додатково введених контрольних основ. Збільшити значення мінімальної кодової відстані можна також за рахунок зменшення числа n інформаційних основ, тобто за рахунок переходу до обчислень з меншою точністю, але з більш високими коригувальними можливостями по контролю та діагностиці помилок даних. Практичні результати досліджень коригувальних можливостей непозиційного коду показали, що при виконанні певних умов, введення тільки однієї контрольної основи, дозволяє не тільки виявляти, але і виправляти виникаючі помилки. Також у розділі представлені аналітичні вирази для визначення коригувальних можливостей НКС. Для подальшої розробки методу контролю даних у СЗК розглянуто метод формування позиційної ознаки НКС.

У четвертому розділі сформульовано принципи контролю непозиційних кодових структур у СЗК. Проаналізовано існуючі методи контролю даних у СЗК, які засновані на процедурі нульвизаціїї та показано, що вони мають значний час реалізації процедури нулевізації, та не вичерпують можливості підвищення швидкодії реалізації процедури нулевізації чисел. На основі сформульованих принципів контролю, у відповідності з поставленими частковими задачами досліджень, вперше отримано метод контролю даних у системі залишкових класів, який на відміну від відомих, заснований на принципі паралельної нульовизації, шляхом поєднання у часі операцій нульовизації симетричних залишків НКС, що контролюється та визначення констант нульовизації, що дозволяє підвищити оперативність контролю даних. Цей метод, у порівнянні з існуючими методами, дозволяє, залежно від довжини машинного слова КСКОЦД, підвищити до 60 % оперативність контролю даних.

В ході досліджень, вперше отримано метод контролю даних у системі залишкових класів, який на відміну від відомих, заснований на використанні

позиційної ознаки непозиційної кодової структури, шляхом паралельного віднімання встановлених констант, що дозволяє підвищити оперативність контролю даних. Цей метод дозволяє зменшити кількість констант, що визначаються у записі однорядкового коду $K_{N_i}^{(n_A)} = \left\{ Z_{N_i-1}^{(A)} \; Z_{N_i-2}^{(A)} \ldots Z_1^{(A)} \; Z_0^{(A)} \right\}$. Цей дало змогу, у порівнянні з існуючими методами, підвищити оперативність контролю даних представлених у СЗК до 60 %.

Під час досліджень вперше отримано метод підвищення достовірності оперативного контролю даних, що представлені у системі залишкових класів, який на відміну від відомих, заснований на використанні позиційної ознаки непозиційної кодової структури, шляхом застосування відповідної основи, що кратна загальному модулю системи залишкових класів, це підвищує достовірність контролю даних. Даний метод дозволяє підвищити достовірність контролю даних в залежності від значення контрольної основи до 4%.

У п’ятому розділі на підставі проведених досліджень та часткових задач вдосконалено метод визначення альтернативної сукупності непозиційної кодової структури у системі залишкових класів, який заснований на використанні функції відповідності значень можливих помилок, шляхом зменшення кількості основ, що перевіряються, які входять в альтернативну сукупність чисел, що підвищує оперативність діагностики помилок даних. Використання вдосконаленого методу дозволяє підвищити оперативність діагностики помилок до 60% в порівнянні з існуючими методами.

Вдосконалено метод оперативної діагностики даних, що представлені у системі залишкових класів, який заснований на формуванні числових інтервалів та ознак даних квадрантів знаходження альтернативних сукупностей чисел, шляхом згортки таблиці відповідності значень можливих помилок, це зменшує час вибірки основ, що перевіряються та підвищує оперативність діагностики помилок даних. Проведені розрахункові

результати показали, що розроблений метод дозволяє підвищити оперативність діагностики помилок даних у залежності від величини розрядної сітки до 19%.

У шостому розділі описані теоретичні основи корекції помилок даних у СЗК. На основі теоретичних положень корекції НКС, представлені методи виправлення помилок у СЗК. Показано, що ці методи засновані на використанні як взаємно простих (R–коди), так і взаємно непростих (L–коди) основ. За результатами аналізу представлених методів корекції НКС показано, що методи які представлені R–кодами, дозволяють за рахунок паралельного виправлення помилок, у ρ раз підвищити оперативність корекції помилок у СЗК (де ρ – кількість можливих залишків НКС, у яких відбулися помилки). Результати досліджень показали, що використання L-кодів, дозволяє розширити клас помилок, що коректуються, це у свою чергу розширює коригувальні можливості L-кодів у СЗК.

Отримані в роботі результати дозволили вирішити наукову-технічну проблему розробки методів оперативного контролю та діагностики даних компонентів комп'ютерної системи, що функціонують у залишкових класах.

Ключові слова

Система числення, система залишкових класів, непозиційна кодова структура, комп'ютерні системи та компоненти обробки цілочислових даних, контроль та діагностика даних, достовірність контролю даних, нульовизація чисел, однорядковий код, паралельна обробка даних.

ABSTRACT

Serhii O. Koshman. Methods and tools for operative data verification and diagnosis of computer system components in residue classes. – Qualification scientific paper, manuscript.

Thesis for a Doctoral Degree in Technology: Specialty 05.13.05 – computer systems and components (Technology). – V. N. Karazin Kharkiv National

University, the Ministry of Education and Science of Ukraine, Kharkiv, 2018.

As a part of study the analysis of modern scientific and technical fields with a necessity in high-speed integer computations was conducted. It was determined that increasing amounts and complexity of computational tasks require significant improvement in processing speed of the arithmetic operations implementation. The research results for improving the operation speed of computer systems and components of integer data processing (CSCIDP) has shown, that in the scope of positional numeral system (PNS) it is impossible to achieve significant rise in computational speed. This is primarily due to the inter-digit relations of the processed numbers in PNS. All of the mentioned factors led the numerous group of scientists, such as I. Akushskiy, D. Yuditzkiy, J. Nikolaichuk, V. Glushkoff, N. Chervyakov, William Jenkins, Amos Omondi, Bin Yan and many others in the computational field to turn their attention towards the non-positional residue classes (RNS) numeral system. Based on the result analysis it was found, that for the present moment main theoretical problems in RNS had been solved and mathematical tool for the high-speed computer system and components construction was developed. The series of positive takes in theoretical realm were obtained, as well as in practical usage of RNS. However the analysis results has shown, that there is yet unsolved problem of constructing effective data control and verification system in RNS. The lack of missioning and results for solving this problem inhibits broad potential of high-speed data processing, which is contained in RNS properties. This fact gives rise to the conflict between a high speed integer arithmetic operations implementation and a slow data control diagnosis and verification. The result analysis of modern trends of computer systems and components development operating in RNS supports the presence of the mentioned conflict. On the one hand because of the existing possibility of significant boost of integer arithmetic operations execution, and on the other hand because of a low efficiency of existing methods and techniques of data diagnosis and verification, due to the significant amounts of time, needed for implementing mentioned procedures.

This is why the development of operative RNS data diagnosis and verification allows to eliminate existing contradictions during the construction of CSCIDP. Obtained scientific results are present in the following order.

In the first chapter scientific fields that require fast and reliable integer calculations execution has been researched, and it was shown that RNS implementation as a CSCIDP number system leads to a significant boost in the performance. The analysis of tasks that work with integer data was made. Existing methods for providing operative data diagnosis and verification has been researched. The analysis of these methods has shown, that they do not meet the requirements for providing efficient data diagnosis and verification all of the time. The concept of high-speed CSCIDP development in RNS was defined, which involves development and implementation of methods and techniques for operative data error diagnosis and verification.

In the second chapter of the paper the principles of non-positional code structure (NCS) construction in RNS were defined and researched, basing on which the analysis of main RNS properties was made. The research of RNS properties impacting the structure and the process of operation of CSCIDP has shown that applying residue classes codes is effective for solving a certain spectrum of tasks. Besides, combining the usage of RNS and binary PNS, while constructing specialized computer systems, can lead to the overall boost of CSCIDP efficiency. In other words, the computer system can be controlled using binary code, while data processing will be based on number representation as an RNS code. Based on the analysis of RNS properties, the principle of fundamental arithmetic operations implementation over the numbers, being represented in a coprime basis system, was reviewed. Herewith the utilization of RNS properties gives a broad spectrum of principles, methods and variants of circuit engineering during CSCIDP construction. Additionally, form the analysis of main RNS properties the conclusion can be made, that CSCIDP in RNS can be related to the easily diagnosable and verifiable objects. This means that structural specifics and functional principles of CSCIDP in RNS allow developing of effective methods for

data error diagnosing and verification, that is unparalleled in PNS. But due to the lack in efficiency of data error diagnosing procedures in RNS, it's required to enhance existing and to develop new data error diagnosing and verification methods.

In chapter three the research of non-positional code structures in RNS repairing properties was made. Based on the analysis of fundamental principles of the error control code theory, in order to estimate the efficiency of any error-control code you need to know the correlation between information redundancy and the ability to detect and repair errors. In order to define correcting capabilities of the codes in residue classes, the concept of minimal code distance $d_{\min}$ between any two vectors (numbers) A_1 and A_2 from the set of components *M*, where these vectors differentiate, is most commonly used. Thus for two adjacent numbers A_1 and A_2 (that differ for a single figure) corresponding vectors are A_1 and A_2, that are distanced equivalently to the arbitrary base m_i for a chosen RNS. In addition both informational and control parts of vectors are equivalent with respect to arithmetic operations implementation in RNS.

This chapter show, that minimal code distance of RNS correcting code depends on the quantity and size of additionally introduced control bases. Minimal code distance incrimination is also possible by decreasing the number n of informational bases, i.e. switching to less accurate computations, but with higher correcting capabilities of data error diagnosis and verification. Practical results of correcting capabilities of non-positional code have shown, that by satisfying certain conditions, introduction of a single control base allows not only to detect, but also to repair occurring errors. As well this chapter contains analytical expressions to determine correcting capabilities of NCS. For further development of RNS data control method the forming method of positional NCS signs was reviewed.

In the fourth chapter the principles of RNS non-positional code structures verification were formulated. Existing methods of RNS data verification, based on

nullification procedure, were analyzed, and it was shown that they require significant nullification procedure implementation time and do not exhaust the potential of number nullification procedure operating speed boost. Based on the formulated verification principles, according to partly stated research tasks, for the first time the method of data verification in residue classes was obtained, that compared to known ones is based on the principle of parallel nullification, by combining in time the nullification operations for NCS symmetrical residues under control and determining nullification constants, which in turn allows to boost data verification efficiency. This method, if compared to other existing methods, depending on the length of CSCIDP computer word allows to boost data verification efficiency for up to 60%.

During the research the method of RNS data verification was obtained for the first time, that when compared to a known ones is based on the utilization of positional signs of a non-positional code structure through the process of parallel subtraction of earlier determined constants, which in turn allows data verification efficiency boost. This method allows to decrease the number of constants, that are being determined in the single-line code expression $K_{N_i}^{(n_A)} = \{Z_{N_i-1}^{(A)} Z_{N_i-2}^{(A)} \ldots Z_1^{(A)} Z_0^{(A)}\}$. In comparison to existing methods, it allowed to boost RNS data verification efficiency for up to 60%.

During the research the method for increasing operative RNS data verification certainty was obtained for the first time, that is unlike known methods is based on the usage of positional signs of the non-positional code structure, by applying the corresponding base, divisible by general residue numeral system module, which in turn increases data control certainty. Given method allows increasing data control certainty depending on the value of control base up to 4%.

In the fifth chapter, based on the performed researches and partial tasks the method for the alternative set of the non-positional code structure determining in residue numeral system was improved, which involves the adherent function for the values of possible errors usage, by reducing amount of bases being controlled, that are being a part of alternative number set, which in turn boosts the data error

verification efficiency.

Implementation of the improved method allows increasing data error verification for up to 60% in comparison to existing methods.

The method for operative data diagnosis in residue classes numeral system was improved, which is based on formation of number intervals and signs of given quadrants of the alternative number set location, by folding the table of corresponding values of possible errors, which reduces time needed for the selection of bases being controlled and boosts data error diagnosis efficiency. Calculated results have shown that the developed method allows boosting the efficiency of data error diagnostics for up to 19% depending on the value of the bit grid.

In the sixth chapter theoretical basis of RNS data error correction was described. Based on the theoretical principles of NCS correction, the methods of errors reparation in RNS were introduced. It was shown, that these methods are based on the usage of coprime (R-codes), as well as complex (L-codes) bases. According to the results of the introduced NCS correction methods' analysis shown, that methods being represented with R-codes by utilizing parallel error correction allow increasing error correction efficiency in ρ times for RNS (where ρ is the amount of possible NCS residues, holding occurred errors). Research results have shown that L-code utilization allow to expand error class being corrected, which in turn enhances L-code correction capabilities in RNS.

The obtained results allowed solving scientific-and-technological problem of operative data diagnosis and verification methods of computer system and components that operate in residue classes.

Key words:

Numeral system, numeral system in residue classes, non-positional code structure, computer systems and components of integer data processing, data control and verification, data verification reliability, numbers nullification, single-line code, parallel data processing.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації

Монографії:

1. Кошман С. А., Краснобаев В. А., Мороз С. А., Курчанов В. Н., Янко А. С. Модели и методы обработки данных в системе остаточных классов: монография. Харьков: ООО "В деле", 2017. 197 с. (*Особистий внесок здобувача: розроблено методи обробки даних, що представлені у СЗК*).

2. ISCI'2017: Information Security in Critical Infrastructures: monograph: / Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov. ASC Academic Publishing, USA, 2017. 207 p. (*Особистий внесок здобувача: розроблено методи обробки даних, що представлені у СЗК*).

3. Koshman S., Krasnobayev V., Kuznetsov A., Rassomakhin S., Zamula A., Kavun S. Effective Data Processing in Coding, Digital Signals and Cryptography: monograph. ASC Academic Publishing, 2018. 352 p. (*Особистий внесок здобувача: розроблено методи обробки даних, що представлені у СЗК*).

Публікації у фахових виданнях України:

4. Кошман С. А. Концепция создания системы обработки цифровой информации на основе использования системы остаточных классов // Радіоелектронні і комп'ютерні системи. 2010. № 7 (48). С. 138-141.

5. Кошман С. О. Метод реалізації арифметичних операцій у системі залишкових класів // Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка. Проблеми енергозабезпечення та енергозбереження в АПК України. 2010. Вип. 102. С. 77-79.

6. Кошман С. А., Загумённая Е. В. Анализ особенностей функционирования автоматизированной системы управления

турбоустановками // Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка. Проблеми енергозабезпечення та енергозбереження в АПК України. 2011. Вип. 116. С. 117-120. (*Особистий внесок здобувача: досліджені особливості проектування КСКОЦД реального часу*).

7. Кошман С. О. Концепція підвищення продуктивності обробки інформації у реальному часі // Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка. Проблеми енергозабезпечення та енергозбереження в АПК України. 2011. Вип. 117. С. 63-65.

8. Кошман С. А., Краснобаев В. А., Маврина М. А. Методы оптимального резервирования в модулярной системе счисления // Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка. Проблеми енергозабезпечення та енергозбереження в АПК України. 2012. Вип. 129. С. 105-108. (*Особистий внесок здобувача: вдосконалено метод оптимального резервування КСКОЦД у СЗК*).

9. Загумённая Е. В., Кошман С. А., Маврина М. А., Краснобаев В. А. Метод арифметического сравнения чисел в классе вычетов // Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка. Проблеми енергозабезпечення та енергозбереження в АПК України. 2012. Вип. 130. С. 72-75. (*Особистий внесок здобувача: розроблено метод арифметичного порівняння чисел у СЗК*).

10. Краснобаев В. А., Маврина М. А., Кошман С. А. Контроль, диагностика и исправление ошибок данных, представленных кодом класса вычетов // Системи обробки інформації: збірник наукових праць. Харків. 2013. № 2(109). С. 48-54. (*Особистий внесок здобувача: досліджено коригувальні властивості кодів, що представлені у СЗК*).

11. Краснобаев В. А., Маврина М. А., Кошман С. А., Курчанов В. Н. Концепция создания компьютерных средств обработки данных на основе использования кодов класса вычетов // Системи обробки інформації: збірник

наукових праць. Харків. 2013. № 4(111). С. 133-138. (*Особистий внесок здобувача: досліджено особливості застосування кодів у СЗК при побудові КСКОЦД*).

12. Кошман С. А., Краснобаев В. А., Сомов С. В., Крючко Е. А. Метод быстрой обработки криптографической информации в модулярной системе счисления // Системи обробки інформації: збірник наукових праць. Харків. 2013. № 6(113). С. 194-198. (*Особистий внесок здобувача: розроблено метод швидкої обробки інформації, що представлена у СЗК*).

13. Кошман С. А., Краснобаев В. А., Тыртышников А. И., Гаркавенко Н. С. Концепция создания отказоустойчивых компьютерных систем обработки информации в системе остаточных классов на основе применения ПЛИС // Системи обробки інформації: збірник наукових праць. Харків. 2013. № 7(114). С. 79-82. (*Особистий внесок здобувача: досліджено шляхи підвищення продуктивності та достовірності обробки даних у КСКОЦД)*.

14. Краснобаев В. А., Кошман С. А., Курчанов В. Н., Гарамась А. В. Метод контроля криптографической информации, представленной в модулярной системе счисления // Збірник наукових праць Харківського університету Повітряних Сил ім. І. Кожедуба. Харків. 2013. Вип. 3(36). С. 104-107. (*Особистий внесок здобувача: розроблено метод контролю, який заснований на принципі нульовизації даних у СЗК*).

15. Краснобаев В. А., Кошман С. А., Маврина М. А. Метод исправления однократных ошибок данных, представленных кодом класса вычетов // Электронное моделирование. 2013. Том 35, № 5. С. 43-56. (*Особистий внесок здобувача: вдосконалено метод виправлення одноразових помилок даних у СЗК*).

16. Краснобаев В. А., Кошман С. А., Маврина М. А. Метод повышения достоверности контроля данных, представленных в системе остаточных классов // Кибернетика и системный анализ. 2014. Том. 50, № 6. С. 167-175. (*Особистий внесок здобувача: дано обґрунтування низької*

достовірності контролю даних представлених у СЗК).

17. Koshman S. A., Krasnobayev V. A., Tyrtyshnikov O. I., Sliusar I. I., Kurchanov V. N. The model and the method of implementation of integer arithmetic operations within the RSA crypto algorithms // Системи обробки інформації: збірник наукових праць. Харків. 2014. № 1(117). С. 117-122. (*Особистий внесок здобувача: вдосконалено метод реалізації цілочислових арифметичних операцій)*.

18. Кошман С. А., Краснобаев В. А., Янко А. С. Математические модели и алгоритмы возведения целых чисел в квадрат по произвольному модулю класса вычетов // Збірник наукових праць Харківського університету Повітряних Сил. Харків. 2014. Вип. 1(38). С. 132-137. (*Особистий внесок здобувача: вдосконалені математичні моделі піднесення цілих чисел у квадрат за довільним модулем класу лишків)*.

19. Krasnobayev V. A., Tyrtyshnikov O. I., Somov S. V., Koshman S. A., Sokol G. V., Rvachova N. V. Mathematical model and tabular method implementation of modular arithmetic operations with crypto transformations in the residue class // Системи обробки інформації: збірник наукових праць. Харків. 2014. № 2(118). С. 119-123. (*Особистий внесок здобувача: вдосконалено метод табличної обробки даних у СЗК)*.

20. Краснобаев В. А., Янко А. С., Кошман С. А. Метод табличной реализации операции умножения в классе вычетов // Системи обробки інформації: збірник наукових праць. Харків. 2014. № 4(120). С. 121-127. (*Особистий внесок здобувача: вдосконалено метод реалізації арифметичних операцій у СЗК*).

21. Кошман С. А., Краснобаев В. А., Чернецкая И. А., Мартыненко А. М. Метод обработки данных в классе вычетов // Збірник наукових праць Харківського університету Повітряних Сил. Харків. 2014. Вип. 2(39). С. 121-126. (*Особистий внесок здобувача: вдосконалено метод обробки даних у СЗК*).

22. Краснобаев В. А., Янко А. С., Гроза П. Н., Кошман С. А.,

Гроза А. П., Бендес Ю. П. Расчет и сравнительный анализ производительности компьютерной системы обработки целочисленных данных, функционирующей в системе остаточных классов // Системи обробки інформації: збірник наукових праць. Харків. 2015. № 1(126). С. 111 - 117. (*Особистий внесок здобувача: проведено розрахунок продуктивності комп'ютерних систем у СЗК*).

23. Краснобаев В. А., Янко А. С., Кошман С. А., Сомов С. А., Бендес Ю. П. Исследование производительности компьютерной системы обработки целочисленных данных, функционирующей в системе остаточных классов // Збірник наукових праць Харківського університету Повітряних Сил. Харків. 2015. Вип. 1(42). С. 48-52. (*Особистий внесок здобувача: виведені аналітичні вирази для розрахунку продуктивності комп'ютерних систем обробки цілочислових даних у СЗК*).

24. Краснобаев В. А., Янко А. С., Кошман С. А., Курчанов В. Н., Бендес Ю. П. Расчет и сравнительный анализ производительности компьютерной системы обработки целочисленных данных, представленных в системе остаточных классов // Системи обробки інформації: збірник наукових праць. Харків. 2015. Вип. 3(128). С. 57-61. (*Особистий внесок здобувача: досліджено вплив властивостей СЗК на продуктивність комп'ютерних систем*).

25. Краснобаев В. А., Янко А. С., Кошман С. А. Метод возведения остатков целых чисел по произвольному модулю системы остаточных классов в степень натурального числа // Радіоелектронні і комп'ютерні системи. Харків. 2015. № 1(71). С. 54–63. (*Особистий внесок здобувача: розроблено метод піднесення залишків за довільним модулем СЗК у ступінь натурального числа)*.

26. Krasnobayev V. A., Yanko A. S., Kurchanov V. N., Koshman S. A. The analysis of the tasks and algorithms of data integer processing in the residual classes system // Радіоелектронні і комп'ютерні системи. 2016. № 1 (75). С. 19-28. (*Особистий внесок здобувача: проведено аналіз задач та алгоритмів*

реалізації цілочислових арифметичних операції у СЗК).

27. Краснобаев В. А., Янко А. С., Кошман С. А. Метод арифметического сравнения данных, представленных в системе остаточных классов // Кибернетика и системный анализ. 2016. Том. 52, № 1. С. 157–162. (*Особистий внесок здобувача: вдосконалено метод арифметичного порівняння даних у СЗК*).

28. Краснобаев В. А., Кошман С. А., Янко А. С. Метод оперативного контроля данных в системе остаточных классов, основанный на принципе последовательной нулевизации // Радіоелектронні і комп'ютерні системи. 2017. № 1 (81). С. 57-68. (*Особистий внесок здобувача: розроблено метод оперативного контролю даних у СЗК на основі принципу нульовизації)*.

29. Кошман С. А., Краснобаев В. А. Метод оперативного диагностирования данных, представленных в системе остаточных классов // Кибернетика и системный анализ. 2018. Том. 54, № 2. С. 182–192. (*Особистий внесок здобувача: розроблено метод оперативного діагностування даних у СЗК*).

***Наукові праці, в яких опубліковані основні наукові результати дисертації у зарубіжних спеціалізованих виданнях*:**

30. Krasnobayev V. A., Koshman S. A. Method of realization of cryptographic RSA transformations on the basis of application of modular number system // International Journal of Biomedical Soft Computing and Human Sciences. 2011. Vol. 17, № 2. P. 31-36. (*Особистий внесок здобувача: вдосконалення методу реалізації криптографічних перетворень на основі використання СЗК*).

31. Krasnobayev V. A., Koshman S. A., Mavrina M. A. A method for increasing the reliability of verification of data represented in a residue number system // Cybernetics and Systems Analysis. November 2014. Vol. 50, Issue 6. P. 969-976. (*Особистий внесок здобувача: розроблено метод підвищення*

достовірності контролю даних представлених у СЗК). (Видання входить до міжнародної наукометричної бази Scopus).

32. Краснобаев В. А., Янко А. С., Бендес Ю. П., Кошман С. А. Метод контроля данных в системе остаточных классов // Оралдын Гылым Жаршысы (Уральский научный вестник): Научно-теоретический и практический журнал. Уральск (Казахстан): ТОО "Уралнаучкнига", 2015. Вып. 5(136). С. 103-117. (*Особистий внесок здобувача: удосконалено метод контролю даних у СЗК)*.

33. Krasnobayev V. A., Yanko A. S., Koshman S. A. The method of error correction in the system of residual classes // Nauka i studia. 2015. NR 5(136). P. 51-62. (*Особистий внесок здобувача: досліджено методи корекції помилок даних у СЗК*).

34. Krasnobayev V. A., Yanko A. S., Koshman S. A. Method for arithmetic comparison of data represented in a residue number system // Cybernetics and Systems Analysis. January 2016. Vol. 52, Issue 1. P. 145-150. (*Особистий внесок здобувача: вдосконалено метод арифметичного порівняння даних у СЗК*). (Видання входить до міжнародної наукометричної бази Scopus).

35. Koshman S. A., Krasnobayev V. A. A method for operational diagnosis of data represented in a residue number system // Cybernetics and Systems Analysis. March 2018. Vol. 54, Issue 2. P. 336-344. (*Особистий внесок здобувача: розроблено метод оперативного діагностування даних у СЗК*). (Видання входить до міжнародної наукометричної бази Scopus)

Патенти:

36. Пристрій додавання і віднімання чисел за модулем *m* модулярної системи числення на основі кільцевого зсуву: пат. 55454 Україна. № u 2010 08060; заявл. 29.06.2010; опубл. 10.12.2010, Бюл. № 23. 4 с. (*Особистий внесок здобувача: алгоритм роботи пристрою для додавання і віднімання чисел за модулем m модулярної системи числення на основі кільцевого зсуву*).

37. Пристрій для додавання та віднімання чисел за модулем *m* модулярної системи числення на основі кільцевого зсуву: пат. 56858 Україна. № u 2010 09485; заявл. 29.07.2010; опубл. 25.01.2011, Бюл. № 2. 6 с. (*Особистий внесок здобувача: алгоритм роботи пристрою для додавання та віднімання чисел за модулем m на основі кільцевого зсуву*).

38. Пристрій для додавання і віднімання чисел за модулем *m* модулярної системи числення на основі кільцевого зсуву з контролем помилок: пат. 56684 Україна. № u 2010 07759; заявл. 21.06.2010; опубл. 25.01.2011, Бюл. № 2. 6 с. (*Особистий внесок здобувача: алгоритм роботи пристрою для додавання і віднімання чисел за модулем m модулярної системи числення на основі кільцевого зсуву з контролем помилок*).

39. Пристрій для додавання і віднімання чисел за модулем *m* модулярної системи числення: пат. 58949 Україна. № u 2010 12782; заявл. 28.10.2010; опубл. 26.04.2011, Бюл. № 8. 4 с. (*Особистий внесок здобувача: алгоритм роботи пристрою для додавання і віднімання чисел за модулем m модулярної системи числення)*.

40. Табличний пристрій для множення у ласі лишків: пат. 68803 Україна. № u 2011 11631; заявл. 03.10.2011; опубл. 10.04.2012, Бюл. № 7. 6 с. (*Особистий внесок здобувача: алгоритм роботи табличного пристрою для множення у класі лишків*).

41. Табличний пристрій для множення двох чисел у класі лишків: пат. 70442 Україна. № u 2011 14342; заявл. 05.12.2011; опубл. 11.06.2012, Бюл. № 11. 6 с. (*Особистий внесок здобувача: алгоритм роботи табличного пристрою для множення двох чисел у класі лишків*).

42. Пристрій для порівняння даних, що представлені у непозиційній системі числення класу лишків: пат. 79587 Україна. № u 2012 12654; заявл. 05.11.2012; опубл. 25.04.2013, Бюл. № 8. 6 с. (*Особистий внесок здобувача: алгоритм роботи пристрою для порівняння даних, що представлені у непозиційній системі числення класу лишків)*.

43. Пристрій для контролю даних комп’ютерних пристроїв

телекомунікаційної системи, що функціонують у класі лишків: пат. 79673 Україна. № u 2012 13145; заявл. 19.11.2012; опубл. 25.04.2013, Бюл. № 8. 4 с. (*Особистий внесок здобувача: алгоритм роботи пристрою для контролю даних комп'ютерної системи, що функціонує у класі лишків)*.

44. Пристрій для контролю та корекції помилок даних комп'ютерних пристроїв комутаційно-комунікаційного вузла телекомунікаційної мережі, що функціонують у класі лишків: пат. 105436 Україна. № a 2013 00476; заявл. 14.01.2013; опубл. 12.05.2014, Бюл. № 9. 6 с. (*Особистий внесок здобувача: алгоритм роботи пристрою для контролю та корекції помилок даних компонентів комп'ютерних систем, що функціонують у класі лишків)*.

45. Пристрій для контролю даних комп'ютерних пристроїв телекомунікаційної системи, що функціонують у класі лишків: пат. 105455 Україна. № a 2013 07289; заявл. 10.06.2013; опубл. 12.05.2014, Бюл. № 9. 6 с. (*Особистий внесок здобувача: метод контролю даних комп'ютерних пристроїв, що функціонують у СЗК*).

46. Пристрій для контролю помилок даних у комп'ютерних пристроях комутаційно-комунікаційного вузла інформаційно-телекомунікаційної системи, що функціонують у класі лишків: пат. 105742 Україна. № a 2013 08773; заявл. 12.07.2013; опубл. 10.06.2014, Бюл. № 11. 6 с. (*Особистий внесок здобувача: алгоритм роботи пристрою для контролю помилок даних у комп'ютерних пристроях комутаційно-комунікаційного вузла інформаційно-телекомунікаційної системи, що функціонують у класі лишків*).

47. Пристрій для реалізації операції множення двох чисел у класі лишків: пат. 91321 Україна. № u 2014 01726; заявл. 24.02.2014; опубл. 25.06.2014, Бюл. № 12. 4 с. (*Особистий внесок здобувача: алгоритм роботи пристрою для реалізації операції множення двох чисел у класі лишків*).

48. Пристрій для арифметичного та алгебраїчного порівняння двох чисел у класу лишків: пат. 92069 Україна. № u 2014 02480; заявл. 12.03.2014; опубл. 25.07.2014, Бюл. № 14. 6 с. (*Особистий внесок здобувача: алгоритм*

роботи пристрою для арифметичного та алгебраїчного порівняння двох чисел у класу лишків).

49. Пристрій для табличної реалізації арифметичних операцій множення та додавання чисел за модулем m_i класу лишків: пат. 106343 Україна. № a 2013 15558; заявл. 30.12.2013; опубл. 11.08.2014, Бюл. № 15. 6 с. (*Особистий внесок здобувача: алгоритм роботи пристрою для табличної реалізації арифметичних операцій множення та додавання чисел за модулем m класу лишків*).

50. Пристрій для множення двох лишків за довільним модулем класу лишків: пат. 92403 Україна. № u 2014 03259; заявл. 31.03.2014; опубл. 11.08.2014, Бюл. № 15. 4 с. (*Особистий внесок здобувача: алгоритм роботи пристрою для множення двох лишків за довільним модулем класу лишків*).

51. Пристрій для піднесення цілих чисел, що представлені у класі лишків, до ступеня натурального числа: пат. 95060 Україна. № u 2014 06854; заявл. 18.06.2014; опубл. 10.12.2014, Бюл. № 23. 4 с. (*Особистий внесок здобувача: алгоритм роботи пристрою для піднесення цілих чисел, що представлені у класі лишків, до ступеня натурального числа*).

52. Пристрій для реалізації операції модульного множення двох чисел, які представлені у системі залишкових класів: пат. 108828 Україна. № a 2014 10608; заявл. 29.09.2014; опубл. 10.06.2015, Бюл. № 11. 6 с. (*Особистий внесок здобувача: алгоритм роботи пристрою для реалізації операції модульного множення двох чисел, які представлені у системі залишкових класів*).

53. Пристрій для множення лишків a_i та b_i числа за довільним модулем m_i системи залишкових класів: пат. 110901 Україна. № a 2015 01377; заявл. 18.02.2015; опубл. 25.02.2016, Бюл. № 4. 6 с. (*Особистий внесок здобувача: алгоритм роботи пристрою для множення лишків a_i та b_i числа за довільним модулем m_i системи залишкових класів*).

54. Пристрій для множення лишків a_i та b_i чисел за модулем m_i: пат. 110913 Україна. № a 2015 05097; заявл. 25.05.2015; опубл. 25.02.2016, Бюл.

№ 4. 6 с. (*Особистий внесок здобувача: алгоритм роботи пристрою для множення лишків a_i та b_i чисел за модулем m_i*).

55. Пристрій для реалізації операції множення та ділення чисел у системі залишкових класів: пат. 112034 Україна. № а 2015 07299; заявл. 20.07.2015; опубл. 11.07.2016, Бюл. № 13. 6 с. (*Особистий внесок здобувача: алгоритм роботи пристрою для реалізації операції множення та ділення чисел у системі залишкових класів*).

56. Пристрій для контролю та діагностики даних, що представлені у системі залишкових класів: пат. 112731 Україна. № а 2015 10904; заявл. 09.11.2015; опубл. 10.10.2016, Бюл. № 19. 6 с. (*Особистий внесок здобувача: алгоритм роботи пристрою для контролю та діагностики даних, що представлені у системі залишкових класів*).

57. Пристрій для визначення лишків дійсних та комплексних чисел у системі залишкових класів: пат. 114063 Україна. № а 2016 06697; заявл. 21.06.2016; опубл. 10.04.2017, Бюл. № 7. 6 с. (*Особистий внесок здобувача: алгоритм роботи пристрою для визначення лишків дійсних та комплексних чисел у системі залишкових класів)*.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

58. Кошман С. А. Метод динамического резервирования в модулярной системе счисления // Інформаційно-керуючі системи на залізничному транспорті: тези доп. Матеріали стендових доповідей та виступів учасників конференції, №4. Алушта, Крим. Алушта, 2012. С. 61-62.

59. Кошман С. А. Особенности применения табличных методов обработки информации в модулярной системе счисления // Новітні технології для захисту повітряного простору: тези доп. Десятої наукової конференції Харківського університету Повітряних Сил імені Івана Кожедуба, 9–10 квітня 2014 р. Харків, 2014. С. 185.

60. Кошман С. А. Концепция реализации немодульных операций в

модулярной системе счисления // Проблеми інформації: тези доп. Другої міжнародної науково-технічної конференції, Київ: ДУТ; Полтава: ПНТУ; Катовище: Катовицький економічний університет; Париж: Університет Париж VII Вєнсент-Сен-Дєні; Білгород: "БДУ"; Черкаси: ЧДТУ; Харків: ХНДІТМ, 12–13 квітня 2014 року. Харків, 2014. С. 94-95.

61. Кошман С. А. Методы контроля, диагностики и коррекции ошибок данных, представленных в системе остаточных классов // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління: тези доп. Четвертої міжнародної науково-технічної конференції, Полтава: ПНТУ; Баку: ВА ЗС АР; Бєлгород: НДУ "БєлДУ"; Кіровоград: КЛА НАУ; Харків: ДП "ХНДІ ТМ". Харків, 2014. С. 66.

62. Кошман С. А. Разработка и исследование методов нулевизации в системе остаточных классов // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління: тези доп. П'ятої міжнародної науково-технічної конференції, Полтава: ПНТУ; Баку: ВА ЗС АР; Бєлгород: НДУ "БєлДУ"; Кіровоград: КЛА НАУ; Харків: ДП "ХНДІ ТМ". Харків, 2015. С. 39.

63. Кошман С. А. Методы нулевизации чисел в системе остаточных классов // Проблеми інформатизації: тези доп. Третьої міжнародної науково-технічної конференції, Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН; Полтава: ПНТУ. Харків, 2015. С. 45.

64. Кошман С. А. Контроль, диагностика и коррекция данных, представленных в системе остаточных классов // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління: тези доп. Четвертої міжнародної науково-технічної конференції, Полтава: ПНТУ; Баку: ВА ЗС АР; Бєлгород: НДУ "БєлДУ"; Кіровоград: КЛА НАУ; Харків: ДП "ХНДІ ТМ". Харків, 2017. С. 42.

65. Koshman S., Yanko A., Krasnobayev V. Algorithms of data processing in the residual classes system // Problems of Infocommunications Science and Technology PIC S&T 2017: abstr. 4th International Scientific-

Practical Conference. Kharkiv, 2017. P. 117-121. (*Особистий внесок здобувача: досліджено принципи побудови непозиційних кодових структур*). (Видання входить до міжнародної наукометричної бази Scopus).

66. Krasnobayev V., Kuznetsov A., Koshman S., Moroz S. Improved method of determining the alternative set of numbers in residue number system // Recent Developments in Data Science and Intelligent Analysis of Information. Proceedings of the XVIII International Conference on Data Science and Intelligent Analysis of Information, June 4–7, 2018. Kyiv, 2018. P. 319-328. (*Особистий внесок здобувача: розроблено метод діагностики даних у СЗК*). (Видання входить до міжнародної наукометричної бази Scopus).

***Наукові праці, які додатково відображають наукові результати дисертації*:**

67. Краснобаев В. А., Кошман С. А., Янко А. С. Методы оперативного контроля данных в системе остаточных классов, основанные на принципе параллельной нулевизации // Прикладная радиоэлектроника: научно-технический журнал. 2016. Том 15, № 3. С. 253-265. (*Особистий внесок здобувача: розроблено метод оперативного контролю даних у СЗК на основі принципу паралельної нульовизації*).

68. Krasnobayev V., Yanko A., Koshman S. The method of error detection and correction in the system of residual classes // Computer science and cybersecurity. 2016. Issue 1(1). P. 58–66. URL: http://periodicals.karazin.ua/cscs/issue/viewIssue/453/510 (call date: 26.12.2016). (*Особистий внесок здобувача: вдосконалено метод виправлення помилок даних у СЗК*).

69. Krasnobayev V., Yanko A., Koshman S. Conception of realization of cryptographic RSA transformations with using of the residue number system // Computer science and cybersecurity. 2016. Issue 2(2). P. 5–12. URL: http://periodicals.karazin.ua /cscs/issue/ viewIssue/ 454/517. (call date: 26.12.2016) (*Особистий внесок здобувача: запропоновані шляхи*

використання СЗК у криптосистемах).

70. Krasnobayev V., Koshman S., Yanko A. Method of tabular realization of arithmetic operations in the system of residual classes // Computer science and cybersecurity. 2016. Issue 3(3). P. 28–35. URL: http://periodicals.karazin.ua/cscs/issue/view/533. (call date: 26.12.2016). (*Особистий внесок здобувача: вдосконалення табличного методу реалізації арифметичних операцій)*.

71. Кошман С. А., Краснобаев В. А., Янко А. С. Усовершенствованный метод определения альтернативной совокупности чисел в системе остаточных классов // Радиотехника. Всеукраинский межведомственный научно-технический сборник. Харьков: ХНУРЭ. 2017. Вип. 189. С. 29-37. (*Особистий внесок здобувача: вдосконалено метод визначення альтернативної сукупності чисел у СЗК*).

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 31
ВСТУП 33
РОЗДІЛ 1. ДОСЛІДЖЕННЯ МЕТОДІВ ПІДВИЩЕННЯ ОПЕРАТИВНОСТІ КОНТРОЛЮ ТА ДІАГНОСТИКИ ПОМИЛОК КОМПОНЕНТІВ КОМП'ЮТЕРНИХ СИСТЕМ ОБРОБКИ ЦІЛОЧИСЛОВИХ ДАНИХ РЕАЛЬНОГО ЧАСУ, ЩО ПРЕДСТАВЛЕНІ У СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ. ФОРМУЛЮВАННЯ ПРОБЛЕМИ ТА ЗАДАЧ ДОСЛІДЖЕНЬ 44
1.1 Дослідження областей науки та техніки, що вимагають швидку та надійну реалізацію цілочислових обчислень. Аналіз завдань та алгоритмів обробки цілочислових даних 44
1.2 Дослідження методів підвищення оперативності контролю та діагности цілочислових даних, що представлені у СЗК, без зниження продуктивності обробки інформації 50
1.3 Формулювання концепції розвитку швидкодіючих комп'ютерних компонентів обчислювальної системи обробки цілочислових даних реального часу у СЗК 55
1.4 Формулювання проблеми та часткових задач досліджень дисертації 59
Висновки до розділу 1 61
РОЗДІЛ 2. НАУКОВІ ОСНОВИ ПОБУДОВИ НЕПОЗИЦІЙНИХ КОДОВИХ СТРУКТУР У СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ 63
2.1 Формулювання принципів побудови непозиційних кодових структур у СЗК 63
2.2 Дослідження впливу властивостей СЗК на структуру та процес функціонування компонентів комп'ютерної системи обробки цілочислових даних 73

2.3 Принципи та методи реалізації цілочислових операцій у СЗК 77
2.3.1 Суматорний принцип реалізації арифметичних операцій у СЗК 79
2.3.2 Принцип кільцевого зсуву у СЗК 86
2.3.3 Табличний принцип реалізації арифметичних операцій у СЗК 91
2.4 Обґрунтування вибору сукупності основ СЗК 93
2.5 Дослідження можливості ефективного контролю та діагностики цілочислових арифметичних операцій у СЗК 96
Висновки до розділу 2 102
РОЗДІЛ 3. ОСНОВИ ТЕОРІЇ ЗАВАДОСТІЙКОГО КОДУВАННЯ ДАНИХ У СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ. МЕТОД ФОРМУВАННЯ ПОЗИЦІЙНОЇ ОЗНАКИ НЕПОЗИЦІЙНОЇ КОДОВОЇ СТРУКТУРИ 104
3.1 Основні поняття та визначення теорії завадостійкого кодування даних у СЗК 104
3.2 Дослідження коригувальних можливостей кодів у СЗК 112
3.3 Метод варіювання коригувальними властивостями завадостійкого коду у СЗК при виконанні обчислювального процесу 116
3.4 Метод формування позиційної ознаки непозиційного коду у СЗК 121
Висновки до розділу 3 125
РОЗДІЛ 4. МЕТОДИ ОПЕРАТИВНОГО КОНТРОЛЮ ДАНИХ У СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ 127
4.1 Формулювання принципів контролю непозиційних кодових структур у СЗК 127
4.2 Основи контролю достовірності даних у СЗК 134
4.3 Метод контролю даних у СЗК на основі принципу порівняння 148

4.4 Методи контролю даних у СЗК на основі принципу нульовизації 154
4.4.1 Метод послідовного віднімання 154
4.4.2 Метод паралельного віднімання 162
4.4.3 Метод послідовного віднімання з попереднім аналізом подальшого залишку непозиційної кодової структури у СЗК 170
4.4.4 Метод контролю даних у СЗК з попереднім аналізом подальших симетричних залишків контрольованого числа, що заснований на принципі паралельної нульовизації 179
4.5 Методи контролю даних у СЗК, що засновані на використанні позиційної ознаки непозиційної кодової структури 195
4.5.1 Метод оперативного контролю даних у СЗК, що заснований на використанні позиційної ознаки НКС 195
4.5.2 Метод підвищення достовірності оперативного контролю даних у СЗК 203
Висновки до розділу 4 213
РОЗДІЛ 5. МЕТОДИ ОПЕРАТИВНОГО ДІАГНОСТУВАННЯ ПОМИЛОК У СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ 214
5.1 Теоретичні основи діагностики даних, що представлені у СЗК 214
5.2 Метод визначення альтернативної сукупності НКС у СЗК 230
5.3 Метод оперативної діагностики непозиційних кодових структур у СЗК на основі підвищення інформативності альтернативної сукупності чисел 247
5.4 Метод оперативної діагностики непозиційних кодових структур на основі застосування процедури інтервальних числових перерізів 257
Висновки до розділу 5 263
РОЗДІЛ 6. МЕТОДИ ОПЕРАТИВНОЇ КОРЕКЦІЇ ПОМИЛОК У СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ 264

6.1 Теоретичні основи корекції помилок даних у СЗК 264
6.2 Метод виправлення помилок даних у СЗК 268
6.3 Метод корекції помилок даних, що представлені у СЗК з двома контрольними основами 281
6.4 Метод оперативної корекції помилок у СЗК у динаміці обчислювального процесу КСКОЦД 286
6.5 Метод оперативної корекції помилок даних у СЗК, яка представлена взаємно непростими основами 290
Висновки до розділу 6 307
ВИСНОВКИ 309
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 316
ДОДАТОК А. Список публікацій здобувача за темою дисертації 337
ДОДАТОК Б. Акти впровадження результатів дисертаційної роботи 351

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АС – альтернативна сукупність

БКН – блок констант нульовизації

ДОП – динаміка обчислювального процесу

ЗП – пристрій, що запам'ятовує

КЛ – клас лишків

КН – константа нульовизації

КРЗ – кільцевий регістр зсуву

КСКОЦД – комп'ютерні системи та компоненти обробки цілочислових даних

МКВ – мінімальна кодова відстань

МПВ –метод паралельного віднімання

НКС – непозиційна кодова структура

ОЗП – оперативний запам'ятовуючий пристрій

ОК – однорядковий код

ОП – оперативності

ОП – операційний пристрій

ОТ – обчислювальний тракт

ПЗП – постійний запам'ятовуючий пристрій

ПКЗ – принцип кільцевого зсуву

ПЛІС – програмовані логічні інтегральні схеми

ПН – процедура нульовизації

ПН ВПЗ – послідовна нульовизація з визначенням подальшого залишку

ПНН ВПЗ – паралельна нульовизація з визначенням подальших залишків

ПО НКС – позиційна ознака непозиційної кодової структури

ППН – процедура послідовної нульовизації

ПСЛ – повна система лишків

ПСНАВЛ – повна система найменших за абсолютною величиною лишків

ПСНДЛ – повна система найменших додатних лишків

ПСННЛ – повна система найменших невід'ємних лишків

ПСЧ – позиційні системи числення

СЗК – система залишкових класів

СК – система контролю

СФП – схема формування ознаки перенесення

СФС – схема формування ознаки суми

ТП – табличний принцип

ВСТУП

Обґрунтування вибору теми дослідження. Сучасною рисою індустріального суспільства є розробка та використання нових прогресивних інформаційних технологій, що засновані на широкому використанні комп'ютерних систем і компонентів. Існує ряд науково-технічних областей і напрямів, де є необхідність у швидких, достовірних і високоточних цілочислових арифметичних обчисленнях. Це, у першу чергу, арифметичні операції над цілими числами і поліномами; цілочислове лінійне програмування; операції над числами і множинами; рішення багатовимірних NP-повних задач; реалізація алгоритмів маршрутизації; множення векторів і матриць; задача швидкого перетворення Фур'є і його додатки; нейромережеві системи обробки даних; задачі військового призначення; цифрова обробка сигналів і зображень; криптографічні перетворення; цілочислова арифметика високої точності; рішення завдань, пов'язаних з дослідженням космічного простору; високоточні цифро-аналогові і аналого-цифрові перетворення та ін.

У зв'язку з постійним ускладненням науково-технічних задач обробки цілочислових даних, що вирішуються, тенденція розвитку комп'ютерних систем і компонентів спрямована на підвищення швидкодії (продуктивності) і достовірності реалізації цілочислових арифметичних операцій.

Результати, що проводились впродовж останніх років, дослідження методів підвищення продуктивності і достовірності обчислень комп'ютерних систем та компонентів обробки цілочислових даних (КСКОЦД), показали, що у межах позиційних систем числення (ПСЧ) цього істотно добитись практично неможливо [1-3]. Це обумовлено у першу чергу основним недоліком сучасних КСКОЦД, що функціонують у ПСЧ: наявність міжрозрядних зв'язків між числами, що оброблюються. Ці зв'язки негативно впливають на архітектуру КСКОЦД і методи реалізації арифметичних операцій, обмежують швидкодію і достовірність виконання арифметичних операцій.

В зв'язку з цим у ПСЧ підвищення продуктивності КСКОЦД здійснюється, передусім, за рахунок підвищення тактової частоти, розвитку і застосування методів та засобів паралельної обробки даних [4-6]. Такий підхід не завжди вирішує задачу кардинального підвищення швидкодії і достовірності виконання арифметичних операцій у ПСЧ.

Ця обставина зумовила необхідність проведення пошуку шляхів підвищення продуктивності, наприклад, на основі використання нових структурних рішень при створенні КСКОЦД, шляхом застосування непозиційної машинної арифметики. Зокрема, на основі використання непозиційної системи числення у залишкових класах (СЗК) [1, 3, 4].

Результати досліджень в області створення швидкодіючих і надійних КСКОЦД відомих авторів (Валах М., Свобода А., Сабо Н., Акушский І. Я., Юдицкий Д. І., Долгов О. І., Николайчук Я. М., Глушков В. М., Торгашов В. А., Амербаєв В. М., Коляда А. А., Черв'яков Н. І., Shimbo A., Paulier P., Thornton M. A., Dreschler R., Miller D. M. та ін.) показали, що використання СЗК, як системи числення КСКОЦД, призначеної для реалізації цілочислових арифметичних операцій, істотно підвищує швидкодію рішення задач певного класу.

Таким чином, використання СЗК, як системи числення, дозволяє істотно, в порівнянні з ПСЧ, підвищити швидкодію (продуктивність) КСКОЦД за рахунок можливості розпаралелювання арифметичних операцій на рівні мікрооперацій. Це здійснюється шляхом використання основних властивостей СЗК.

У шістдесятих – сімдесятих роках минулого століття, у зв'язку з науково-технічними розробками таких КСКОЦД у СЗК, як А-340А, К-340А, Т-340А, "Алмаз", система 5Э53 і ЕОМ "Вычет" та їх масовим виробництвом на підприємствах промисловості СРСР, у світі проводились серйозні наукові дослідження в області модулярної арифметики (МА) [7-9]. З'явилось багато публікацій на цю тему у пресі, у тому числі і фундаментальних монографій [10-12]. Окрім цього за останні роки були розроблені наступні КСКОЦД у

СЗК: бортовий комп'ютер управління авіаційним двигуном, розроблений Би. С. Гаспаром (СРСР); модулярні цифрові фільтри, розроблені Е. До. Лебедєвим (СРСР); бортовий комп'ютер Star (США); спеціалізовані процесори ДПФ (США, Південна Корея); ряд військових спеціалізованих бортових комп'ютерів (США, Японія); спеціалізовані процесори ЦОС (США); комп'ютери Sprint для робототехніки (США, Японія); у 2011 році, у рамках програми "Університетський кластер" АН РФ, у В'ятському державному університеті для вирішення проблеми високоточних і швидких цілочислових матричних обчислень, на основі табличного методу виконання арифметичних операцій, був створений, пройшов випробування і функціонує обчислювальний кластер у СЗК; у китайській компанії "Tpv Display Technology (Wuhan, China) Co., Ltd" при розробці і впровадженні безпровідної сенсорної мережі системи контролю стану промислового устаткування при виготовленні моніторів; на підприємстві ТОВ "Релком-Поділля" при розробці системи відеоспостереження на основі безпровідних мультимедійних сенсорних мереж; у корпорації "Cypress Semiconductors" при розробці апаратно-програмного забезпечення для модулів CY8CKIT - 050 PsoC 5 і CyFi (CYRF7936), які можуть бути використані у безпровідних сенсорних мережах [13-15].

Проте, відсутність ефективних методів і систем контролю та діагностики все ще стримує широке практичне впровадження СЗК в якості систему числення КСКОЦД.

Аналіз результатів проектування і функціонування КСКОЦД, що функціонує у СЗК, показав, що усі існуючі методи, системи і засоби контролю та діагностики комп'ютерних систем і компонентів мають значний час реалізації відповідних процедур. Ця обставина обумовлює низьку оперативність існуючих методів, систем і засобів контролю та діагностики помилок у СЗК.

Результати аналізу сучасних тенденцій розвитку комп'ютерних систем і компонентів, що функціонують у системі залишкових класів, підтверджують

наявність наступної конфліктної ситуації. З одного боку, між існуючою можливістю значного підвищення швидкодії виконання цілочислових арифметичних операцій у СЗК. З іншого боку, низькою оперативністю існуючих систем і засобів контролю та діагностики результатів обчислень у СЗК за рахунок значного часу реалізації перерахованих процедур.

Вочевидь, що в цьому випадку, існуючі засоби контролю та діагностики КСКОЦД у СЗК "гальмують" широкі потенційні можливості швидкої обробки даних, що закладені у непозиційній машинній арифметиці. Цю обставину породжує протиріччя між високою швидкодією реалізації цілочислових арифметичних операцій і низькою оперативністю контролю та діагностики даних у СЗК. Це протиріччя обумовлене відсутністю ефективних методів оперативного контролю та діагностики помилок даних компонентів комп'ютерної системи, що функціонує у СЗК.

Ця обставина обумовлює мету даної дисертаційної роботи.

Мета і завдання дослідження. Метою роботи є підвищення оперативності контролю та діагностики помилок даних, що представлені у системі залишкових класів.

Для досягнення мети дисертації необхідно сформулювати і вирішити важливу і актуальну науково-технічну проблему дисертації, результати рішення якої дозволили б усунути існуюче протиріччя між високою швидкодією реалізації цілочислових арифметичних операцій і низькою (недостатньою) оперативністю контролю та діагностики даних.

Науково-технічна проблема дисертації. Розробка методів оперативного контролю та діагностики даних компонентів комп'ютерної системи, що функціонують у залишкових класах.

Використання результатів вирішення проблеми сприятиме подальшому розвитку теорії і практики непозиційної машинної арифметики в області контролю та діагностики даних, що представлені у СЗК. Це, у свою чергу, дозволяє розширити область ефективного використання СЗК в якості системи числення комп'ютерних систем і компонентів обробки цілочислових

даних.

Протиріччя між високою швидкодією реалізації цілочислових арифметичних операцій у СЗК і низькою оперативністю операцій контролю та діагностики даних усувається за рахунок результатів рішення сформульованих у дисертації приватних завдань досліджень проблеми.

Часткові задачі досліджень. На основі загальної науково-технічної проблеми дисертації, сформульовані наступні часткові задачі досліджень:

1 – дослідження методів підвищення оперативності контролю та діагностики цілочислових даних, що представлені у системі залишкових класів, без зниження продуктивності обробки інформації;

2 – дослідження впливу властивостей системи залишкових класів на структуру і процес функціонування компонентів комп'ютерної системи обробки цілочислових даних;

3 – дослідження коригувальних властивостей непозиційних кодових структур у системі залишкових класів;

4 – розробка методу контролю даних у системі залишкових класів, що заснований на принципі паралельної нульовизації;

5 – розробка методу контролю даних у системі залишкових класів, що заснований на використанні позиційної ознаки непозиційної кодової структури;

6 – розробка методу підвищення достовірності оперативного контролю даних, що представлені у системі залишкових класів;

7 – вдосконалення методу визначення альтернативної сукупності непозиційних кодових структур у системі залишкових класів;

8 – вдосконалення методу оперативної діагностики даних, що представлені у системі залишкових класів.

Об'єкт дослідження – процеси контролю та діагностики помилок даних, що представлені у системі залишкових класів.

Предмет дослідження – методи та засоби оперативного контролю та діагностики цілочислових даних компонентів комп'ютерної системи, що

функціонують у системі залишкових класів.

Зв'язок роботи з науковими програмами, планами, темами, грандами. Дисертаційну роботу виконано на кафедрі безпеки інформаційних систем і технологій факультету комп'ютерних наук Харківського національного університету імені В. Н. Каразіна відповідно до НДР № 0118U002024 "Аналіз, дослідження, розробка та стандартизація криптографічних систем для захисту інформації в пост-квантовому середовищі, в умовах інформаційних і гібридних війн" (здобувач – виконавець); № 0117U004832 "Розробка математичних моделей і методів синтезу, формування та обробки сигнально-кодових конструкцій для захищених телекомунікаційних систем подвійного призначення" (здобувач – виконавець); № 0119U002546 "Формулювання та розробка принципів, методів і засобів швидкої та достовірної обробки цілочисельних даних, що представлені у непозиційній системи числення залишкових класів в комп’ютерних системах та мережах подвійного призначення" (здобувач – виконавець).

Частина досліджень проводилась на кафедрі автоматизації та комп'ютерно-інтегрованих технологій Харківського національного університету сільського господарства імені Петра Василенка в рамках НДР № 0113U003306 "Концепція, принципи, методи та засоби створення швидкодіючих і надійних систем обробки даних у реальному часі на основі застосування непозиційної системи числення у класі лишків" (здобувач – виконавець).

Участь автора у вказаних науково-дослідних роботах і проектах, в яких здобувач був безпосереднім виконавцем, полягає у розробці методів контролю та діагностики помилок КСКЦОД.

Методи дослідження – в основу проведених у роботі досліджень були покладені принципи системного аналізу, теорія чисел, теорія обчислювальних процесів та систем, а також теорія кодування у СЗК. При вирішенні першої та другої задач досліджень використовувались теорія

обчислювальних процесів та систем, а також розділи теорія подільності і теорія порівнянь теорії чисел. При рішенні подальших задач досліджень використовувалась теорія завадостійкого кодування у СЗК.

Наукова новизна результатів дисертації.

1. **Вперше** отримано метод контролю даних у системі залишкових класів, який на відміну від відомих, заснований на принципі паралельної нульвизації, шляхом поєднання у часі операцій нульвизації симетричних залишків непозиційної кодової структури, що контролюється і визначення констант нульвизації, що дозволяє підвищити оперативність контролю даних.

2. **Вперше** отримано метод контролю даних у системі залишкових класів, який на відміну від відомих, заснований на використанні позиційної ознаки непозиційної кодової структури, шляхом паралельного віднімання встановлених констант, що дозволяє підвищити оперативність контролю даних.

3. **Вперше** отримано метод підвищення достовірності оперативного контролю даних, що представлені у системі залишкових класів, який на відміну від відомих, заснований на використанні позиційної ознаки непозиційної кодової структури, шляхом застосування відповідної основи, що кратна загальному модулю системи залишкових класів, це підвищує достовірність контролю даних.

4. **Вдосконалено** метод визначення альтернативної сукупності непозиційної кодової структури у системі залишкових класів, який заснований на використанні функції відповідності значень можливих помилок, шляхом зменшення кількості основ, що перевіряються, які входять в альтернативну сукупність чисел, що підвищує оперативність діагностики помилок даних.

5. **Вдосконалено** метод оперативної діагностики даних, що представлені у системі залишкових класів, який заснований на формуванні числових інтервалів та ознак даних квадрантів знаходження альтернативних

сукупностей чисел, шляхом згортки таблиці відповідності значень можливих помилок, це зменшує час вибірки основ, що перевіряються та підвищує оперативність діагностики помилок даних.

*Наукове значення роботи***.** Отримані наукові результати в сукупності є розвитком теорії непозиційної системи числення у системі залишкових класів та спрямовані на створення методів оперативного контролю та діагностики непозиційних кодових структур.

Практичне значення отриманих результатів.

1. Результати рішення сформульованої у дисертації важливої та актуальної науково-технічної проблеми можуть бути покладені в основу науково-методологічного апарату для практичного створення високопродуктивних КСКОЦД, які функціонують у СЗК.

2. Розроблені та удосконалені у дисертаційній роботі методи контролю та діагности помилок даних доцільно використовувати при створенні системи контролю та корекції помилок для перспективних КСКОЦД у СЗК.

3. Застосування запропонованих у дисертації методів оперативного контролю даних у СЗК, які засновані на використанні принципу нульовизації і позиційній ознаці непозиційної кодової структури, дозволяє на 25-60% (у порівнянні з існуючими методами контролю) скоротити час контролю, що підвищує оперативність процедури контролю.

4. Запропоновані методи оперативної діагностики даних у СЗК дозволяють до 30% (у порівнянні з існуючими методами діагностики) скоротити час контролю, що підвищує оперативність процедури діагностики.

5. Розглянуті методи оперативного виправлення помилок даних у СЗК сприяли розробці засобів, які на відміну від існуючих дозволяють у ρ раз підвищити оперативність корекції помилок у СЗК. Де ρ – кількість можливих залишків НКС, в яких сталися помилки.

6. На підставі запропонованих методів обробки даних у дисертації розроблені алгоритми для їх реалізації у відповідності, з якими синтезовані засоби обробки даних у СЗК у вигляді пристроїв, на які отримано 35 патентів

України. Це підтверджує актуальність, новизну та практичну значущість отриманих у дисертації результатів.

Результати дисертаційної роботи впроваджені: у приватне акційне товариство "Інститут інформаційних технологій", м. Харків, акт впровадження від 16.06.2017 р., на кафедрі безпеки інформаційних систем і технологій Харківського національного університету імені В. Н. Каразіна при виконанні НДР "Розробка математичних моделей та методів синтезу, формування та обробка сигнально-кодових конструкцій для захищений телекомунікаційних систем подвійного призначення" (ДР № 0117U004832, 2017-2020 р .р.), акт впровадження від 05.09.2018 р., на кафедрі безпеки інформаційних систем і технологій Харківського національного університету імені В. Н. Каразіна при виконанні НДР "Аналіз, дослідження, розробка та стандартизація криптографічних систем для захисту інформації в пост-квантовому середовищі, в умовах інформаційних і гібридних війн" (ДР № 0118U002024, 2018 р.), акт впровадження від 05.09.2018 р., а також в навчальний процес кафедри безпеку інформаційних систем і технологій Харківського національного університету імені В. Н. Каразіна в дисципліну "Математичні основи проектування та оптимізації інформаційно-комутаційних систем", акт впровадження від 22.06.2018 р., в навчальний процес кафедри автоматизації та комп'ютерно-інтегрованих технологій Харківського національного технічного університету сільського господарства імені П. Василенка в дисципліну "Мікропроцесорні керуючі пристрої", акт впровадження від 21.02.2017 р.

Особистий внесок здобувача полягає у розробці методів оперативного контролю та діагностики даних компонентів комп'ютерної системи, що функціонують у системі залишкових класів, що дозволяє усунути протиріччя між високою швидкодією реалізації цілочислових арифметичних операцій та низькою оперативністю контролю та діагностики даних.

Використання результатів вирішення протиріччя сприятиме подальшому розвитку теорії і практики кодування у СЗК. Це, у свою чергу,

дозволяє розширити область ефективного використання СЗК в якості системи числення комп'ютерних систем і компонентів обробки цілочислових даних.

Аналіз та систематизація теоретичних і практичних відомостей та результатів за темою дисертації, формулювання наукового напрямку, вибір об’єктів та постановка наукових завдань дисертаційної роботи виконано дисертантом особисто. Розробку методів та засобів оперативного контролю та діагностики даних, що представлені у СЗК, а також проведення порівняльного аналізу дисертант виконував самостійно.

Обговорення основних положень дисертаційної роботи виконано спільно з науковим консультантом д.т.н., професором Краснобаєвим (Харківський національний університет імені В. Н. Каразіна).

Результати дисертаційної роботи повністю відображено в публікаціях.

Всі співавтори згодні із внеском здобувача. Робота не містить плагіату та запозичень. У докторській дисертації не містяться результати кандидатської дисертації.

Апробація матеріалів дисертації. Основні положення дисертаційної роботи та результати досліджень доповідалися і обговорювалися та були схвалені на міжнародних науково-технічних семінарах, науково технічних конференціях і форумах: Міжнародних науково-практичних конференціях "Проблеми енергозабезпечення та енергозбереження в АПК України" (м. Харків, 2010 – 2012 р.р.), 25-й міжнародній конференції "Перспективные компьютерные, управляющие и телекоммуникационные системы для железных дорог Украины. (м. Алушта, Крим, 2012 р.), десятій науковій конференції "Новітні технології – для захисту повітряного простору" (м. Харків, Україна, 2014 р.), другій та третій міжнародній науково-технічній конференції "Проблеми інформації" (м. Полтава, Україна, 2014, 2015 р.р.), четвертій, п’ятій, сьомій міжнародній науково-технічній конференції "Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління" (м. Полтава, Україна, 2014, 2015, 2017 р.р.).

Публікації. Основні наукові результати дисертації опубліковані у 71 друкованій роботі, з яких 3 колективні монографії, 37 наукових статей (у тому числі з них 26 статей у наукових фахових виданнях України, 3 статті включені у міжнародну наукометричну базу "Scopus"), 22 патенти України, 9 тез доповідей на фахових вітчизняних і міжнародних науково-технічних конференціях (2 з яких включені у міжнародну наукометричну базу "Scopus").

Структура та обсяг дисертації. Дисертаційна робота складається зі вступу, 6 розділів, загальних висновків, списку використаних джерел та 2 додатків. Обсяг загального тексту дисертації складає 360 сторінок (14,7 д.а.), з них основного тексту 266 сторінок (11,7 д.а.). Робота ілюстрована 36 таблицями та 30 рисунками. Список використаних джерел містить 181 найменування.

РОЗДІЛ 1. ДОСЛІДЖЕННЯ МЕТОДІВ ПІДВИЩЕННЯ ОПЕРАТИВНОСТІ КОНТРОЛЮ ТА ДІАГНОСТИКИ ПОМИЛОК КОМПОНЕНТІВ КОМП'ЮТЕРНИХ СИСТЕМ ОБРОБКИ ЦІЛОЧИСЛОВИХ ДАНИХ РЕАЛЬНОГО ЧАСУ, ЩО ПРЕДСТАВЛЕНІ У СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ. ФОРМУЛЮВАННЯ ПРОБЛЕМИ ТА ЗАДАЧ ДОСЛІДЖЕНЬ

1.1 Дослідження областей науки та техніки, що вимагають швидку та надійну реалізацію цілочислових обчислень. Аналіз завдань та алгоритмів обробки цілочислових даних

У даний час існує ряд областей та напрямків науки і техніки, де є необхідність у швидких, надійних і високоточних цілочислових арифметичних обчисленнях. Можна сказати, що практично у всіх областях науки використовують цілочислові арифметичні обчислення. Це в першу чергу такі галузі науки як: математика, фізика, астрономія, технічні науки, геодезія і метеорологія, метрологія, сейсмологія ін.

Результати, що проводились протягом останніх років, досліджень в області інформаційних технологій різними групами вчених та інженерів, методів підвищення продуктивності, надійності, живучості, а також достовірності обчислень КСКОЦД, показали, що в межах ПСЧ цього істотно домогтися практично неможливо [16-18].

До теперішнього часу виник розрив між зростаючими вимогами до підвищення продуктивності та надійності КСКОЦД реального часу, з одного боку, і неможливістю задоволення цих запитів на основі використання існуючих позиційних систем числення, з іншого боку.

Пошук шляхів підвищення ефективності функціонування КСКОЦД, показав, що одним з можливих варіантів є використання нових архітектурних рішень шляхом застосування непозиційної машинної арифметики. Зокрема, на основі використання СЗК. Відома китайська теорема про залишки (задача

відновлення вихідного числа A_k за сукупністю його залишків (лишків) $\{a_i\}$ від ділення його на ряд $m_1, m_2, ..., m_n$ натуральних чисел (модулів) СЗК), яка до цього трактувалася як структурна теорема абстрактної алгебри, гарантувала вказаний паралелізм, в обчисленнях над цілими числами, за умови, що результат кільцевих операцій належить діапазону цілих чисел, який визначається добутком модулів СЗК. Результати проведених досліджень методів реалізації арифметичних операцій у СЗК привели до створення нової машинної арифметики. Висхідна своїми ідейними корінням до класичних праць Ейлера, Гауса та Чебишева з теорії порівнянь, СЗК внесла нові ідеї у розробку методів створення високопродуктивних і наднадійних КСКОЦД [19-21].

Однак у вісімдесятих роках минулого століття по ряду об'єктивних і суб'єктивних причин інтерес до СЗК різко знижується. Це було обумовлено в першу чергу смертю директора Центру мікроелектроніки, що займається розробкою загальної теорії та практичним створенням ЕОМ у СЗК, розташованого у м. Зеленограді Московської обл., керівника і головного ініціатора проекту Лукіна Федора Вікторовича і, у зв'язку з цим, повним припиненням практичних робіт в напрямку використання СЗК. [1]

В даний час знову зростає інтерес до використання СЗК [22-24]. Він викликаний, перш за все, такими обставинами:

- появою чисельних науково-теоретичних публікацій, присвячених теорії і практиці створення комп'ютерних систем і компонентів у СЗК [25–27];

- широким розповсюдженням мобільних процесорів, в яких потрібна висока продуктивність обробки даних при незначному споживанні енергії;

- відсутність міжрозрядних переносів у процесі виконання арифметичних операцій додавання і множення чисел у СЗК дозволяє знизити споживання енергії;

- великий інтерес до СЗК виявляють банківські структури, де необхідно у реальному часі надійно і достовірно обробляти великі масиви даних, тобто

потрібні високопродуктивні засоби для високонадійних обчислень з самокорекцією помилок, що характерно для кодів у СЗК;

- збільшення щільності елементів на одному кристалі не у всіх випадках дозволяє провести якісне і повне тестування; у цьому випадку зростає важливість забезпечення відмовостійкого функціонування КСКОЦД [28-30];

- необхідність використання спеціалізованих КСКОЦД для виконання великої кількості операцій над векторами, які вимагають високої швидкості виконання цілочислових операцій додавання і множення (задачі множення матриць, задачі скалярного добутку векторів, перетворення Фур'є і т.д.) [31-33];

- широке впровадження мікроелектроніки в усі сфери життєдіяльності людини значно підвищило актуальність і важливість, раніше рідкісних, а тепер таких масових науково-практичних задач, як цифрова обробка сигналів та зображень, розпізнання образів, криптографія, обробка та зберігання багаторозрядної інформації і т.п.; дана обставина вимагає величезних обчислювальних ресурсів, що перевищують існуючі можливості [34-36];

- існуючий рівень розвитку мікроелектроніки підходить до межі своїх можливостей з точки зору забезпечення продуктивності та надійності, існуючих і перспективних комп'ютерних систем та компонентів обробки в реальному часі великих масивів даних; на зміну їй йдуть наноелектроніка, молекулярна електроніка, мікромеханіка, біоелектроніка, оптичні, оптоелектронні і фотонні ЕОМ та ін., ще дуже далекі від реального широкого промислового виробництва і застосування [37-39];

- сучасний розвиток інтегральної схемотехніки дозволяє по-новому поглянути на принципи побудови пристроїв із застосуванням СЗК та надає широкі можливості по використанню нових методів проектування (наприклад, методологія проектування систем на кристалі - SoC) як при розробці окремих обчислювальних блоків, так і комп'ютерних систем в цілому; інтегральна технологія дає можливість більш гнучкого проектування

комп'ютерних систем і компонентів та дозволяє реалізовувати пристрої на основі СЗК настільки ж ефективно, як і на основі двійкової системи числення; крім того, в даний час для підвищення ефективності розробки комп'ютерних пристроїв широкого поширення набули різного роду системи автоматизованого проектування (САПР); в цьому відношенні, проектування комп'ютерних систем і компонентів на основі СЗК нічим не відрізняється від розробки за допомогою даних САПР двійкових блоків даних у ПСЧ [40-43];

- на сьогодні Україна, на жаль, на відміну від теоретичних розробок, технологічно відстає від зарубіжної мікроелектроніки ряду провідних країн; в цьому випадку цілком доцільно використовувати наявне теоретичні напрацювання та практичний досвід створення ефективних комп'ютерних систем і компонентів у СЗК.

Розглянемо деякі задачі, які оперують з цілочисловими даними.

1. Задача множення двох матриць у СЗК. Розглянемо задачу множення двох A і B квадратних матриць дорівнює розмірності $N \times N$. У вузлах матриці містяться цілі числа. Матриці A і B представляються відповідно у вигляді:

$$A = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1N} \\ a_{21} & a_{22} & \cdots & a_{2N} \\ \vdots & & \vdots & \vdots \\ a_{N1} & a_{N2} & \cdots & a_{NN} \end{vmatrix} \text{ і } B = \begin{vmatrix} b_{11} & b_{12} & \cdots & b_{1N} \\ b_{21} & b_{22} & \cdots & b_{2N} \\ \vdots & & \vdots & \vdots \\ b_{N1} & b_{N2} & \cdots & b_{NN} \end{vmatrix}.$$

Результат множення двох матриць A і B буде представлятися у вигляді

$$C = \begin{vmatrix} c_{11} & c_{12} & \cdots & c_{1N} \\ c_{21} & c_{22} & \cdots & c_{2N} \\ \vdots & & \vdots & \vdots \\ c_{N1} & c_{N2} & \cdots & c_{NN} \end{vmatrix}.$$

Відомо, що базовою операцією (БО) при обчисленні добутку двох матриць є операція виду

$$c_{ij} = \sum_{i,j}^{N} (a_{ik} \cdot b_{kj}) = a_{i1} \cdot b_{1j} + a_{i2} \cdot b_{2j} + a_{i3} \cdot b_{3j} + \ldots + a_{iN} \cdot b_{Nj} \ \ (i, j = \overline{1, N}),$$

де c_{ij} - відповідний елемент лежить на перетині i - рядка та j - стовпця матриці C. Як видно з алгоритму БО кількість множень і додавань дорівнює відповідно N і $N-1$. Загальна кількість БО в алгоритмі множення двох матриць, тобто при визначенні значення $C = A \times B$, дорівнює кількості N^2 елементів c_{ij} $(i, j = \overline{1, N})$ матриці C розмірністю $(N \times N)$.

2. Задача визначення найкоротшої довжини шляху для передачі повідомлення в комп'ютерній мережі. Суть даної задачі полягає у визначенні оптимальної (найкоротшої) довжини шляху між будь-якою парою вузлів КМ, представленої у вигляді неорієнтованого графа. Завдання вирішується матричних методом (метод В. Г. Лазарєва), який вимагає знання структури КМ у цілому і тому найбільш часто застосовується при централізованому управлінні. Він визначає дистанційну (матриця рішень, матриця найкоротших довжин шляхів, дисперсійна матриця) матрицю. При матричному методі проводяться операції над матрицею L довжин гілок мережі, а параметром що оптимізується є довжина шляху між будь-якою парою вузлів графа, де вихідна матриця довжин шляхів представляється у вигляді:

$$L^{(1)} = \left| l_{ij} \right|^{(1)},$$

де чисельне значення довільного елемента $l_{ij}^{(1)}$ вихідної матриці L

визначає в умовних одиницях відстань між вузлами *i* та *j*. Якщо вузли *i* та *j* не сусідньої (відсутнє ребро), то $l_{ij} = \infty$. Відстань всередині вузла вважається нульовою ($l_{ii} = 0$). Довжину найкоротших шляхів між усіма парами вузлів мережі можна визначити шляхом використання так званої операції "зведення вихідної матриці $L^{(1)}$ у R-ю ступінь" ($R \le (N-1)$, тобто число ітерацій R не може перевищувати значення $N-1$ (N - число вузлів графа).

Звичайне зведення матриці у ступінь є послідовне множення її саму на себе $(R-1)-n$ раз (множення "зліва", тобто $L^{(R)} = L^{(1)} \cdot L^{(R-1)}$). Якщо $l_{im}^{(1)}$ - елемент *i*-го рядка та *m*-го стовпця матриці $L^{(1)}$, а $l_{mj}^{(R-1)}$ - елемент *m*-го рядка та *j*-го стовпця матриці $L^{(R-1)}$, то, за правилом множення матриць, елемент $l_{ij}^{(R^*)}$ матриці $L^{(R)}$ дорівнює:

$$l_{ij}^{(R^*)} = l_{i1}^{(1)} \cdot l_{1j}^{(R-1)} + l_{i2}^{(1)} \cdot l_{2j}^{(R-1)} + \ldots + l_{im}^{(1)} \cdot l_{mj}^{(R-1)} + \ldots + l_{iN}^{(1)} \cdot l_{Nj}^{(R-1)}. \qquad (1.1)$$

Що стосується виконання задачі маршрутизації у виразі (1.1) для визначення значення $l_{ij}^{(R^*)}$ замінимо операцію "множення" звичайним складанням, а операцію "складання" – вибором мінімуму з отриманих значень сум:

$$l_{ij}^{(R)} = \min\left\{\sum_{i,j}^{N}\left(l_{im}^{(1)} + l_{mj}^{(R-1)}\right)\right\},\ m = \overline{1, N}. \qquad (1.2)$$

Покажемо, що значення $l_{in}^{(R)}$ дорівнює "вазі" x_{in} вузла *i* по відношенню до виділеного вузла *n*, тобто мінімальній відстані до нього. Дійсно,

$$\begin{cases} x_{in}^{(1)} = l_{in}^{(1)}, \\ x_{in}^{(2)} = \min\limits_{m}\left(l_{im}^{(1)} + x^{(1)}{}_{mn}\right) = \min\limits_{m}\left(l_{im}^{(1)} + l^{(1)}{}_{mn}\right) = l_{in}^{(2)}, \\ \vdots \\ x_{in}^{(R)} = \min\limits_{m}\left(l_{im}^{1} + x_{mn}^{R-1}\right) = \min\limits_{m}\left(l_{im}^{(1)} + l^{(R-1)}{}_{mn}\right) = l_{in}^{(R)}. \end{cases} \quad (1.3)$$

Отже, значення $l_{ij}^{(R)}$, при $R \le N-1$ (R - число прохідних гілок графа) є довжиною найкоротшого шляху між вузлом i та вузлом j КМ. Для конкретної мережі обчислюють матрицю $L^{(R)}$, для якої $L^{(R)} = L^{(R-1)}$. У цьому випадку отримаємо матрицю рішень. Після цього обчислення припиняються. Як видно, базова операція для даного цілочислового алгоритму складається з двох основних операцій додавання і порівняння. Загальна кількість базових операцій типу $c_{ij} = \sum\limits_{i,j}^{N}(a_{ik} \cdot b_{kj}) = a_{i1} \cdot b_{1j} + a_{i2} \cdot b_{2j} + a_{i3} \cdot b_{3j} + \ldots + a_{iN} \cdot b_{Nj}$, $(i, j = \overline{1, N})$ так само дорівнює N^2. Відзначимо, що наведений матричний метод оптимізації може бути використаний не тільки для пошуку шляху мінімальної довжини, а й самого надійного шляху – шляху з мінімальним значенням ймовірності втрат повідомлень. Для цього необхідно знайти такий шлях, в якому добуток ймовірностей ω_{ij} справного стану окремих його ділянок l_{ij} має максимальну величину:

$$P_K = \max \prod_{\rho=1}^{n} \omega_{ij}, \quad (1.4)$$

де n - число транзитних ділянок K-го шляху ($K = 1,2,3,\ldots$) КМ.

1.2 Дослідження методів підвищення оперативності контролю та діагности цілочислових даних, що представлені у СЗК

Контроль і діагностика покликані забезпечити пошук у КСКОЦД

виникаючих несправностей з метою їх подальшого усунення.

Під несправністю будемо розуміти порушення нормального технічного стану КСКОЦД, який визначається на етапі розробки об'єкту та знаходить відображення у правилах його експлуатації, що закріплюються технічною документацією.

Контроль – це перевірка КСКОЦД на наявність відмови. Результатом контролю є вибір однієї з двох альтернативних відповідей: позитивної – об'єкт працездатний або негативної – об'єкт непрацездатний.

Відмова – це таке порушення працездатності об'єкту, коли в ньому з'являється стійка несправність. Стійкою вважається несправність, яка, з'явившись, не може самоусунутись. Порушення працездатності КСКОЦД проявляється у неправильному (не передбаченому заздалегідь) його функціонуванні (хоч б в одному з режимів, експлуатації, що допускаються правилами). Таким чином, відмова є подією, поява якої унеможливлює подальше використання КСКОЦД по своєму прямому призначенню до тих пір, поки несправність, що з'явилася, не буде усунена.

Діагностика – це пошук несправностей, що привели до відмови КСКОЦД. Результатом діагностики є визначення конкретного місця розташування і характеру знайдених несправностей або зазначення тих частин, в яких ці несправності виникли.

Методи контролю працездатності КСКОЦД тісно пов'язані з експлуатацією її як об'єкту обслуговування. Від того, наскільки раціонально вони вибрані, залежатиме ефективність експлуатаційного обслуговування КСКОЦД. При проектуванні такої складної системи, як КСКОЦД, і її програмного забезпечення слід враховувати особливості експлуатації та ефективність тих або інших методів контролю працездатності в процесі експлуатації КСКОЦД. Необхідні експлуатаційні характеристики КСКОЦД мають бути включені як початкові параметри в процесі проектування всіх елементів КСКОЦД.

Розглянемо основну класифікацію автоматичних методів контролю та

діагностики КСКОЦД.

При апаратному контролі (діагностиці) пошук несправностей у пристрої (чи окремих його частинах) здійснюється обладнанням, що спеціально передбачене, яке не потрібне, якщо відмови не виникають. Це устаткування при зовнішньому контролі (діагностиці) не входить у пристрій, що контролює (діагностує), а при внутрішньому розглядається як додаткове (по відношенню до основного). Достоїнствами апаратних методів є висока швидкість пошуку несправностей і можливість фіксації нестійких несправностей, а недоліком – наявність додаткового (надмірного) обладнання.

При програмному контролі (діагностиці) за допомогою спеціальних програм організовуються такі режими автоматичної роботи, при яких блоки та елементи пристрою взаємно перевіряють один одного. Програмний контроль та діагностика використовують власні функціональні можливості пристрою, тому є внутрішніми. Це їх недолік, оскільки пристрій або окремі його частини працюють не по своєму прямому призначенню. Проте достоїнства програмних методів контролю (діагности) – можливість їх постійного вдосконалення (за рахунок зміни програм) у процесі експлуатації, коли досвід що накопичується, підказує нові, ефективніші технічні рішення, а апаратні переробки практично виключені.

Апаратно-програмний контроль, поєднує достоїнства обох вище розглянутих методів контролю та значною мірою вільний від їх недоліків. При такому контролі частина обладнання пристрою в деякі періоди часу, що задаються програмою, перемикається з рішення основної задачі на контроль правильності функціонування іншої частини обладнання, що продовжує рішення задачі. У даному випадку тільки частина пристрою не виконує роботу по своєму прямому призначенню.

Залежно від того, яка частина часу роботи пристрою відводиться на пошук несправностей, а також від засобів, що притягаються, методи контролю і діагностики можна розділити на оперативні та тестові.

При оперативному контролі (діагностиці) пошук несправностей виконується спеціально передбаченими для цих цілей технічними засобами впродовж усього часу роботи пристрою.

На відміну від цього тестовий контроль (діагностика) здійснюється переведенням пристрою (чи його окремих частин), на тих або інших інтервалах часу, в спеціальні допоміжні режими роботи. Ці режими не пов'язані з прямим функціональним призначенням пристрою і вводяться лише для пошуку несправностей. Тут завжди беруть участь дві характерні частини апаратури. Одна є контрольованою (діагностованою), виступаючи в ролі об'єкту контролю (діагности), та належить пристрою, в якому відбувається пошук несправностей. Інша частина є контролюючою (діагностуючою) і не обов'язково входить в даний пристрій. Цю частину апаратури (на яку покладаються функції автоматичного керування процесом пошуку несправностей) зазвичай називають базою.

У процесі тестового контролю (діагности) за допомогою апаратурних і програмних засобів, що входять до складу бази, здійснюється формування і видача на входи об'єкту контролю (діагности) деякої безлічі вхідних наборів, а також прийом та аналіз вихідних наборів, що отримуються на виходах об'єкту. Кожен вхідний (вихідний) набір є цілком певною комбінацією сигналів на входах (виходах) об'єкту. На підставі аналізу вихідних наборів, що вироблюється у базі, здійснюваного за формальними правилами (наприклад, шляхом порівняння з еталонними вихідними наборами), визначаються результати контролю (діагности). Дані про результати контролю та діагностики використовуються для реалізації заходів по усуненню несправностей.

Досвід показує, що контроль здійснити, як правило, простіше, ніж діагностику. Крім того, реально виникаючі обмеження на практичну придатність процедур контролю та діагностики призводять до того, що зі збільшенням кількості контрольованого (діагностуючого) обладнання, рішення задач пошуку несправностей різко ускладнюється. Усе це, природно,

впливає на технічні рішення, використовуються на практиці. Зокрема, наприклад, часто віддають перевагу апаратно-програмному методу пошуку несправностей при наступному поєднанні: оперативний апаратний контроль (у процесі функціонування пристрою) плюс тестова програмна діагностика (у спеціальних режимах, не пов'язаних з прямим функціональним призначенням пристрою).

При технічному втіленні тестових способів контролю та діагностики, прагнучи до максимального спрощення процедур пошуку несправностей, зазвичай дотримуються наступної стратегії. Спочатку виконують контроль, а потім, у разі виявлення відмови, переходять до діагностики. Як контроль, так і діагностику в загальному випадку реалізують поетапно, причому на кожному етапі пошук несправностей здійснюється у блоках пристрою, доступних для контролю та діагностики з боку бази. Після контролю і встановлення працездатності тих або інших блоків пристрою вони включаються у базу. Таке розширення бази потрібне для забезпечення пошуку несправностей в тих блоках, які спочатку були недоступні для контролю (діагностики) [44-46].

Усередині блоку, доступного для контролю (діагностики), пошук несправностей організовується за наступним принципом. Несправності, що виникли в елементах блоку, проявляються у вигляді спотворення вихідних сигналів. Якщо спотворення сигналу на виході деякого елементу є причиною спотворення сигналу на тому або іншому виході блоку, то говорять, що між відповідними виходами елементу та блоку є чутливий шлях. Якщо ж спотворення сигналу на виході елементу не призводить до спотворення сигналу на цьому виході блоку, то говорять, що між відповідними виходами елементу та блоку чутливий шлях відсутній. Щоб у процесі пошуку, несправність елементу проявилася на виходах блоку у формі зміни його вихідного набору, досить підібрати будь-який з таких вхідних наборів (хоч б один такий завжди існує, інакше не можна говорити про несправність), при якому ця несправність виразиться у вигляді спотворення сигналу на виході

елементу, що відмовив, і буде чутливий шлях між виходом цього елементу і принаймні одним виходом блоку.

У процесі пошуку несправностей шляхом належного вибору послідовності вхідних наборів забезпечують:

– при контролі – щоб кожна з даних несправностей проявилася (виявилася) хоча б один раз;

– при діагностиці - щоб різні несправності проявилися по-різному.

1.3 Формулювання концепції розвитку швидкодіючих комп'ютерних компонент обчислювальної системи обробки цілочислових даних реального часу у СЗК

Сучасна теорія кодування має у розпорядженні великий арсенал методів і засобів для підвищення інформаційної надійності систем обробки даних. Широкому впровадженню методів інформаційного резервування, яке дозволяло б контролювати помилки в системах обробки, сприяє використання для цього кодів у залишкових класах.

Використання методів інформаційного резервування дозволяє врахувати те, що одержувача інформації, у кінцевому підсумку, не цікавлять ні величина помилки, ні її місцезнаходження. Вони базуються на імовірнісних гіпотезах про кратність помилок. Одержувача цікавить лише вірна за деяким критерієм інформація для подальшого використання. Ця особливість має бути закладена ще при проектуванні системи обробки даних.

До коду, який зміг би контролювати помилки, що виникають у засобах обробки інформації, передусім пред'являються вимоги арифметичності. Під арифметичністю коду, що контролює помилки, розуміється його властивість, яка полягає в тому, що при виконанні будь-якої арифметичної операції над двома "правильними" кодовими словами (числами) результат також є "правильним" кодовим словом. При цьому бажано, щоб у процесі обчислення помилки не переміщувалися з розряду в розряд. Коди, що задовольняють

вищеперерахованим вимогам, відомі. Одним з представників цього класу кодів є коди у залишкових класах [47-49].

Універсальність кодів у залишках пояснюється не лише їх високі корегуючи здібності, арифметичність та можливістю боротьби з пакетами помилок, але і їх пристосованістю до гнучкої зміни коригуючих властивостей, без зміни способу кодування.

Система числення у залишкових класах відкриває можливість використання єдиного завадостійкого коду для боротьби з помилками, що виникають при передачі та обробці даних у КСКОЦД.

При цьому, якщо операції над залишками проводяться за правилами модулярної арифметики, то безліч точок даного простору залишків задовольнятиме усім аксіомам додавання та множення, тобто код у залишках є арифметичним кодом. Під арифметичністю коду будемо розумітимемо такі його властивості, маючи які код зберігає здатність контролювати помилки при виконанні над ним арифметичних операцій. Достоїнством подібного коду є те, що він може бути використаний як для перевірки правильності виконання арифметичних операцій, так і для підвищення завадозахищеності [50-52].

Відмітимо, якщо виконується за програмою деякий ланцюг арифметичних операцій, істинний результат якого у разі відсутності помилок у ході обчислення має бути правильним числом, і нехай у процесі обчислення на одному етапі мав місце збій у цифрах по деякій основі m_i. Тоді кінцевий результат ланцюга може містити помилку тільки по цій же основі m_i. Інакше кажучи, в процесі обчислення помилки, що виникають зберігають свої місця і не переміщаються в основи, не порушені первинною помилкою.

Основними вимогами, які пред'являються до КСКОЦД, є висока надійність та живучість. Оскільки створити абсолютно надійні компоненти систем принципово неможливо, виник іншій, новий напрям – відмовостійкі

обчислювальні системи, тобто системи, що здатні продовжувати функціонувати при виникненні різноманітних збоїв та відмов частини обладнання.

Існують два напрями для підвищення надійності обчислювальних систем: запобігання несправностям та створення відмовостійких систем.

При використанні першого напряму намагаються усунути усі можливі джерела відмов, конструюючи систему з високонадійних компонентів. Проте в цьому випадку у міру наближення інтенсивності відмов елементів до порогових значень, що обумовлюються фізичними параметрами або технологією, вартість системи різко зростає. Крім того, оскільки при першій же відмові або збої нормальне функціонування системи припиняється, і для її експлуатації потрібно постійний персонал, що веде до дорожчання системи.

При використанні другого напряму імовірність відмови компонентів не знижується, але до системи пред'являються додаткові вимоги: вона повинна безпомилково працювати при відмовах окремих компонентів. Ці додаткові вимоги і, отже, відмовостійке функціонування системи забезпечуються за рахунок введення різноманітних форм надмірності : апаратною, програмною і тимчасовою.

Надмірність може бути використана і для поліпшення інших важливих характеристик обчислювальних структур. Широкі перспективи мають обчислювальні структури, реалізовані на основі непозиційних систем числення, які дають можливість виключити час перенесення при виконанні арифметичних операцій. Останнє у багатьох випадках дозволяє підвищити одночасно надійність, живучість і швидкодію при помірних витратах апаратурних засобів. Однією з таких систем числення є система залишкових класів.

Узагальнений алгоритм функціонування будь-якої відмовостійкої системи зводиться до наступних стандартних процедур:

– виявлення відмови у системі;

– діагностування пристрою, що відмовив;

– оцінка викликаного відмовою ушкодження;

– усунення пристрою, що відмовив, і відновлення втраченої інформації.

При цьому засоби забезпечення відмовостійкості обчислювальних систем, що функціонують в позиційній системі числення, мають ряд істотних недоліків. Основними з них є:

– значні апаратні і програмні витрати, необхідні для реалізації відмовостійкого спецпроцесора;

– застосування структурного резервування, як на рівні окремого обчислювального модуля, так і на рівні усієї паралельної системи ускладнює обчислювальний комплекс, підвищує його енергоспоживання;

– складність реалізації процедур пошуку і локалізації помилки в процесі обчислень;

– складність написання та реалізації програми самотестування;

– значні тимчасові витрати на реконфігурацію структури;

– необхідність перезапуску програми після відновлення працездатної структурної конструкції обчислювальної системи, що неприйнятно при виконанні завдання в масштабі реального часу.

У той же час структура непозиційних КСКОЦД, наближається до високої міри однорідності, що дозволяє істотно поліпшити такий параметр, як живучість.

Так само застосування системи залишкових класів забезпечує незалежну і паралельну обробку кожного розряду числа. З урахуванням малої розрядності оброблюваних операндів КСКОЦД у СЗК може бути виконана у вигляді набору таблиць для реалізації ряду основних модульних операцій [53-55].

Надмірне кодування у СЗК забезпечує живучість апаратури навіть в катастрофічних ситуаціях, коли потік несправностей дуже великий. Така система видаватиме результат з меншою точністю або з дещо уповільненою, але цілком достатньою, для якісного функціонування апаратури швидкодією.

Слід зазначити, що СЗК з двома контрольними основами дозволяє

повністю зберегти працездатність спецпроцесора при відмовах будь-яких двох елементів. А при виникненні третього і навіть четвертого відмов, все ще може виконати програму при деякому зменшенні точності та швидкості обчислень.

Ця властивість є одним з чинників, на яких базується розробка структури відмовостійких непозиційних КСКОЦД з поступовою деградацією без помітного збільшення апаратурних витрат, тобто резервування, і забезпечує створення обчислювальних систем, що допускають можливість продовження роботи при відмові частини елементів структури.

Поєднання вимог високої надійності та швидкої обробки даних дозволяє створити унікальну структуру непозиційного нейрокомп'ютера завдяки модульній організації по обробці, передачі та зберіганню інформації.

Таким чином, концепція розвитку швидкодіючих комп'ютерних компонент обчислювальної системи обробки цілочислових даних у СЗК полягає в розробці та застосуванні методів і засобів оперативного контролю, діагностики та корекції помилок даних [56].

Використання розроблених методів засобів оперативного контролю, діагности та корекції помилок даних дозволять усунути конфліктну ситуацію між існуючою можливістю значного підвищення швидкодії виконання цілочислових арифметичних операцій у СЗК і низькою оперативністю існуючих систем і засобів контролю, діагности та корекції результатів обчислень у СЗК. Це у свою чергу дозволить вирішити протиріччя між високою швидкодією реалізації цілочислових арифметичних операцій і низькою оперативністю контролю, діагности та корекції даних у СЗК.

1.4 Формулювання проблеми та часткових задач досліджень дисертації

Таким чином, з приведеного вище матеріалу, очевидно, що існуючі методи контролю та діагности помилок даних, які представлені у СЗК не

завжди задовольняють зростаючим вимогам до їх оперативності. Значний час контролю та діагности даних позбавляє однієї з переваг СЗК – надшвидкої реалізації процесу обробки цілочислових даних. Не усунений вищезгаданий недолік процесів контролю та діагности даних КСКОЦД у СЗК, з одного боку, і позитивні попередні результати досліджень, присвячені можливості підвищення оперативності цих процесів, з іншого боку, і визначили мету, наукову-прикладну проблему, часткові задачі досліджень, тему та зміст цієї дисертаційної роботи.

Тема дисертаційної роботи, присвячена розробці та дослідженню методів та засобів оперативного контролю та діагности даних компонент комп'ютерної системи у системі залишкових класів є дуже важливою як на цьому етапі, так і для подальшої перспективи розвитку обчислювальної техніки. Для вирішення конфліктної ситуації, у роботі сформульована нова, важлива та актуальна науково-технічна проблема по розробці методів оперативного контролю та діагностики даних компонентів комп'ютерної системи, що функціонують у залишкових класах.

Для вирішення науково-технічної проблеми в роботі необхідно вирішити наступні часткові задачі досліджень: дослідити методи підвищення оперативності контролю та діагностики цілочислових даних, що представлені у системі залишкових класів, без зниження продуктивності обробки інформації; дослідити вплив властивостей системи залишкових класів на структуру і процес функціонування компонентів комп'ютерної системи обробки цілочислових даних; дослідити коригувальні властивості непозиційних кодових структур у системі залишкових класів; розробити метод контролю даних у системі залишкових класів, що заснований на принципі паралельної нульовизації; розробити метод контролю даних у системі залишкових класів, що заснований на використанні позиційної ознаки непозиційної кодової структури; розробити метод підвищення достовірності оперативного контролю даних, що представлені у системі залишкових класів; вдосконалити метод визначення альтернативної

сукупності непозиційних кодових структур у системі залишкових класів; вдосконалити метод оперативної діагностики даних, що представлені у системі залишкових класів.

Висновки до розділу 1

У першому розділі дисертації вирішено **першу задачу** досліджень.

1. Результати досліджень галузей науки і техніки, де вирішуються задачі обробки цілочислових даних, показали, що усі існуючі методи, системи та засоби контролю та діагностики комп'ютерних систем і компонентів мають значний час реалізації відповідних процедур. Ця обставина обумовлює низьку оперативність існуючих методів, систем і засобів контролю та діагностики помилок у СЗК.

2. У розділі проведено дослідження методів підвищення оперативності контролю та діагностики цілочислових даних, що представлені у системі залишкових класів, без значного зниження продуктивності обробки інформації. Показано, що існуючі методи контролю та діагности цілочислових даних не завжди задовольняють вимогам їх високої оперативності. На підставі результатів проведених досліджень сформульована концепція розвитку комп'ютерних компонент обчислювальної системи обробки цілочислових даних у СЗК, яка полягає в наступному: з метою підвищення ефективності функціонування КСКОЦД необхідно розробити методи, системи та засоби оперативного контролю та діагностики помилок даних. Використання розроблених методів і засобів оперативного контролю та діагности помилок даних дозволяє усунути конфліктну ситуацію між існуючою можливістю значного підвищення швидкодії виконання цілочислових арифметичних операцій у СЗК та низькою оперативністю існуючих систем та засобів контролю та діагности результатів обчислень у СЗК.

3. У цьому розділі сформульована мета, науково-технічна проблема, а також тема дисертації. На підставі сформульованої проблеми у розділі

представлені часткові наукові задачі проблеми досліджень. Визначені об'єкт та предмет досліджень.

Основні положення цього розділу викладені у публікаціях автора [19-21, 23, 24, 28-31, 38, 39, 56].

РОЗДІЛ 2. НАУКОВІ ОСНОВИ ПОБУДОВИ НЕПОЗИЦІЙНИХ КОДОВИХ СТРУКТУР У СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ

2.1 Формулювання принципів побудови непозиційних кодових структур у СЗК

Першим поштовхом до дослідження СЗК, для можливого застосування її у новій непозиційній машинній арифметиці, стали опубліковані в 1955 - 1960 рр. роботи чеських вчених Валаха, Сабо та Свободи. Значний внесок у розвиток теорії та практики непозиційного кодування у залишках і використання його для побудови надпродуктивних, надійних і високостійких КСКОЦД внесли радянські учені : Акушский І. Я., Юдицкий Д. І., Долгов О. І., Амербаев В. М., Лукін Ф. В., Глушков В. М., Лебедєв С. А., Базилевський Ю. А., Шрейдер Ю. А., Андріанов Є. С., Корнев М. Д., Остапенко Н. К., Кисунько Г. В., Боргів А. І., Евстигнєєв В. Г., Червяків Н. І., Синьков М. В., Інютін С. А., Коляда А. А., Пак. И. Т., Вишинський В. А., Торгашов В. А., Морозов В. Н., Фінько О. А., Овчаренко Л. А. та ін. Окрім цього великий внесок у розвиток та становлення СЗК внесли наступні учені: Blum T., Kawamura S., Ko Ae M., Sano F., Shimbo A., Paulier P., Thornton M.A., Dreschler R., Miller D. і багато інших.

Теоретичні основи побудови числової системи у СЗК є розвитком широко відомого в теорії чисел розділу порівнянь. У 1955 – 1957 рр. уперше А. Свобода, М. Волох та інші учені вказали на можливість надмірного кодування цілих чисел за допомогою набору залишків $\{a_i\}$ від ділення цих чисел на взаємно попарно прості натуральні числа $\{m_i\}$, $i=\overline{1,n}$, що називаються основами або модулями СЗК.

Дамо загальне визначення непозиційної системи числення у залишкових класах.

Нехай заданий ряд натуральних чисел $\{m_i\}$, $i=\overline{1,n}$, що називаються

основами (модулями) СЗК. Під системою числення у залишкових класах, в широкому сенсі, розумітимемо таку систему числення, у якій натуральне число A представляється сукупністю залишків (лишків) $\{a_i\}$ від ділення цього числа на основи m_i. Число A представляється у вигляді $A=(a_1,a_2,...,a_n)$, де $a_i = A-[A/m_i]m_i$ [57-59].

Відмітимо, що, як правило, СЗК розуміється і використовується у вузькому сенсі. У цьому випадку задамо набір взаємно попарно простих чисел $m_1, m_2, ..., m_n$, тобто найбільший загальний дільник (НЗД) будь-якої пари основ СЗК дорівнює одиниці, тобто НЗД $(m_i, m_j)=1;\ \ i \neq j$. Для представлення числа A у СЗК необхідно визначити набір таких лишків $\{a_i\}$, щоб виконувалась система наступних порівнянь:

$$\begin{aligned} A &= a_1 (\mathrm{mod}\, m_1), \\ A &= a_2 (\mathrm{mod}\, m_2), \\ &\vdots \\ A &= a_n (\mathrm{mod}\, m_n). \end{aligned},$$

У діапазоні $[0, M)$ обробки даних, де $M=\prod_{i=1}^{n} m_i$, сукупність залишків a_i однозначно визначають число A. Для числа $A \geq M$ це визначення неоднозначне. Таким чином, число A у СЗК представляється у вигляді набору залишків

$$A_{СЗК} = (a_1 \| a_2 \| ... \| a_n).$$

З точки зору інформаційного резервування (використання завадостійких кодів) коди СЗК є подальшим вдосконаленням відомих у ПСЧ арифметичних багатозалишкових AN-кодів. Відомо, що багатозалишковий код у ПСЧ представляється у вигляді

$$A'_k = [A_k; A_k(\mathrm{mod}\, m_1), A_k(\mathrm{mod}\, m_2), ..., A_k(\mathrm{mod}\, m_i), ..., A_k(\mathrm{mod}\, m_{n-1}), A_k(\mathrm{mod}\, m_n)],$$

тобто

$$A'_k = (A_k; a_1 \| a_2 \| ... \| a_n), \text{ де } a_i = A_k - [A_k / m_i]m_i.$$

При виконанні умови $\prod_{i=1}^{n} m_i \geq A_k$, сукупність залишків $\{a_i\}$ однозначно визначає операнд A_k та чисельне значення A_k стає не потрібним, а багатозалишковий код набирає вигляду коду СЗК $A'_k = (a_1 \| a_2 \| ... \| a_n)$, що дозволяє реалізувати модульні операції по окремим незалежним трактам, оперуючи тільки із залишками $\{a_i\}$.

Відповідно до визначення СЗК, НКС $A_{СЗК} = (a_1 \| a_2 \| ... \| a_n)$ утворюється за рахунок отримання залишків $\{a_i\}$ на основі використання принципів утворення залишків a_i числа $A_{СЗК} = (a_1 \| a_2 \| ... \| a_n)$. А саме, наступних принципів.

1. Принцип незалежності утворення залишків $a_i = A - [A / m_i]m_i$ числа $A_{СЗК} = (a_1 \| a_2 \| ... \| a_n)$.

2. Принцип рівноправності будь-якого з n залишків a_i у числі $A_{СЗК} = (a_1 \| a_2 \| ... \| a_n)$.

Принципи утворення залишків a_i числа $A_{СЗК} = (a_1 \| a_2 \| ... \| a_n)$ обумовлюють наступні основні властивості СЗК:

- незалежність залишків $a_i = A - [A / m_i]m_i$ у числі $A_{СЗК} = (a_1 \| a_2 \| ... \| a_n)$;

- рівноправність залишків a_i у числі $A_{СЗК} = (a_1 \| a_2 \| ... \| a_n)$;

- малорозрядність $\alpha = [\log_2(m_i - 1)] + 1$ залишків a_i у СЗК.

Таке представлення чисел дозволяє організувати процес реалізації арифметичних операцій, в якому обробка усіх відповідних залишків чисел

здійснюється незалежно та паралельно у часі. В цьому випадку узагальнена структурна схема КСКОЦД у СЗК буде представляти собою набір окремих мікро-ЕОМ, що функціонують незалежно один від одного та паралельно у часі, причому кожна за своїм визначеним модулем m_i [35, 60, 61].

Як було описано вище, у СЗК кожне число представляється у вигляді сукупності малорозрядних позиційних чисел (лишків), що є залишками від ділення вихідного числа на взаємно прості основи. У звичайній двійковій ПСЧ виконання арифметичної операції (наприклад, додавання двох чисел) виконувалось послідовно по розрядах двійкових чисел, починаючи з молодшого. При цьому може утворюватись одиниця перенесення в наступний старший розряд, що і визначає порозрядну послідовність обробки. На підставі існуючих властивостей СЗК з'явилась можливість розпаралелювати цей процес: усі арифметичні операції над залишками a_i по кожній основі m_i виконуються незалежно по відповідних залишках і паралельно в часі. Отже, у зв'язку з їх малою розрядністю, можливо нескладно і швидко виконувати арифметичні операції при будь-якому методі їх реалізації.

Мала розрядність $\alpha = [\log_2(m_i - 1)] + 1$ залишків a_i числа $A_{СОК} = (a_1 \| a_2 \| ... \| a_n)$ забезпечує можливість реалізації арифметичних операцій у СЗК за допомогою табличної арифметики, при якій результат операції не обчислюється кожного разу, а, одноразово розрахований, поміщається у пристрій, що запам'ятовує (ЗП), і при необхідності зчитується з нього. Тобто при табличній арифметиці арифметична операція у СЗК виконується за один період синхронізуючої частоти (машинний такт). Невирішені задачі виникають при переповнюванні діапазону представлення чисел і при округленні результатів. На рішення цих задач знадобилося маса сил та інтелекту математиків. Табличним методом у СЗК можна виконувати не лише прості операції, але і складні функції, і теж за один машинний такт. Цим визначається одна з парадоксальних властивостей СЗК: ефективна

продуктивність модулярної комп'ютерної системи може бути значно, у рази, у десятки та сотні разів вище, ніж у позиційної з тією ж тактовою частотою (при одній і той самій елементній базі). Дійсно, операцію, яку звичайна КСКОЦД виконує за 100 тактів, модулярна КСКОЦД виконує за один такт, звичайно, її ефективна продуктивність на цих операціях за інших рівних умов у 100 разів вище. Окрім цього, є ще варта уваги особливість СЗК. Так, ввівши до інформаційних основ СЗК додаткові (контрольні) основи, утворюється додаткова інформаційна надмірність, що забезпечує контроль і корекцію помилок у процесі виконання операцій. Арифметичність НКС є однією з найважливіших переваг СЗК перед усіма ПСЧ. Жодна з них не дозволяє знаходити і тим більше виправляти помилки у процесі виконання арифметичних операцій. Навпаки, в арифметичному пристрої вони, раз виникнувши, безконтрольно розмножуються. У результаті у КСКОЦД, що працюючих у традиційних позиційних системах числення, контроль та виправлення помилок (контроль на парність, надмірне кодування, мажорування і тому подібне) забезпечуються тільки у системах зберігання і передачі інформації. Арифметико-логічні пристрої – одне з основних джерел збоїв та помилок у КСКОЦД, залишаються безконтрольними. Зараз, коли увесь процесор розміщується в одному кристалі СБІС, ПЛІС це не так критично. В ті часи, коли процесор займав шафу або декілька, містив багато тисяч окремих елементів і контактів, а також кілометри провідників, він був гарантованим джерелом різних перешкод і збоїв, причому безконтрольних.

Непозиційна система числення у СЗК розглядається як варіант узагальненої системи числення, в якій будь-яке натуральне число *A,* включаючи нуль, представляється у вигляді сукупності найменших позитивних залишків (лишків) від ділення вихідного числа *A* на ряд заданих $m_1, m_2, ..., m_n$ натуральних чисел. У літературі часто не зовсім справедливо термін СЗК ототожнюється з таким поняттям, як "клас лишків" (КЛ). В деяких випадках ця обставина може заважати аналізу результатів рішення завдань обробки даних, представлених у СЗК. У зв'язку з цим важливо

розглянути, як співвідносяться між собою поняття СЗК та КЛ. Дамо визначення поняттю "клас лишків".

Розглянемо множину $\{A\}$ усіх натуральних чисел, включаючи нуль. З безлічі натуральних чисел виберемо довільне число (модуль) m_i. При діленні будь-якого натурального числа A на модуль m_i може вийти наступна сукупність залишків: 0 (число A ділиться на модуль m_i без остачі), 1, 2, ... нацело $m_i - 2$ та $m_i - 1$. Уся безліч натуральних чисел, враховуючи нуль, можна розбити на m_i (0, 1, 2, ... $m_i - 2$ та $m_i - 1$) різних груп чисел (класів лишків), включаючи у кожний КЛ числа, які при діленні на модуль m_i дають однаковий залишок. Вважається, що ці числа порівнянні між собою по модулю m_i. Клас лишків по модулю m_i СЗК можна позначити символом $КЛ_j^{(i)}$, де: i - номер основи впорядкованої ($m_i < m_{i+1}$) СЗК ($i = \overline{1, n}$); j - номер КЛ у системі лишків для цього модуля m_i ($j = \overline{0, m_i - 1}$). У загальному випадку класом лишків $КЛ_j^{(i)}$ по модулю m_i будемо називати безліч усіх цілих чисел, включаючи нуль, які при діленні на модуль m_i дають однаковий позитивний залишок. Враховуючи відоме співвідношення $(-A) \bmod m_i = (m_i \cdot k - A) \bmod m_i (k = 1, 2, 3, ...)$, усі КЛ по довільному модулю m_i СЗК можна представити у вигляді [12, 61]

$$
\begin{array}{lcccccccc}
КЛ_0^{(i)} = & \overline{0} & \{..., & -2 \cdot m_i, & -m_i, & 0, & m_i, & 2 \cdot m_i, & 3 \cdot m_i, & ...\}, \\
КЛ_1^{(i)} = & \overline{1} & \{..., & -(2 \cdot m_i - 1), & -(m_i - 1), & 1, & m_i + 1, & 2 \cdot m_i + 1, & 3 \cdot m_i + 1, & ...\}, \\
КЛ_2^{(i)} = & \overline{2} & \{..., & -(2 \cdot m_i - 2), & -(m_i - 2), & 2, & m_i + 2, & 2 \cdot m_i + 2, & 3 \cdot m_i + 2, & ...\}, \\
КЛ_3^{(i)} = & \overline{3} & \{..., & -(2 \cdot m_i - 3), & -(m_i - 3), & 3, & m_i + 3, & 2 \cdot m_i + 3, & 3 \cdot m_i + 3, & ...\}, \\
 & & \vdots & & & \vdots & & & & \vdots \\
КЛ_j^{(i)} = & \overline{j} & \{..., & -(2 \cdot m_i - j), & -(m_i - j), & j, & m_i + j, & 2 \cdot m_i + j, & 3 \cdot m_i + j, & ...\}, \\
 & & \vdots & & & \vdots & & & & \vdots \\
КЛ_{m_i-2}^{(i)} = & \overline{m_i - 2} & \{..., & -(m_i + 2), & -2, & m_i - 2, & 2 \cdot m_i - 2, & 3 \cdot m_i - 2, & 4 \cdot m_i - 2, & ...\}, \\
КЛ_{m_i-1}^{(i)} = & \overline{m_i - 1} & \{..., & -(m_i + 1), & -1, & m_i - 1, & 2 \cdot m_i - 1, & 3 \cdot m_i - 1, & 4 \cdot m_i - 1, & ...\}.
\end{array}
\qquad (2.1)
$$

Якщо з кожного КЛ (2.1) узяти по одному довільному лишку, то така сукупність з m_i чисел називатиметься повною системою лишків (ПСЛ) по

модулю m_i. Узявши з кожного КЛ по одному певному лешку, складемо можливі варіанти ПСЛ за модулем m_i: 0, 1, 2, 3, ..., $m_i - 1$ – повна система найменших невід'ємних лишків (ПСННЛ); m_i, 1, 2, 3, ..., $m_i - 1$ – повна система найменших додатних лишків (ПСНДЛ); 0, 1, 2, - 2, ..., - 1 - повна система найменших за абсолютною величиною лишків (ПСНАВЛ).

Так, як у межах кожного модуля оперують тільки з натуральними числами, включаючи нуль, то для утворення СЗК з основами $m_1, m_2, ..., m_n$ необхідно з кожної сукупності КЛ використати n ПСННЛ. В цьому випадку всі можливі КЛ ($K^{(1)}$) для першого m_1, для другого ($K^{(2)}$) m_2 та останнього ($K^{(n)}$) m_n модулів СЗК, представлені відповідно виразами (2.2), (2.3) і (2.4).

Для першого m_1 модуля СЗК маємо наступну сукупність КЛ

$$
\begin{aligned}
КЛ_0^{(1)} &= \overline{0} \;\{\; 0, \quad m_1, \quad 2\cdot m_1, \quad 3\cdot m_1, \quad ... \;\}, \\
КЛ_1^{(1)} &= \overline{1} \;\{\; 1, \quad m_i+1, \quad 2\cdot m_1+1, \quad 3\cdot m_1+1, \quad ... \;\}, \\
КЛ_2^{(1)} &= \overline{2} \;\{\; 2, \quad m_1+2, \quad 2\cdot m_1+2, \quad 3\cdot m_1+2, \quad ... \;\}, \\
&\vdots \\
КЛ_{m_1-2}^{(1)} &= \overline{m_1-2} \;\{\; m_1-2, \quad 2\cdot m_1-2, \quad 3\cdot m_1-2, \quad 4\cdot m_1-2, ... \;\}, \\
КЛ_{m_i-1}^{(1)} &= \overline{m_1-1} \;\{\; m_1-1, \quad 2\cdot m_1-1, \quad 3\cdot m_1-1, \quad 4\cdot m_1-1, ... \;\}.
\end{aligned}
\tag{2.2}
$$

Очевидно, що для модуля m_1 СЗК ПСННЛ буде складатися з лишків: $0, 1, 2, ..., m_1 - 1$.

Для другого m_2 модуля СЗК маємо наступну сукупність КЛ

$$
\begin{aligned}
КЛ_0^{(2)} &= \overline{0} \quad \{\ 0, \quad m_2, \quad 2\cdot m_2, \quad 3\cdot m_2, \quad \ldots\ \},\\
КЛ_1^{(2)} &= \overline{1} \quad \{\ 1, \quad m_2+1, \quad 2\cdot m_2+1, \quad 3\cdot m_2+1, \quad \ldots\ \},\\
КЛ_2^{(2)} &= \overline{2} \quad \{\ 2, \quad m_2+2, \quad 2\cdot m_2+2, \quad 3\cdot m_2+2, \quad \ldots\ \},\\
&\qquad\qquad \vdots\\
КЛ_{m_2-2}^{(2)} &= \overline{m_2-2} \quad \{\ m_2-2, \ 2\cdot m_2-2, \ 3\cdot m_2-2, \ 4\cdot m_2-2, \ \ldots\ \},\\
КЛ_{m_2-1}^{(2)} &= \overline{m_2-1} \quad \{\ m_2-1, \ 2\cdot m_2-1, \ 3\cdot m_2-1, \ 4\cdot m_2-1, \ \ldots\ \}.
\end{aligned}
\tag{2.3}
$$

Для модуля m_2 СЗК ПСННЛ буде складатися з лишків: $0, 1, 2, ..., m_2-1$.

Для останнього m_n модуля СЗК маємо

$$
\begin{aligned}
КЛ_0^{(n)} &= \overline{0} \quad \{\ 0, \quad m_n, \quad 2\cdot m_n, \quad 3\cdot m_n, \quad \ldots\ \},\\
КЛ_1^{(n)} &= \overline{1} \quad \{\ 1, \quad m_n+1, \quad 2\cdot m_n+1, \quad 3\cdot m_n+1, \quad \ldots\ \},\\
КЛ_2^{(n)} &= \overline{2} \quad \{\ 2, \quad m_n+2, \quad 2\cdot m_n+2, \quad 3\cdot m_n+2, \quad \ldots\ \},\\
&\qquad\qquad \vdots\\
КЛ_{m_n-2}^{(n)} &= \overline{m_n-2} \quad \{m_n-2, \ 2\cdot m_n-2, \ 3\cdot m_n-2, \ 4\cdot m_n-2, \ \ldots\ \},\\
КЛ_{m_n-1}^{(n)} &= \overline{m_n-1} \quad \{m_n-1, \ 2\cdot m_n-1, \ 3\cdot m_n-1, \ 4\cdot m_n-1, \ \ldots\ \}.
\end{aligned}
\tag{2.4}
$$

Для модуля m_n ПСННЛ буде складатися з лишків: $0, 1, 2, ..., m_n-1$.

Таким чином, СЗК характеризується використанням *n*, по числу основ, ПСННЛ.

Наведемо приклад визначення ПСЛ для модуля $m_i = 5$ СЗК. Класи лишків за модулем п'ять можна представити у загальному вигляді

$$
\begin{aligned}
&\overline{0} \ \{ \ldots -10, \quad -5, \quad 0, \quad 5, \quad 10, \quad \ldots\ \},\\
&\overline{1} \ \{ \ldots -9, \quad -4, \quad 1, \quad 6, \quad 11, \quad \ldots\ \},\\
&\overline{2} \ \{ \ldots -8, \quad -3, \quad 2, \quad 7, \quad 12, \quad \ldots\ \},\\
&\overline{3} \ \{ \ldots -7, \quad -2, \quad 3, \quad 8, \quad 13, \quad \ldots\ \},\\
&\overline{4} \ \{ \ldots -6, \quad -1, \quad 4, \quad 9, \quad 14, \quad \ldots\ \}.
\end{aligned}
$$

Узявши з кожного КЛ по одному лишку, складемо усі варіанти повних систем лишків за модулем п'ять:

0, 1, 2, 3, 4 – ПСННЛ;
5, 1, 2, 3, 4 – ПСНДЛ;
0, 1, 2, - 2, - 1 – ПСНАВЛ.

За визначенням, у СЗК за модулю 5 використовується ПСННЛ 0, 1, 2, 3, 4.

Взагалі, існує думка, що можливо у прямому розумінні СЗК може не називатися системою числення. Дійсно, основи СЗК пов'язані одна з одною так, що вони вибираються певним чином та закріплюються постійними модулями для даної СЧ. Кожна остача по модулю є інформаційно-незалежною від інших остач, проте при реалізації арифметичних операцій у межах кожної остачі використовується, як правило, двійкова або унітарна СЧ.

Таким чином, СЗК, можливо, визначити не як систему числення, а як особливу конструкцію кодової числової структури даних, тобто спеціальним чином закодований блок числових даних [62-64].

Слід зауважити, що у пропонованому підході, СЗК не протиставляється двійковою ПСЧ, а служить як би її розширенням, що дозволяє ефективно вирішувати певний клас задач. Тому, можливо, найбільш ефективним, у даному випадку, представляється підхід, що поєднує у собі комбіноване застосування СЗК та двійкової ПСЧ при побудові спеціалізованих обчислювальних комп’ютерних систем та компонентів. При цьому, наприклад, керування всією комп’ютерною системою може здійснюватися звичайними двійковими командами та блоками, а обробка даних виконується на основі модулярного представлення чисел. Таким чином, використання достоїнств і переваг СЗК, разом з традиційними двійковими методами побудови комп’ютерних систем та компонентів, може привести до

підвищення продуктивності КСКОЦД у цілому.

Для відповіді на питання про доцільність використання СЗК необхідно провести дослідження впливу основних властивостей на структуру і принципи функціонування КСКОЦД. Можлива логічна схема алгоритму досліджень ефективного застосування СЗК може бути представлена у наступному виді:

– визначити області та напрями науки і техніки, де потрібні цілочислові обчислення; показати, в яких задачах та алгоритмах (вказати найбільш важливі з них) застосовуються цілочислові обчислення; в першу чергу задачі та алгоритми, в які входять такі операції як арифметичні операції додавання, віднімання та множення у додатному та у від'ємному числових діапазонах, а також операції арифметичні та алгебраїчні порівняння чисел;

– обґрунтувати вимоги актуальності і необхідності підвищення швидкодії цілочислових обчислень, тобто обґрунтувати необхідність підвищення продуктивності КСКОЦД (щоб підвищити швидкодію цілочислових обчислень необхідно створити КСКОЦД підвищеної (в порівнянні з існуючими) продуктивності);

– розглянути існуючі та можливі перспективні методи підвищення продуктивності КСКОЦД, що функціонують в ПСЧ; можливий висновок: існуючі та перспективні методи підвищення продуктивності КСКОЦД у ПСЧ не завжди задовольняють зростаючим вимогам по підвищенню швидкодії реалізації цілочислових обчислень (виділити головні причини);

– розглянути один з можливих (описаних у сучасній літературі) варіантів створення високопродуктивних КСКОЦД на основі СЗК; на основі аналізу властивостей СЗК та результатів попередніх і сучасних досліджень теоретичних і практичних розробок у сфері застосування непозиційної системи числення, обґрунтувати можливість її ефективного застосування для підвищення продуктивності КСКОЦД.

2.2 Дослідження впливу властивостей СЗК на структуру та процес функціонування компонентів комп'ютерної системи обробки цілочислових даних

Одним з можливих перспективних напрямів в області розробки високопродуктивних, надійних і відмовостійких КСКОЦД є перехід до обробки даних у машинній арифметиці з нетрадиційним представленням операндів. До теперішнього часу найбільше практичне застосування знайшли КСКОЦД, що використовують непозиційні модулярні коди у СЗК.

Коротко проведемо аналіз основних властивостей СЗК [25-27].

1. *Незалежність залишків.* Це дає можливість побудови КСКОЦД у вигляді сукупності (по числу основ СЗК) інформаційно-незалежних трактів обробки даних, що функціонують кожен по своєму окремому модулю m_i СЗК, незалежно один від одного та паралельно у часі. При такій побудові КСКОЦД, обладнання буде мати модульність конструкції, що дозволить здійснювати ремонт і технічне обслуговування апаратури, не перериваючи рішення задачі. У цьому випадку для здійснення профілактичних заходів по технічному обслуговуванню КСКОЦД не потрібен висококваліфікований обслуговуючий персонал.

Структура КСКОЦД у СЗК, що складається з сукупності незалежних трактів обробки даних, дозволяє розпаралелювати алгоритм, що обробляється на рівні мікрооперації, що принципово неможливе для жодної з існуючих ПСЧ. Загальний час обробки даних КСКОЦД, що функціонують у СЗК, визначається часом реалізації операції у тракті обробки даних по найбільшій основі m_i СЗК. Ця обставина дозволяє, використовуючи табличний принцип обробки інформації, реалізувати більшість арифметичних операцій за один такт роботи КСКОЦД.

Окрім цього, помилки, що виникають за рахунок відмов (збоїв) схем обробки значень двійкових розрядів у довільному тракті КСКОЦД, не

"розмножуються", як в ПСЧ, в сусідні старші розряди, а залишаються в межах однієї остачі СЗК. Властивість незалежності залишків дозволила створити унікальну систему контролю та корекції помилок у динаміці обробки даних (без зупинки обробки даних) при введенні мінімальної інформаційної надмірності. Це суттєво для КСКОЦД, що функціонують у режимі реального часу.

У цьому випадку, помилка, що виникла у тракті обробки даних по основі m_i, або зберігається у цьому тракті до кінця обчислень, або самоусувається (наприклад, якщо після спотворення остачі a_i проміжний результат множитиметься на число, що має нульову цифру по основі m_i) у процесі подальших обчислень. При цьому неважливо, мала місце одноразова або багатократна помилки, або навіть пачка помилок довжиною не більше за значення числа $[\log 2(m_i - 1) + 1]$ двійкових розрядів у межах одного залишку по модулю m_i СЗК.

2. *Равноправность залишків.* Будь-який залишок a_i числа A у СЗК містить інформацію про усе початкове число, що дає можливість програмними засобами замінити спотворений тракт по модулю m_i на справний (наприклад, контрольний тракт) по модулю m_j $(m_i < m_j)$, не перериваючи рішення задачі. Відомо, що СЗК з двома контрольними основами дозволяє повністю зберегти працездатність КСКОЦД обробки даних при відмовах будь-яких двох працюючих трактів. При відмовах третього або четвертого трактів, КСКОЦД продовжує виконувати програму обробки даних при деякому зменшенні точності або швидкості обчислень. У цьому випадку видно, що КСКОЦД у СЗК має властивість поступової деградації по надійності функціонування, точності та швидкодії обробки даних.

Ця властивість використання КСКОЦД, що функціонують у СЗК, обумовлює одну з наступних відмітних особливостей класу лишків. Система обробки даних, що функціонує у СЗК, може мати різну надійність при

рішенні конкретної задачі залежно від вимог, що пред'являється до точності, об'єму пам'яті і швидкодії при їх рішенні. Тобто у процесі рішення задачі у реальному часі, можливо, здійснення "обмінних" операцій між точністю обчислень, швидкодією та надійністю функціонування КСКОЦД.

Відмітимо, що спільне використання першої та другої властивостей обумовлює наявність у КСКОЦД одночасно трьох видів резервування: структурного, інформаційного та функціонального.

3. *Малорозрядність залишків.* Ця властивість СЗК дозволяє використати табличний принцип (табличну машинну арифметику) обробки даних. У цьому випадку більшість арифметичних операцій виконуються за один часовий такт роботи КСКОЦД, що істотно підвищує швидкодію реалізації алгоритмів. Одночасно з цим, використання табличних методів обробки даних дозволяє на базі матричних схем створити високонадійні КСКОЦД обробки інформації.

Використання властивостей СЗК дає можливість широкого вибору принципів, методів та варіантів системотехнічних рішень при створенні КСКОЦД.

Відмітимо основні принципи реалізації раціональних операцій у СЗК: суматорнийпринцип (на базі малорозрядних двійкових суматорів); прямий логічний принцип реалізації арифметичних операцій, заснований на описі модульних операцій на рівні систем перемикальних функцій булевої алгебри; принцип кільцевого зсуву, заснований на використанні кільцевих регістрів зсуву; табличний принцип (на основі використання матричних ПЗП).

Ефективність використання властивостей СЗК для підвищення продуктивності обробки даних, відмовостійкості, надійності та живучості функціонування КСКОЦД полягає в наступному.

1. Підвищення продуктивності обробки даних КСКОЦД досягається за рахунок можливості організації у СЗК паралельної обробки інформації і застосування табличного принципу обробки даних.

2. Підвищення відмовостійкості, надійності та живучості КСКОЦД

можливо за рахунок того, що властивість пасивної відмовостійкості апріорі закладена у початковій структурі КСКОЦД, що функціонують у СЗК. Це досягається за рахунок особливої структури вихідних КСКОЦД у СЗК, що має вигляд подібний до виду резервованої обчислювальної структури у ПСЧ.

3. Модульність структури КСКОЦД у СЗК дає можливість ефективніше, ніж у ПСЧ використати спосіб активної відмовостійкості, що робить вузли і блоки КСКОЦД добре пристосованими до контролю та діагности даних.

4. Структура КСКОЦД у СЗК забезпечує взаємний позитивний вплив на надійність і відмовостійкість шляхом використаня одночасно трьох видів резервування: структурного, інформаційного та функціонального. Це дозволяє ефективніше, ніж у ПСЧ використати методи пасивної та активної відмовостійкості.

5. Апріорна схильність структури КСКОЦД у СЗК до адаптації шляхом, наприклад, поступової деградації. Це дає можливість організації процесу контролю і корекції помилок у СЗК у динаміці обробки даних, при введенні мінімальної інформаційної надмірності. Це досягається за рахунок додаткового використання тимчасового резервування.

6. Можливість організації у динаміці передачі та обробки даних, між надійністю функціонування КСКОЦД, швидкодією обробки даних та точністю рішення задачі.

Результати аналізу основних властивостей СЗК дозволяють зробити висновок про те, що такі КСКОЦД, відносяться до легко контрольованих і легко діагностованих об'єктів. Відмічені особливості структури та принципів функціонування КСКОЦД у СЗК сприяють розробці ефективних методів контролю та діагности помилок даних, що не мають аналогів у ПСЧ [65].

Таким чином, використання основних властивостей СЗК дає передумови до можливості створення ефективних методів контролю та діагности помилок даних при введенні мінімальної інформаційної і часової надмірності.

Проте низька достовірність контролю інформації, а також недостатня оперативність процедур діагностики помилок даних у СЗК, обумовлює необхідність вдосконалення існуючих та розробку нових методів контролю та діагностики помилок даних.

2.3 Принципи та методи реалізації цілочислових операцій у СЗК

Характерною рисою сучасного інформаційного суспільства є зміщення вектору значущості інтересів держави у бік розробки та використання нових прогресивних інформаційних технологій, які останніми роками являються складовими стратегічних ресурсів будь-якої країни. Досягнення високих економічних та соціальних результатів, підвищення частки України у світовій економічній системі значною мірою залежить від масштабів і темпів проведення глобальної інформатизації усього суспільства. Одним з найбільш важливих напрямів розвитку науково-технічного прогресу у сфері створення і використання нових телекомунікаційних систем є розвиток і впровадження ефективних комп'ютерних систем і компонентів обчислювальної техніки.

Зростаюча складність сучасних задач обробки цифрових сигналів даних випереджає темпи підвищення обчислювальної потужності існуючих універсальних позиційних комп'ютерів. У цьому аспекті основним напрямом вдосконалення обчислювальних пристроїв у ПСЧ є задоволення вимог неухильного росту продуктивності реалізації цілочислових обчислень. Теоретичні, експериментальні та промислові дослідження, що проводяться, а також розробки в цьому напрямі дозволили обґрунтувати перспективний напрям росту продуктивності реалізації цілочислових обчислень у ПСЧ, заснований на принципі розпаралелювання обчислень [66-68].

Застосування основних методів підвищення продуктивності в ПСЧ, заснованих на розпаралелюванні обчислень, шляхом використання деяких властивостей задач і алгоритмів, що вирішуються, не в усіх випадках дозволяє підвищити продуктивність обчислень. Сфера застосування їх

обмежується класом вирішуваних задач. Окрім цього, сам процес штучного розчленовування алгоритму, визначення і виділення незалежних обчислювальних гілок вимагає великих трудовитрат, причому, не завжди можливе розпаралелювання довільних алгоритмів взагалі. Відмітимо, що усі існуючі методи підвищення продуктивності у ПСЧ мають загальний недолік: неможливість максимально розпаралелювати алгоритми, що вирішуються на рівні елементарних операцій.

Одним з можливих напрямів у рішенні задачі підвищення продуктивності цілочислових обчислень є перехід до машинної арифметики з нетрадиційним представленням операндів. Нині з множини нетрадиційних машинних арифметик для практичного застосування в обчислювальних комп'ютерних системах для обробки цифрових сигналів пропонуються наступні: СЗК; коди Фібоначі; біноміальна система числення; модулярна комплексна арифметика Гауса; арифметика у кільці поліномів.

З перерахованих нетрадиційних машинних арифметик, для швидкої реалізації операцій формування та обробки сигналів у дійсній числовій області обчислень, найбільше практичне застосування отримала СЗК. Малорозрядність залишків у зображенні чисел у СЗК дає можливість широкого вибору варіантів системотехнічних рішень при реалізації модульних операцій [69-71].

Відомо, що на відміну від ПСЧ у СЗК існує три принципи реалізації модульних (арифметичних) операцій. Розглянемо ці принципи.

Суматорний принцип. Методи реалізації модульних операцій, що засновані на суматорному принципі, припускають використання малорозрядних двійкових суматорів по модулю m_i.

Принцип кільцевого зсуву (ПКЗ). Методи реалізації модульних операцій, що засновані на цьому принципі, припускають використання кільцевих регістрів зсуву.

Табличний (матричний) принцип реалізації арифметичних операцій (ТП). Методи реалізації модульних операцій, що засновані на табличному

принципі, припускають використання малорозрядних матричних ПЗП (комутаторів).

Розглянемо методи і алгоритми технічної реалізації модульних арифметичних операцій, що входять до складу операцій процедур формування та обробки сигналів, що засновані на перерахованих принципах реалізації даних у СЗК.

2.3.1 Суматорний принцип реалізації арифметичних операцій у СЗК

У СЗК дії виконуються над числами, що представленими у вигляді спеціальних машинних кодів у прийнятій системі числення. Під системою числення розуміється спосіб позначення чисел з метою визначення їх кількісного значення за допомогою символів, що мають певні кількісні ознаки. Символи, що застосовуються для зображення чисел, називаються цифрами. Залежно від способу зображення чисел, за допомогою цифр, існуючі СС умовно ділять на позиційні та непозиційні системи. Позиційною називається СС, в якій кількісне значення кожної цифри розряду залежить від її місця (позиції) у вихідному числі. У ПСЧ будь-яке число можна зобразити у вигляді послідовності цифр заданої СС

$$A = (a_{\rho-1}, a_{\rho-2}, \cdots, a_1, a_0), \qquad (2.5)$$

де ρ – розрядність операндів.

Причому кожна цифра a_i (2.5) може приймати одне з можливих значень $0 \le a_i \le q-1$. Кількість q різних цифр, що використовуються для зображення чисел у ПСЧ, називається основами q-ічної системи числення ($q = 2$ – двійкова СЧ; $q = 3$ – трійкова СЧ; $q = 10$ – десяткова СЧ і так далі).

Найпростіше реалізуються процеси виконання арифметичних операцій над операндами, що представлені у двійковому коді ($q=2$), тобто у двійковій позиційній системі числення. У цьому випадку операнд представляється у вигляді

$$A = a_{\rho-1}\cdot 2^{\rho-1} + a_{\rho-2}\cdot 2^{\rho-2} + \quad \cdots \quad + a_1\cdot 2 + a_0, \tag{2.6}$$

де $a_i = \overline{0,1}$, $(i = \overline{0,\rho-1})$.

Багаторозрядні двійкові числа додаються, віднімаються, множаться та діляться за тими ж правилами, що і у десятковій СЧ. Оскільки операція додавання грає основну роль в обчислювальному процесі, то розглянемо її детальніше.

У звичайних двійкових позиційних системах числення операція додавання двох чисел $A_{ПСЧ}$ і $B_{ПСЧ}$, де $A = a_{\rho-1}\cdot 2^{\rho-1} + a_{\rho-2}\cdot 2^{\rho-2} + \quad \cdots \quad + a_1\cdot 2 + a_0$, і $B = b_{\rho-1}\cdot 2^{\rho-1} + b_{\rho-2}\cdot 2^{\rho-2} + \quad \cdots \quad + b_1\cdot 2 + b_0$, здійснюється за допомогою використання суматора. Суматор – це вузол, що виконує операцію арифметичного додавання (підсумовування) двох чисел (слів). Під додаванням розуміється процес утворення слів з числовими значеннями $S = s_{\rho-1}\cdot 2^{\rho-1} + s_{\rho-2}\cdot 2^{\rho-2} + \quad \cdots \quad + s_1\cdot 2 + s_0$.

Значення S_{i+1} суми $(i+1)$-го розряду суматора, а також значення C_{i+1} перенесення у сусідній старший розряд суматора визначаються наступними співвідношеннями

$$\begin{cases} C_{i+1} = a_{i+1}\wedge b_{i+1} \vee \left(a_{i+1}\vee b_{i+1}\right)\wedge c_i; \\ S_{i+1} = \left(a_{i+1}\oplus b_{i+1}\right) \bmod 2 \vee c_i. \end{cases} \tag{2.7}$$

$$\begin{cases} C_0 = a_0 \wedge b_0; \\ S_0 = (a_0 \oplus b_0) \bmod 2, \end{cases} \tag{2.8}$$

де a_{i+1}, b_{i+1} – значення $(i+1)$-х розрядів чисел, відповідно, A і B;

a_0, b_0 – значення нульових розрядів чисел, відповідно, A і B;

C_0 – значення сигналу перенесення нульового розряду суматора;

S_0 – значення суми нульового розряду $(a_i, b_i, c_i, s_i \in 0, 1)$.

Схема організації додавання у i -му двійковому розряді $a_{i+1} + b_{i+1} + c_i$ представлена на рис. 2.1, а на рис. 2.2 представлена схема додавання у дворозрядному двійковому позиційному суматорі.

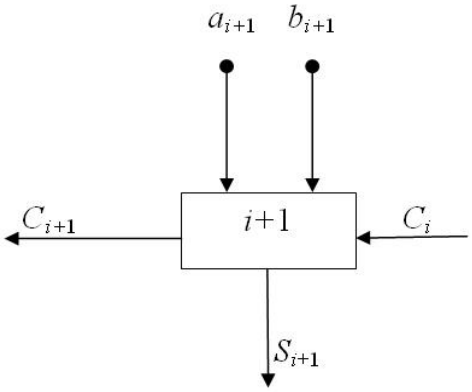

Рис. 2.1 Схема одного $(i+1)$ – го розряду двійкового суматора у ПСЧ

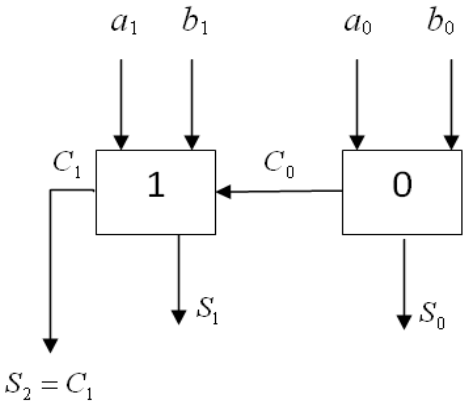

Рис. 2.2 Дворозрядний двійковий суматор у ПСЧ

У таблицях 2.1 і 2.2 представлені алгоритми реалізації арифметичної операції додавання, відповідно, для $(i+1)$-го розряду суматора і для дворозрядного двійкового суматора у ПСЧ.

На рис. 2.3 представлена загальна схема обробки інформації у $(i+1)$-му розряді двійкового суматора у ПСЧ.

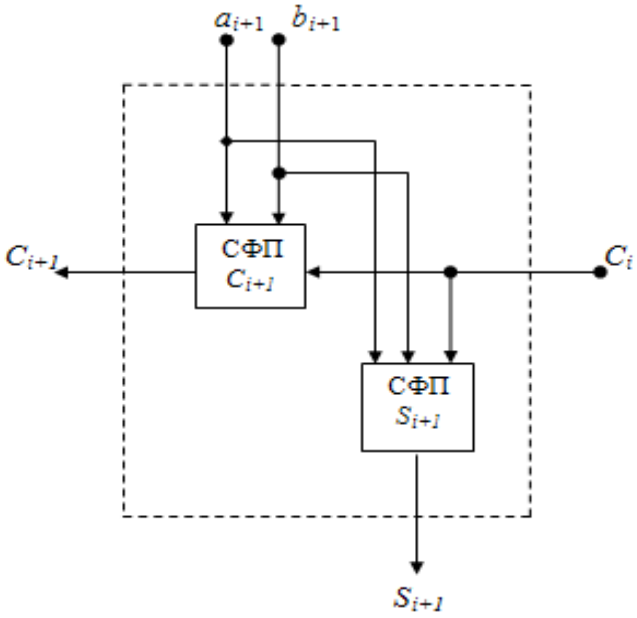

Рис. 2.3 Схема обробки інформації у $(i+1)$-му розряді двійкового суматора у ПСЧ

Таблиця 2.1

Алгоритм обробки інформації в *i*-му розряді суматора у ПСЧ $(i=\overline{0,\rho-1})$

№ п.п.	a_{i+1}	b_{i+1}	C_i	S_{i+1}	C_{i+1}
1	0	0	0	0	0
2	0	0	1	1	0
3	0	1	0	1	0
4	0	1	1	0	1
5	1	0	0	1	0
6	1	0	1	0	1
7	1	1	0	0	1
8	1	1	1	1	1

Схема обробки даних складається з двох окремих схем обробки інформації: схема формування ознаки C_{i+1} перенесення (СФП C_{i+1}); схема формування ознаки S_{i+1} суми (СФС S_{i+1}). На рис. 2.4 представлена принципова схема обробки інформації в $(i+1)$-му розряді двійкового суматора. Аналіз процесу додавання двох чисел за допомогою позиційного суматора показав, що основна складність при реалізації арифметичних операцій у ПСЧ – це організація процесу створення і поширення цифр C_i перенесення від молодшого розряду суматора до старшого розряду [72].

Таблиця 2.2

Алгоритм обробки інформації дворозрядного двійкового суматора у ПСЧ

A		B		S_2	S_1	S_0
a_1	a_0	b_1	b_0			
0	0	0	0	0	0	0
0	0	0	1	0	0	1
0	0	1	0	0	1	0
0	0	1	1	0	1	1
0	1	0	0	0	0	1
0	1	0	1	0	1	0
0	1	1	0	0	1	1
0	1	1	1	1	0	0
1	0	0	0	0	1	0
1	0	0	1	0	1	1
1	0	1	0	1	0	0
1	0	1	1	1	0	1
1	1	0	0	0	1	1
1	1	0	1	1	0	0
1	1	1	0	1	0	1
1	1	1	1	1	1	0

Наявність міжрозрядних зв'язків суматора у ПСЧ обумовлює наступні недоліки:

– тривалість виконання арифметичних операцій, яка залежить від величини l розрядної сітки суматора (для отримання кінцевого результату операції доводиться чекати кінця поширення перенесень C_i на всю довжину машинного слова);

– помилка, що виникла в одному двійковому розряді суматора, у процесі перенесення від молодших розрядів до старших поширюється по всій довжині машинного слова; ця обставина обумовлює той факт, що відмова (збій) схеми обробки інформації одного двійкового розряду суматора здатна викликати не лише одноразові, але і багатократні помилки в отриманому результаті підсумовування.

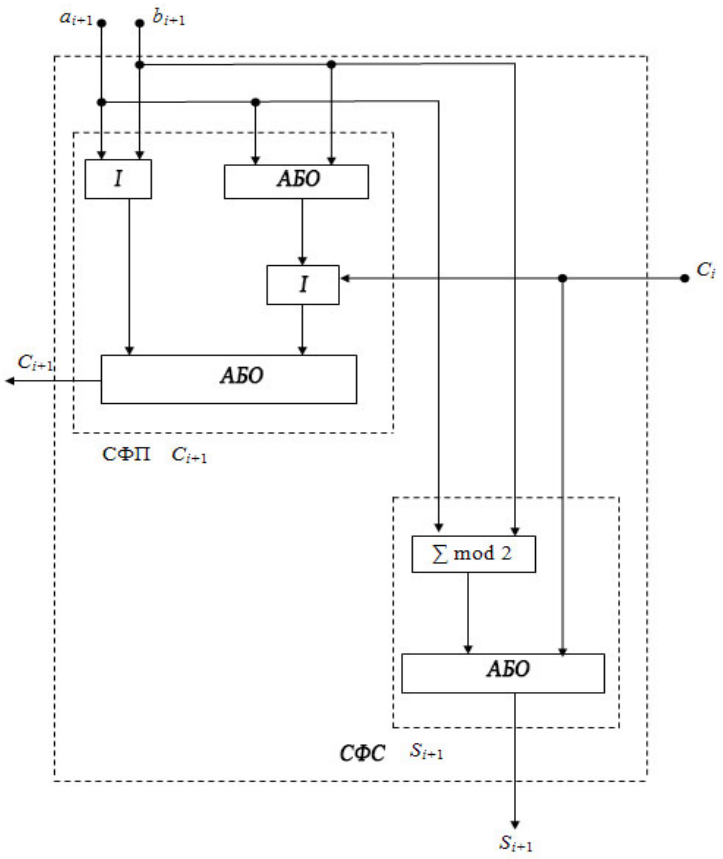

Рис. 2.4 Принципова схема обробки інформації у $(i+1)$-му розряді двійкового суматора у ПСЧ

$$\begin{cases} C_{\rho-1} = S_\rho = a_{\rho-1} \wedge b_{\rho-1} \vee \left(a_{\rho-1} \vee b_{\rho-1}\right) \wedge c_{\rho-2} = a_{\rho-1} \wedge b_{\rho-1} \vee \left(a_{\rho-1} \vee b_{\rho-1}\right) \wedge \\ \wedge \left[\mathrm{a}_{\rho\text{-}2} \ \wedge \ \mathrm{b}_{\rho\text{-}2} \ \vee \ (\mathrm{a}_{\rho\text{-}2} \ \vee \ \mathrm{b}_{\rho\text{-}2}) \ \wedge \ \mathrm{c}_{\rho\text{-}3} \right] = \\ = \overset{\rho\text{-}1}{\underset{i=1}{V}} (\mathrm{a}_{\rho\text{-}\mathrm{i}} \ \wedge \ \mathrm{b}_{\rho\text{-}\mathrm{i}} \ \vee \ \mathrm{a}_{\rho\text{-}\mathrm{i}} \ \vee \ \mathrm{b}_{\rho\text{-}\mathrm{i}}) \ \vee \ (\mathrm{a}_0 \ \wedge \ \mathrm{b}_0). \end{cases} \tag{2.6}$$

$$\begin{cases} S_{\rho-1} = (a_{\rho-1} + b_{\rho-1}) \bmod 2 \vee c_{\rho-2} = \\ = (a_{\rho-1} + b_{\rho-1}) \bmod 2 \vee (a_{\rho-2} \wedge b_{\rho-2} \vee a_{\rho-2} \vee b_{\rho-2}) \wedge c_{\rho-3} = \\ = (a_{\rho-1} + b_{\rho-1}) \bmod 2 \vee (a_{\rho-2} \wedge b_{\rho-2} \vee a_{\rho-2} \vee b_{\rho-2}) \vee \\ \vee (a_{\rho-3} \wedge b_{\rho-3} \vee a_{\rho-3} \vee b_{\rho-3}) \wedge c_{\rho-4} = \\ = (a_{\rho-1} + b_{\rho-1}) \bmod 2 \vee (a_{\rho-2} \wedge b_{\rho-2} \vee a_{\rho-2} \vee b_{\rho-2}) \wedge \\ \wedge (a_{\rho-3} \wedge b_{\rho-3} \vee a_{\rho-3} \vee b_{\rho-3}) \wedge \ldots \wedge (a_0 \wedge b_0) = \\ = (a_{\rho-1} + b_{\rho-1}) \bmod 2 \cdot \overset{\rho-2}{\underset{i=1}{V}} (a_{\rho-1-i} \wedge b_{\rho-1-i} \vee a_{\rho-1-i} \vee b_{\rho-1-i}) \vee (a_0 \wedge b_0). \end{cases} \tag{2.7}$$

Спотворення результату S_{i+1} операції $a_{i+1} + b_{i+1} + c_i$ в $(i+1)$-му двійковому розряді суматора (тобто $S_{i+1} \to \overline{S}_{i+1}$ $1 \to 0$ або $0 \to 1$) залежить від функціонування СФП S_{i+1} (див. вираз (2.7), рис. 2.8). Схема формування ознаки C_{i+1} визначає сигнал перенесення у $(i+2)$-й двійковий розряд суматора. Таким чином, спотворення результату (тобто значень $S_{i+1} \to \overline{S}_{i+1}$ або $C_{i+1} \to \overline{C}_{i+1}$) операції підсумовування у $(i+1)$-му двійковому розряді суматора у ПСЧ відбувається за рахунок відмов (збоїв) схем формування значень S_{i+1} і C_{i+1} (див. рис. 2.4). Помилка виду $C_{i+1} \to \overline{C}_{i+1}$ виникає як за рахунок перенесення помилки $\overline{C}_{i+1}$, що виникла у СФП C_{i+1}, так і у процесі перенесення $(C_{i+1} \to \overline{C}_{i+1})$ значення $\overline{C}_{i+1}$ від $(i+1)$-го розряду до $(i+2)$-го розряду суматора.

Відмітимо основні недоліки суматорного принципу реалізації арифметичних операцій:

– складність синтезу двійкових суматорів;

– значний час перетворення інформації для великих розрядних сіток, що визначається максимальною основою СЗК;

– складність реалізації операції множення;

– не ефективне використання двійкових елементів, внаслідок надмірності максимальних чисел, які можуть бути представлені суматорами, у порівнянні з величинами основ СЗК;

– низька достовірність обчислень за рахунок помилок, що виникають у процесі обчислень та за рахунок або у процесі перенесень проміжних значень порозрядного підсумовування.

Технічна реалізація пристроїв формування та обробки сигналів компонент комп'ютерної системи, як і взагалі схемна реалізація будь-якої системи числення, визначається не лише логічною специфікою, але і обладнанням, що застосовується та організацією цього обладнання [73-75].

2.3.2 Принцип кільцевого зсуву у СЗК

Особливість ПКЗ полягає у тому, що результат арифметичної операції $(a_i \pm b_i) \bmod m_i$ за довільним m_i модулем СЗК, заданою сукупністю $\{m_j\}$ $(j = \overline{1,n})$ основ, визначається без обчислення значень величин S_i і C_i, а тільки за рахунок циклічних зсувів заданої цифрової структури. Дійсно, відома теорема Келі встановлює ізоморфізм між елементами кінцевої абелевої групи та елементами групи перестановок [76-78]. У цьому випадку матриця додавання для довільного m_i модуля СЗК буде задана табл. 2.3 (для $m_i = 5$ – табл. 2.4).

Одним з висновків теореми Келі являється висновок про те, що відображення елементів абелевої групи на групу усіх цілих чисел є гомоморфним. Ця обставина дозволяє організувати процес визначення результату арифметичних операцій у СЗК за допомогою використання ПКЗ. Так, операнд у СЗК представляється набором з n залишків $\{a_i\}$, що

утворюються шляхом послідовного ділення початкового числа A на n попарно простих чисел $\{m_i\}$, $(i=\overline{1,n})$. У цьому випадку сукупність залишків $\{m_i\}$ безпосередньо ототожнюється з сумою n простих полів Галуа виду $\sum_{i=1}^{n} GF(m_i)$. При розгляді методу реалізації арифметичних операцій у СЗК зручно і достатньо розглянути варіант для довільного кінцевого поля Галуа $GF(m_i)$ при $i = const$, тобто для конкретної приведеної системи лишків за модулем m_i. Нехай для заданої операції модульного додавання $(a_i + b_i) \bmod m_i$ у полі $GF(m_i)$ складена таблиця Келі (таблиця. 2.3). З існування нейтрального елементу в полі $GF(m_i)$ витікає, що у табл. 2.3 є рядок (стовпець), в якому елементи цього поля стоять у порядку зростання, а з того факту, що в полі лишків $GF(m_i)$ ці елементи різні (порядок групи дорівнює m_i), витікає, що в кожному рядку (стовпці) табл. 2.3 містяться усі елементи поля рівно по одному разу. Використання перерахованих властивостей дозволяє реалізувати операції модульного додавання та віднімання у СЗК шляхом застосування ПКЗ за допомогою n кільцевих $M = m_i([\log_2(m_i - 1)] + 1)$ - розрядних регістрів зсуву (КРЗ) [79, 80].

Нехай довільна алгебрична система представлена у вигляді

$$S = (G, \otimes ($$

де G - непуста множина;

$\otimes$ - тип операції, що визначена для будь-яких двох елементів a_i, $b_i \in G$.

Операція $\oplus$ додавання у множині класів лишків R, породжених ідеалом J, утворює нове кільце, що називається кільцем класів лишків R/J. Його можна представити у вигляді Z/m_i, де Z – множина цілих чисел $0, \pm1, \pm2, \ldots$. (Якщо основа СЗК m_i – просте число, то Z/m_i – поле). Ця обставина

обумовлює можливість реалізації арифметичної операції додавання у СЗК без міжрозрядних перенесень (як у ПСЧ) шляхом тільки кільцевого зсуву вмісту розрядів КРЗ.

При двійковому кодуванні операндів вихідна цифрова структура для кожного модуля (основи) СЗК представляється у вигляді вмісту першого рядка (стовпця) таблиці модульного додавання (віднімання) $(a_i \pm b_i) \bmod m_i$ виду (див. рис. 2.5)

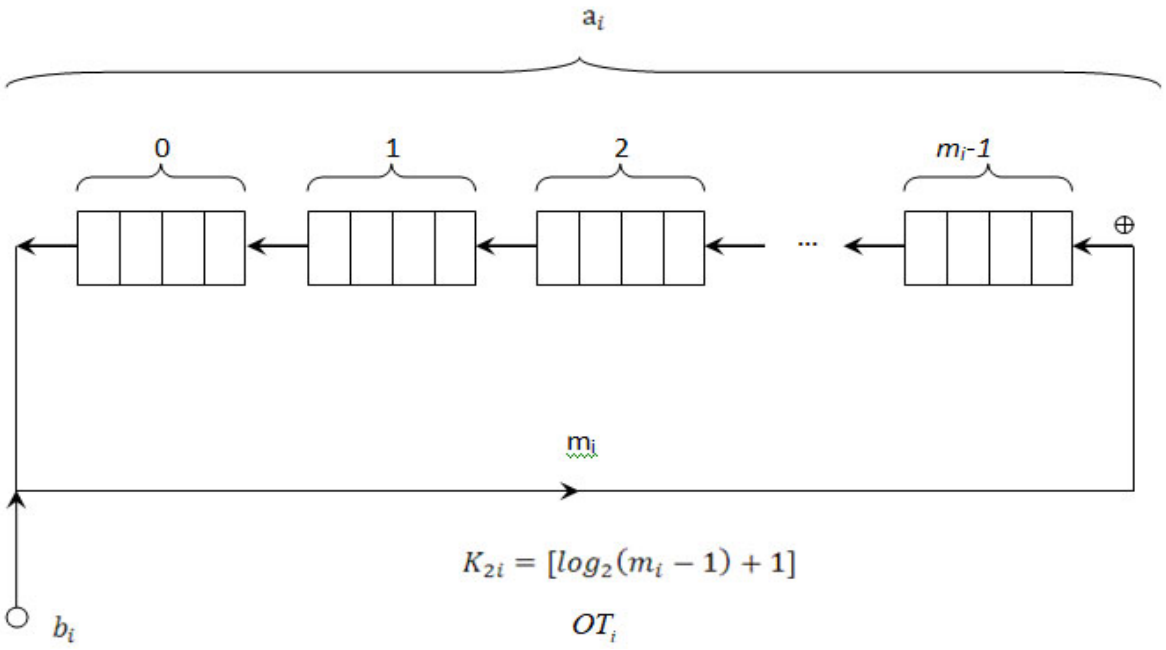

Рис. 2.5 Суматор по модулю m_i у СЗК (BT_i)

$$P_{вих}^{(m_i)} = \left[P_0(a_0) \| P_1(a_1) \| \ldots \| P_{m_i-1}(a_{m_i-1}) \right], \tag{2.8}$$

де || – операція конкатенації (приєднання, склеювання);

$P_v(a_v)$ – k -розрядний двійковий код, що відповідає значенню a_v-го залишку $(a_v = \overline{0, m_i - 1})$ числа по модулю m_i, $k = \left[\log_2(m_i - 1) + 1\right]$.

Для заданого конкретного модуля $m_i = 5$, вихідна цифрова структура вмісту КРЗ має вигляд $P_{вих}^{(5)} = [000 \| 001 \| 010 \| 011 \| 100]$.

Таблиця 2.3

Таблиця Келі для довільного значення m_i

b_i	a_i				
	0	1	2	...	$m_i - 1$
0	0	1	2	...	$m_i - 1$
1	1	2	3	...	0
2	2	3	4	...	1
...	...	...	...	...	...
$m_i - 1$	$m_i - 1$	0	1	...	$m_i - 2$

Таблиця 2.4

Таблиця Келі для $m_i = 5$

b_i	a_i				
	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Таким чином, за допомогою кільцевих регістрів зсуву, що використовуються у ПСЧ, легко реалізувати цілочислові арифметичні операції у СЗК. При цьому ступені циклічних перестановок, виходячи з (2.8), визначаються наступними виразами:

$$\left[P_0(\alpha_0) \| P_1(\alpha_1) \| \ldots \| P_{m_i-1}(a_{m_i-1}) \right] =$$

$$= \left[P_z(a_z) \| P_{z+1}(a_{z+1}) \| \ldots \| P_0(a_0) \| \ldots \| P_{m_i-1}(a_{m_i-1}) \right]^Z ; \qquad (2.9)$$

$$\left[P_0(a_0) \| P_1(a_1) \| \ldots \| P_{m_i-1}(a_{m_i-1}) \right]^{-Z} =$$

$$= \left[P_{m_i-1-z}(a_{m_i-1-z}) \| \ldots \| P_{m_i-z}(a_{m_i-z1}) \| \ldots \| \right.$$

$$\left. \| \ldots P_0(a_0) \| P_1(a_1) \| \ldots \| P_{m_i-z-2}(a_{m_i-z-2}) \right]. \qquad (2.10)$$

Відмітимо, що $\left[P_0(a_0)\,||\,P_1(a_1)\,||\,...\,||\,P_{m_i-1}(a_{m_i-1})\right]^{m_i}=\varepsilon$, тобто при $z=m_i$ усі елементи впорядкованої множини $\left\{P_j(a_i)\right\}$ $(j=\overline{0,m_i-1})$ залишаються на початковому місці. На рис. 2.6 представлена спрощена схема операційного пристрою у СЗК на основі використання ПКЗ. При технічній реалізації цього методу перший операнд a_i визначає номер a_{a_i} розряду $P_{a_i}(a_{a_i})$, з вмістом результату модульної операції за модулем m_i, а другий операнд b_i – число розрядів КРЗ (b_ik –двійкових розрядів), на які необхідно провести зсуви початкового вмісту КРЗ. На рис. 2.7 представлена спрощена схема операційного пристрою для однобайтового $(l=1)$ процесора у СЗК.

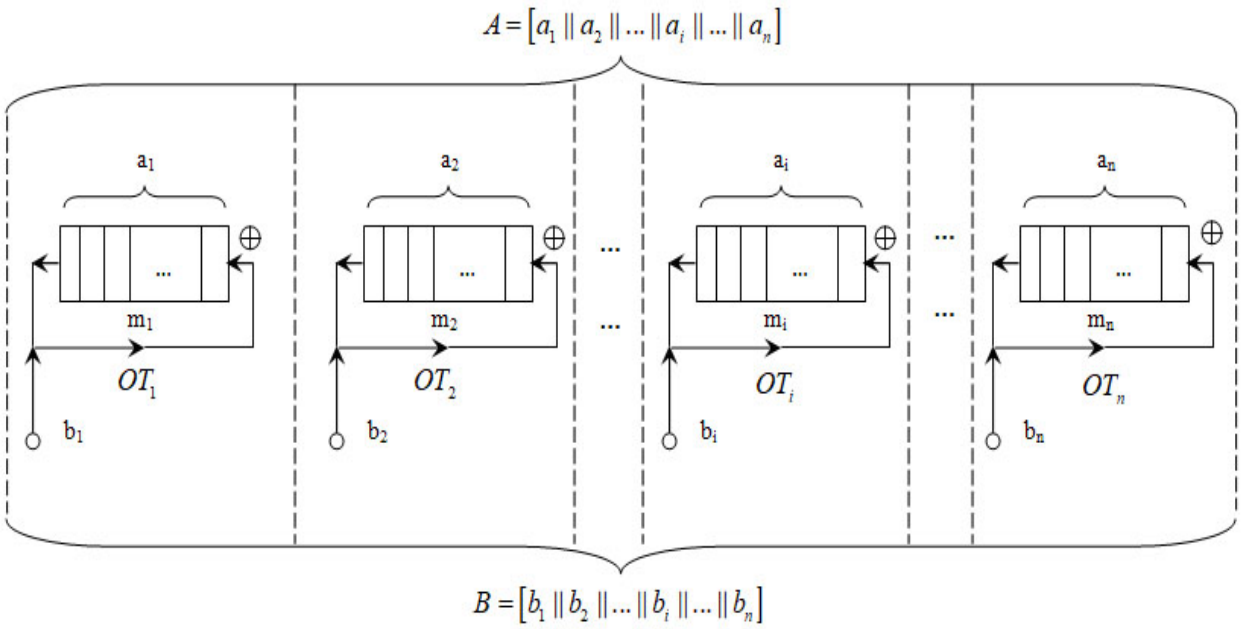

Рис. 2.6 Схема операційного пристрою у СЗК

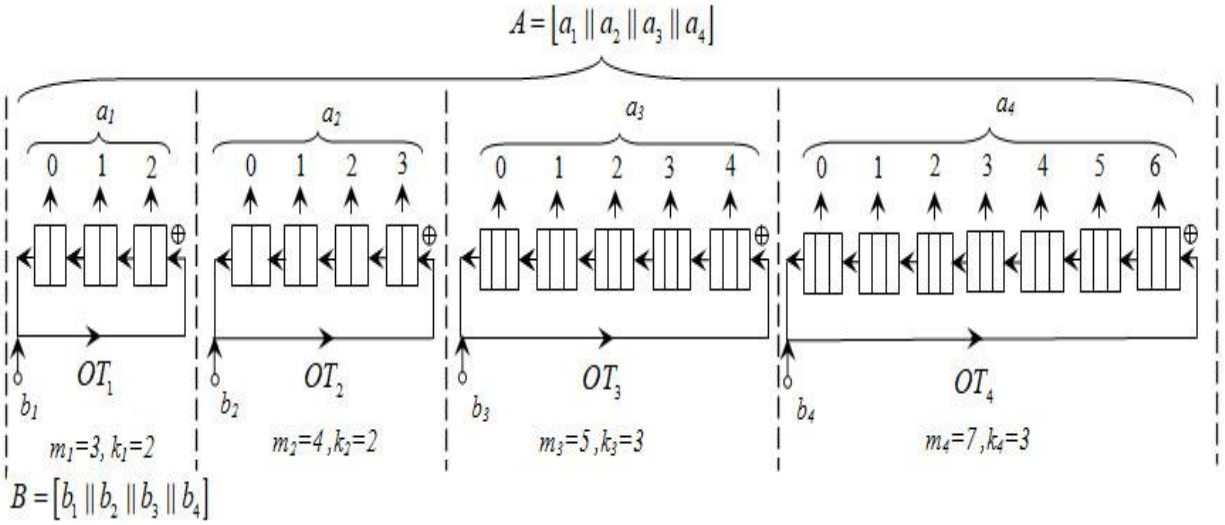

Рис. 2.7 Спрощена схема операційного пристрою у СЗК для однобайтового $(l = 1)$ процесора

2.3.3 Табличний принцип реалізації арифметичних операцій у СЗК

Розвиток сучасної мікроелектронної бази, заснованої в основному на застосуванні великих та надвеликих інтегральних схем, а також програмованих логічних пристроїв (ПЛІС), дав поштовх до дослідження можливості застосування у ПСЧ табличного методу обробки інформації. Застосування табличного методу обробки даних за рахунок можливості розпаралелювання елементарної операції може забезпечити надвисоку продуктивність КСКОЦД.

Таким чином, використання табличного методу обробки даних дуже ефективно для підвищення продуктивності КСКОЦД [81-83].

Таблична реалізація арифметичних операцій у СЗК.

У ПСЧ виконання арифметичної операції припускає послідовну обробку двійкових розрядів операндів за правилами, що визначені змістом цієї операції, і не може бути закінчено до тих пір, поки не будуть послідовно визначені значення усіх проміжних результатів з урахуванням усіх зв'язків

між розрядами [84-86].

Пошук шляхів підвищення продуктивності КСКОЦД реального часу привів до необхідності розробки методу табличної реалізації модульних операцій. У загальному випадку табличний операційний пристрій (ОП) КСКОЦД для реалізації арифметичних операцій (які реалізується в унітарному коді) являє собою двовхідний ПЗП. Для кожного з входів ПЗП кількість вхідних шин для l-байтової ($8l$ двійкових розрядів) КСКОЦД дорівнює 2^{8l}. При цьому загальна кількість логічних схем збігу І у вузлах ПЗП (яке в основному і визначає загальну кількість обладнання табличного операційного пристрою КСКОЦД) дорівнює $N_{\text{l ПСЧ}} = 2^{8l} \times 2^{8l} = 2^{16l}$. Очевидно, що таблична реалізація цілочислових модульних арифметичних операцій у ПСЧ доцільна тільки для значення $l = 1$. Дійсно, у цьому випадку $N_1 = 2^{16} = 65536$, що є прийнятною кількістю обладнання для сучасного розвитку елементної бази. Проте, як відзначалося вище, тенденція розвитку засобів обробки цифрової інформації спрямована на збільшення довжини розрядної сітки КСКОЦД. Так для випадків $l = 4$ та $l = 8$ маємо, що $N_{4ПСЧ} = 2^{32} \times 2^{32} = 2^{64}$ та $N_{8ПСЧ} = 2^{64} \times 2^{64} = 2^{128}$. Якщо врахувати, наприклад, що $2^{32} = 4294967296$, $2^{64} = 18446744073709551616$ та $2^{128} \approx 3{,}4 \times 10^{38}$, то очевидно, що табличний метод реалізації арифметичних операцій у ПСЧ практично не прийнятний. Інші результати можна отримати, якщо розглянути СЗК. Дійсно, у загальному випадку, при реалізації алгоритмів модульної обробки інформації для табличного ОП КСКОЦД потрібно $N_{lСЗК} = \sum_{i=1}^{n} m_i^2$ схем збігу І. Тоді для КСКОЦД у СЗК з $l = 4$ та $l = 8$ відповідно маємо $N_{4СЗК} = 2397$ та $N_{8СЗК} = 13275$, що цілком прийнятно при реалізації арифметичних операцій додавання, віднімання та множення у СЗК при використанні такої елементної мікроелектронної бази як ВІС, НВІС або ПЛІС [87-89].

Основні достоїнства табличного варіанту побудови ОП КСКОЦД у СЗК:

– табличні схеми мають високу надійність, оскільки реалізуються у

вигляді компактних ПЗП; в цьому випадку увесь тракт ОП КСКОЦД будується за блоковим принципом, що покращує ремонтопридатність КСКОЦД (зменшується час відновлення $T_в$ КСКОЦД) [90-92];

– простота побудови табличних схем і дешифраторів, які мають кількість виходів, що відповідають основі СЗК;

– висока швидкодія; результат операції може бути отриманий у момент надходження вхідних операндів, тобто за один такт; час виконання арифметичних операцій у СЗК порівняний з тактовою частотою обчислювача, що принципово неможливе для позиційних обчислювальних машин при існуючій елементній базі.

2.4 Обґрунтування вибору сукупності основ СЗК

Завдання синтезу структури КСКОЦД у СЗК безпосередньо пов'язане з вибором сукупності основ (модулів) СЗК, що безпосередньо визначають діапазон обробки інформації та побічно її апаратурні витрати. Це, у свою чергу, істотним чином впливає на безвідмовність та продуктивність КСКОЦД реального часу. Сформулюємо загальну задачу мінімізації кількості обладнання КСКОЦД при заданих вимогах обробки інформації для даного діапазону розрядної сітки у наступному виді

$$\begin{cases} M = \prod_{i=1}^{n} m_i = const, \\ V_{СЗК}^{(n)} = \sum_{i=1}^{n} f(m_i) \to \min, \end{cases} \qquad (2.11)$$

де M – діапазон розрядної сітки КСКОЦД;

n – число інформаційних модулів КСКОЦД;

$f(m_i)$ – функція зв'язку апаратних витрат для i -го модуля СЗК.

Для суматорного принципу реалізації арифметичних операцій маємо наступне значення функції $f(m_i) =]\log_2 m_i[$. У цьому випадку відносна кількість обладнання, приведена до одного двійкового розряду довжини розрядної сітки КСКОЦД, буде дорівнювати величині $V_{COK} = \sum_{i=1}^{n}]\log_2 m_i[\approx \log_2 M$.

Мінімальним значенням загальних витрат обладнання буде величина log2*M* та оптимізація набору модулів КСКОЦД зводиться до зменшення суми логарифмічних дефектів η_i модулів СЗК по кожній основі, що відповідає раніше викладеним виводам. Згідно з нерівністю Коши маємо наступну нерівність

$$\left[\prod_{i=1}^{n} m_i \right]^{\frac{1}{n}} \le \left[\sum_{i=1}^{n} m_i \right] / n . \qquad (2.12)$$

При табличному принципі реалізації модульних операцій у СЗК маємо те, що $f(m_i) = m_i^2$. У цьому випадку очевидна наступна рівність

$$\prod_{i=1}^{n} m_i^2 = \left[\prod_{i=1}^{n} m_i \right]^2 = M^2 = min . \qquad (2.13)$$

Умови рівності модулів та їх взаємної простоти, при збереженні допустимої величини тимчасових витрат на виконання цілочислових арифметичних операцій, диктує необхідність можливого переходу до багаторівневої (багатоступінчастої СЗК) структури побудови КСКОЦД. Проте ця задача оптимізації вимагає окремих серйозних досліджень. Виходячи з досліджень, проведених у [93-95] та ґрунтуючись на властивостях СЗК сформулюємо у загальному вигляді алгоритм оптимізації основ системи залишкових класів:

– задається ряд натуральних чисел $2,3,4,\ldots$;

– з метою забезпечення взаємно-однозначної відповідності між операндами у СЗК та у ПСЧ у числовому діапазоні $\left[0, M=\prod_{i=1}^{n} m_i\right)$ робиться вибір сукупності основ, які задовольняють умові $M=\prod_{i=1}^{n} m_i \geq 2^l$;

– будь-яка пара основ СЗК повинна задовольняти умові взаємної простоти, тобто НОД $\left(m_i, m_j\right)=1$ для $i, j=\overline{1,n}\ (i \neq j)$;

– з метою простоти реалізації арифметичних операцій у від'ємному числовому діапазоні одна з основ СЗК має бути парною, тобто $M \equiv 0(\mathrm{mod}\ 2)$;

– критерій оптимізації основ СЗК – мінімальна кількість обладнання операційного пристрою КСКОЦД; у формалізованому виді цей критерій представляється по-різному – залежно від принципу реалізації арифметичних операцій; так, для принципу кільцевого зсуву (на основі використання кільцевих регістрів зсуву) критерій оптимізації може бути представлений залежно від методу реалізації ПКЗ; для методу двійкового позиційно-залишкового кодування критерій оптимізації представляється у вигляді $\sum_{i=1}^{n}\left(\left\{\left[\log_2\left(m_{i-1}\right)\right]+1\right\}\right)=\min$, а для методу унітарного позиційно-залишкового кодування – $\sum_{i=1}^{n} m_i=\min$, а для табличного принципу реалізації – $\sum_{i=1}^{n}(m_i)^2=\min$ [96].

Результати оптимізації набору основ СЗК для табличного принципу представлені у табл. 2.5.

Таблиця 2.5

Вихідні дані та результати попередніх розрахунків кількості обладнання КСКОЦД у СЗК

l (n)	ПСЧ (двійкова)		СЗК				δ, %
	$V_{ПН}^{(l)}$	$V_{СН}^{(l)}$	Інформаційні основи	Контрольні основи	$V_{ПН}^{(l)}$	$V_{СН}^{(l)}$	
1 (4)	8	24	m_1=3, m_2=4 m_3=5, m_4=7	m_5=11, m_6=13, m_7=17	10	23	4
2 (6)	16	48	m_1=2, m_2=5, m_3=7, m_4=9, m_5=11, m_6=13	m_7=17, m_8=19, m_9=23, m_{10}=29, m_{11}=31	19	44	8

2.5 Дослідження можливості ефективного контролю та діагностики цілочислових арифметичних операцій у СЗК

У роботі розглядаються системи зі взаємно простими основами СЗК, які мають надмірність представлення чисел, у зв'язку з цим їх можна використати для виявлення та виправлення помилок, що виникають в процесі зберігання, передачі або перетворення інформації і ці коди найбільш придатні для використання у КСКОЦД [44, 97, 98].

Припустимо, що один з символів кодового слова $\tilde{A}$ змінив своє значення у результаті дії якої-небудь завади. Отриманий у результаті новий (спотворений) вектор $\tilde{A}'$ знаходиться на відстані, рівному одиниці від вектора $\tilde{A}$. Таку помилку можна виявити лише у тому випадку, якщо вектор

$\tilde{A}'$ не є кодовим словом. Тому усі кодові слова мають бути віддалені від вектору $\tilde{A}'$ на відстань, більшу одиниці. Чим більше відстань між кодовими словами, тим більше помилок може виявляти ти виправляти такий код.

Кодом, що коригує, у системі залишкових класів назвемо підмножину K множини P, що складається з L різних векторів $\tilde{A}$, кожному з яких відповідає одне і тільки одне число $\tilde{A} \in L$. Оскільки множини K і L містять однакове число елементів, кожному числу $A \in L$ відповідає один і тільки один вектор $\tilde{A} \in K$. Вектори, що належать коду, будемо називати також кодовими славами.

Відповідність між векторами $\tilde{A} \in P$ і числами $A \in L$ можна встановити різними способами. Проте властивості кодів практично не залежать від вибору того або іншого способу, а в основному визначаються лише числами L, M та P. Тому надалі будемо припускати, що числу $A = \{a_1 \| a_2 \| ... \| a_m\}_M$ відповідає вектор $\tilde{A} = (\tilde{a}_1 \| \tilde{a}_2 \| ... \| \tilde{a}_m)$ у тому і тільки тому випадку, якщо $a_i = \tilde{a}_i$ для будь-кого $i = 1, 2, ..., m$. Отже $\tilde{A} = \{A\}_M$.

При оцінці ефективності будь-якого коригувального коду, необхідно знати зв'язок між надмірністю та можливостями виявляти або виправляти помилки. Для визначення цих можливостей найчастіше використовують поняття мінімальної кодової відстані, тобто найменшої відстані між двома будь-якими кодовими словами. Відстанню d між будь-якими двома векторами $\tilde{A}_1$ і $\tilde{A}_2$ з множини P назвемо число компонент, в яких ці вектори відрізняються один від одного.

Надалі під поодинокою помилкою розумітимемо будь-яке спотворення символу, що відноситься до якого-небудь одного модуля, а t-кратною помилкою назвемо будь-які спотворення символів, що відповідають довільним t основам. Проте у деяких випадках при розгляді L-кодів будемо використовувати поняття поодинокої і t-кратних двійкових помилок, розуміючи під ними спотворення символом двійкового представлення

залишків $a_1,...,a_m$. Крім того, будемо вважати, що помилки носять, адитивний характер та однозначно визначаються вектором $\{\Delta\}_M$, вага якого дорівнює кратності помилки. Спотворений вектор $\tilde{A}'$ отримується у результаті додавання (чи віднімання) кодового слова та вектору помилки $\tilde{A}' = \tilde{A} + \tilde{\Delta}$.

Як випливає з вищесказаного R-кодом називається такий коригувальний код, векторам якого відповідають числа, що представлені у СЗК зі взаємно простими основами. Ці коди можуть мати будь-яку мінімальну відстань залежно від ступеня надмірності, причому, для будь-якої заданої СЗК величина R однозначно визначає можливості коригувальні можливості коду. Між коригувальними можливостями R-кодів і точністю обчислень, існує обернено пропорційна залежність. На одній і тій же КСКОЦД можна одні обчислення виконувати з високою точністю, але невеликою надійністю, а інші – з меншою точністю, проте з більш високою надійністю і швидкістю, оскільки час виконання основних операцій пропорційний числу інформаційних модулів.

У тих же випадках, коли відбуваються відмови в апаратурі, тобто помилки носять постійний характер, доводиться безперервно коригувати їх, що істотно зменшує продуктивність КСКОЦД. Особливо неприємні відмови схем додавання і множення в арифметичному пристрої, оскільки у цьому випадку дуже важко виправляти помилки у відповідних символах чисел.

Проте визначною особливістю коригувальних кодів, у системі залишкових класів є те, що вони дозволяють вести обчислення, не виправляючи кожного разу спотворені символи, що обумовлене рівноправністю усіх основ СЗК. При появі постійних помилок в якій-небудь групі основ можна виключити ці модулі з системи і подальші обчислення вести у скороченій СЗК. Природно, що в цьому випадку спотворені символи не робитимуть ніякого впливу на хід обчислень.

Як правило, при виключенні з СЗК якої-небудь основи мінімальна

відстань R-коду зменшується на одиницю (при незмінній точності обчислень). Тому, якщо імовірність одночасної відмови двох або більшого числа модулів досить мала, можна вважати, що R-код, дозволяє виправляти помилки постійного типу у будь-яких $d-2$ основах системи за умови, що основи, в яких локалізуються ці помилки, виключаються з СЗК. При цьому перехід до обчислень у скорочених СЗК не впливає на результати операцій, що виконуються з цілими числами.

Мінімальна відстань для коригувального коду, у СЗК пропорційна числу контрольних модулів k. Як правило, загальне число модулів m, що входять у СЗК, зазвичай є фіксованим, а число інформаційних основ n може змінюватись залежно від вимог, що пред'являються до точності рішення задачі. Чим нижче ці вимоги, тим вище коригувальні можливості R-коду, оскільки $k=m-n$. Тому при відмові у будь-якому модулі можна зберегти коригувальну здатність коду, за рахунок зменшення точності обчислень.

Слід зазначити, що при зменшенні точності обчислень збільшується швидкість обробки інформації, оскільки швидкодія КСКОЦД змінюється прямо пропорційно числу інформаційних модулів.

У системі залишкових класів можна представляти не лише числа, але й адресну частину команд. У результаті з'являється можливість виявляти і виправляти помилки, що виникають у дешифраторі адреси запам'ятовуючого пристрою, лічильнику команд, суматорі індексів та в інших елементах адресного тракту.

Припустимо, що запам'ятовуючий пристрій містить *N* комірок та числа, що відповідають номерам комірок, представлені у СЗК з основами $m_1,...,m_n,m_{n+1}$. Якщо і $m_1<m_2<...<m_{n+1}$ і $M=m_1\cdot m_2\cdot...\cdot m_n$, то такий код може виявити будь-яку поодиноку помилку. Зазвичай при появі помилки у коді адреси доводиться зупиняти КСКОЦД (якщо код не дозволяє виправити цю помилку). Якщо ж адреси представлені у системі залишкових класів, то сигнал помилки можна використати для переходу до тієї частини програми,

яка розміщується у перших M / m_n або меншій кількості комірок запам’ятовуючого пристрою. У цих комірках може зберігатися програма якого-небудь контрольного тесту, після виконання якого відбувається повернення до робочої програми. Якщо помилка була випадковою, коригувальна здатність коду, залишиться незмінною. Якщо ж помилка викликана відмовою якого-небудь елементу адресного тракту, то перехід до виконання програми, що розміщена у комірках з номерами, що не перевищують M / m_n, еквівалентний підвищенню на одиницю мінімальної кодової відстані. При цьому з'являється можливість визначити номер модуля, що відмовив. Виключивши цей модуль із СЗК, можна продовжити виконання робочої програми.

Таким чином, R-код з мінімальною відстанню $d = 2$ дозволяє виправляти поодинокі помилки постійного типу.

Зазвичай у керуючих КСКОЦД використовуються запам'ятовуючі пристрої двох типів. Для зберігання програми та різних констант служить постійний запам'ятовуючий пристрій (ПЗП), а дані (вихідні, проміжні та результати) зберігаються в оперативному запам'ятовуючому пристрої (ОЗП). Тому якщо помилка сталася в адресному тракті ОЗП, то для локалізації модуля, що відмовив, слід перейти до такої ділянки програми, у процесі виконання якої використовуються лише перші M / m_n комірки ОЗУ. Природно, що ця ділянка програми не обов'язково повинна носити тестовий характер.

Припустимо, що КСКОЦД вирішує ряд різних самостійних задач і програми, що відповідають деяким з цих задач, можна розмістити у перших M / m_n комірках ПЗП. Тоді при виключенні якого-небудь модуля попередню коригувальну здатність коду, можна зберегти, якщо обмежитися лише виконанням програм, що розташовані в перших M / m_n комірках ПЗП.

При появі другої помилки номер несправного модуля можна визначити, переходячи до програм, що розташовані у перших $M / (m_{n-1} \cdot m_n)$

комірках і т. д

Таким чином, використання приведеного вище коригувального коду, дозволяє забезпечити безпомилкове виконання усієї програми, що записана у ЗП при відмові будь-якого модуля системи залишкових класів, в якій представлений код адреси, або безпомилкове виконання частини програми, що записана у перших M / m_n комірках ПЗП при відмові двох будь-яких модулів, або частині програми, що записана у перших $M / (m_{n-1} \cdot m_n)$ комірках ПЗП при відмові трьох будь-яких модулів і т.д.

Те ж саме справедливе і для оперативного запам'ятовуючого пристрою. Різниця полягає лише в тому, що при відмові яких-небудь модулів адресного тракту ОЗП доводиться переходити до таких частин програми, при виконанні яких використовуються тільки M / m_n, $N / (m_{n-1}\, m_n)$ комірок ОЗП і т.д.

Тобто застосування системи залишкових класів дозволяє істотно підвищити надійність КСКОЦД. Навіть у тих випадках, коли кількість елементів, що відмовили, перевищує коригувальні можливості R-коду, система все ще може вирішувати ряд найбільш важливих завдань, хоча, швидше за все, з меншою точністю.

У зв'язку з тим, що СЗК має властивості незалежності і рівноправності залишків, навіть у тому випадку, коли вихідна СЗК не надмірна, відмова елементів, що відносяться до будь-якого з модулів, не призводить до повного виходу КСКОЦД з ладу. Якщо яким-небудь чином встановити факт появи помилки і локалізувати її, то, виключаючи несправний модуль з СЗК, можна продовжувати обчислення при деякому зменшенні точності. Тому, застосовуючи для виявлення помилок, що виникають у ході рішення задачі, програмні методи контролю, можна забезпечити високу надійність КСКОЦД, що працюють у системі залишкових класів, не притягаючи практично ніякої додаткової апаратури.

Після локалізації несправної основи надалі машина продовжує працювати у скороченій СЗК, тобто з меншою точністю. Тим часом

несправний блок можна ремонтувати, а усунувши несправність, знову повернутися до обчислень у вихідній системі залишкових класів.

Подібний спосіб доцільно використати лише у тому випадку, коли є додатковий резерв часу для повторного вирішення завдання з почерговим виключенням модулів. Проте зазвичай при рішенні багатьох завдань керування, вихідні величини за час одного прорахунку змінюються не значно. Тому час, що витрачається на повторні рішення задачі, практично не впливає на характеристики системи керування.

Час пошуку несправного модуля можна значно скоротити, якщо замість повторних рішень задачі у скороченій СЗК вести обчислення у повній системі залишкових класів, але використати основи m_{n-1} і m_n у якості контрольних. Звісно, при цьому зменшується точність обчислень у $m_{n-1} \cdot m_n$ раз. Тому, якщо КСКОЦД працює у не надмірній системі залишкових класів, то, вирішуючи задачі у функціональних кодах, можна підвищити надійність машини за допомогою простих програмних методів [99-101].

Висновки до розділу 2

У другому розділі вирішено другу задачу досліджень.

1. З метою визначення можливості створення ефективних методів, систем і засобів оперативного контролю та діагностики даних у СЗК у розділі сформульовані принципи побудови НКС. На підставі сформульованих принципів побудови НКС проведені дослідження впливу властивостей СЗК на структуру і процес функціонування компонентів комп'ютерної системи обробки цілочислових даних. Результати дослідження лягли в основу формулювання принципів технічної реалізації цілочислових арифметичних операцій у СЗК.

У розділі сформульовані три принципи технічної реалізації арифметичних цілочислових операцій: суматорний (на основі використання малорозрядних двійкових суматорів по модулю СЗК); принцип кільцевого зсуву (на основі використання кільцевих регістрів зсуву) і табличний

(матричний) принцип, який заснований на використанні постійних запам'ятовуючих пристроїв.

На основі результатів досліджень показана можливість створення ефективних методів, систем і засобів контролю, діагностики і корекції даних у СЗК.

2. На основі використання принципів технічної реалізації арифметичних операцій, у розділі розглянуті методи реалізації цілочислових операцій, на підставі яких розроблені алгоритми виконання модульних і немодульних операцій, відповідно до яких синтезований клас пристроїв обробки даних у СЗК. Приведені оцінки апаратної і часової складності реалізації цих методів.

На розроблені пристрої обробки даних у СЗК отримано 35 патентів України.

Основні положення цього розділу викладені у публікаціях автора [60, 61, 65, 76-80, 89-91, 95].

РОЗДІЛ 3. ОСНОВИ ТЕОРІЇ ЗАВАДОСТІЙКОГО КОДУВАННЯ ДАНИХ У СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ. МЕТОД ФОРМУВАННЯ ПОЗИЦІЙНОЇ ОЗНАКИ НЕПОЗИЦІЙНОЇ КОДОВОЇ СТРУКТУРИ

3.1 Основні поняття та визначення теорії завадостійкого кодування даних у СЗК

У загальному випадку, для корекції помилок даних необхідно, щоб кодова структура мала певну коригувальну здатність. Для цього треба ввести певну інформаційну надмірність, тобто застосувати метод інформаційного резервування. Це повною мірою відноситься до НКС у СЗК [102, 103].

Для будь-якого довільного СЗК величина надмірності $R = M_0 / M$ однозначно визначає коригувальні можливості непозиційного завадостійкого коду. Коригувальні коди, у СЗК можуть мати будь-які значення мінімальної кодової відстані (МКВ) $d_{\min}^{(СЗК)}$. Це залежить від значення величини R надмірності. Зв'язок між надмірністю R коригувального коду, значенням $d_{\min}^{(СЗК)}$ МКВ, і кількістю k контрольних основ СЗК наступна. Коригувальний код, має значення $d_{\min}^{(СЗК)}$ МКВ у тому випадку, якщо ступінь R надмірності не менше добутку будь-яких $d_{\min}^{(СЗК)} - 1$ основ СЗК. З одного боку маємо, що $R \geq \prod_{i=1}^{d_{\min}^{(СЗК)}-1} m_{q_i}$, а з іншого боку – $R = M_0 / M = \prod_{i=1}^{n+k} m_i / \prod_{i=1}^{n} m_i = \prod_{i=1}^{k} m_{n+i}$. У цьому випадку, правомірно стверджувати, що $d_{\min}^{(СЗК)} - 1 = k$ або

$$d_{\min}^{(СЗК)} = k + 1. \tag{3.1}$$

Існує два підходи до рішення задачі забезпечення НКС у СЗК необхідними коригувальними властивостями.

Перший підхід. Знаючи вимоги до коригувальних властивостей НКС, наприклад, по кількості тих, що виявляються $t_{виявл.}$ або тих, що виправляються $t_{випр.}$ помилок, ввести, за рахунок кількості k або величини $\{m_{n+k}\}$ контрольних основ, необхідну інформаційну надмірність R. Надмірність R визначає мінімальну кодову відстань $d_{\min}^{(СЗК)}$ НКС у СЗК.

Тоді, відповідно до теорії завадостійкого кодування, для впорядкованої $(m_i < m_{i+1})$ СЗК маємо, що

$$t_{виявл.} \le d_{\min}^{(СЗК)} - 1, \tag{3.2}$$

$$t_{виявл.} \le k; \tag{3.3}$$

$$t_{випр.} \le \left[\frac{d_{\min}^{(СЗК)} - 1}{2} \right], \tag{3.4}$$

$$t_{випр.} \le \left[\frac{k}{2} \right]. \tag{3.5}$$

Другий підхід. При заданій НКС $A_{СЗК} = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n \| ... \| a_{n+k})$ (при заданому значенні k) коригувальні можливості (що визначаються значенням $d_{\min}^{(СЗК)}$) коду у СЗК визначаються відповідно до виразів (3.3) і (3.5).

Відмітимо, що якщо впорядкована СЗК розширюється шляхом додавання k контрольних основ до n інформаційних модулів, то МКВ $d_{\min}^{(СЗК)}$ завадостійкого коду збільшується на величину k (див. вираз (3.1)).

Збільшити значення $d_{\min}^{(СЗК)}$ можна також за рахунок зменшення числа n інформаційних основ, тобто за рахунок переходу до обчислень з меншою точністю. Вочевидь, що між коригувальними можливостями

завадостійких кодів R і точністю W обчислень у СЗК існує обернено пропорційна залежність. Одна і та ж КСКОЦД може виконувати арифметичні та інші операції з високою W точністю, але невеликою коригувальною здатністю R або з меншою W точністю, але з більш високою коригувальною можливістю R по контролю, діагности та виправленню помилок даних, а також з більш високою швидкодією обробки даних (час виконання основних операцій у СЗК обернено пропорційний до числа n інформаційних основ) [44, 104, 105].

Оцінка ефективності застосування класу лишків для підвищення оперативності контролю даних КСКОЦД значно залежить від конкретної структури цифрового пристрою обробки даних та від елементної бази, що використовується. Вона також залежить і від вимог, які пред'являються до точності, швидкодії, надійності та достовірності рішення задач комп’ютерної системи. У той же час достовірність отриманого результату обчислень залежить від організації процедур контролю та діагностики помилок. Для цього розглянемо основні поняття та визначення теорії завадостійкого кодування у СЗК.

Зв'язок між мінімальною відстанню коду, тобто найменшою відстанню між кодовими словами, і його коригувальними можливостями, встановлюється наступними двома відомими твердженнями [44].

Твердження 3.1. Коригувальний код у СЗК може виявити вусі сукупності з l або меншого числа помилок лише у тому випадку, якщо мінімальна кодова відстань коду більша за l, тобто

$$d_{\min} \geq l + 1. \tag{3.6}$$

Твердження 3.2. Коригувальний код у СЗК може виправити усі сукупності з k або меншого числа помилок лише у тому випадку, якщо мінімальна кодова відстань коду більше подвоєного числа помилок, тобто

$$d_{\min} \geq 2k+1. \qquad (3.7)$$

Покажемо необхідність виконання умови (3.7) для корекції k-кратних помилок. Якщо мінімальна відстань коду менша, ніж $2k+1$ то знайдуться, принаймні, два кодові слова A_1 і A_2, різниця яких має вагу, що не перевищує $2k$. Відповідно завжди можна знайти два такі вектори помилок Δ_1 і Δ_2, що $A_1 - A_2 = \Delta_1 - \Delta_2$. Отже, за значенням спотвореного вектору не можна однозначно отримати кодове слово, що і вимагалося довести.

З тверджень 3.1 і 3.2 витікає, що коригувальний код у СЗК, що виправляє будь-які k помилок і, крім того, що виявляє будь-які $k+1$ помилок, повинен мати мінімальну відстань, рівну $2k+1$. Таким чином, визначивши мінімальну відстань коду, можна отримати уявлення про його коригувальні можливості. Слід враховувати, що мінімальна відстань є досить грубою характеристикою, що не розкриває повністю структуру і можливості коду. Зокрема, якщо відстань між більшістю кодових слів перевищує мінімальну, то такий код можна використати для виявлення або виправлення значної частини помилок більш високої кратності в порівнянні з кратностями, що визначаються твердженнями 3.1 і 3.2. Тому можна вважати, що мінімальна кодова відстань коду дозволяє встановити, лише гарантовану кількість помилок, що виявляються або виправляються. Відмітимо, що мінімальну кодову відстань коду можна визначити, якщо відомі ваги кодових слів.

Твердження 3.3. Мінімальна кодова відстань коригувального коду, у СЗК дорівнює мінімальній вазі ненульових кодових слів, якщо множина L не містить числа протилежних знаків.

Обмеження, що накладаються твердженням 3.3 на безліч L, не відносяться до L-кодів, оскільки у цих кодів на відміну від двох інших коригувальних кодів у СЗК сума, різниця та добуток будь-яких кодових слів обов'язково є кодовими словами.

У класі лишків *R*-кодом називається такий коригувальний код, векторам якого відповідають числа, що представлені у СЗК зі взаємно простими основами. Ці коди можуть мати будь-яку мінімальну відстань залежно від ступеня надмірності, причому, як випливає з приведеної нижче теореми, для будь-якої заданої СЗК величина R однозначно визначає коригувальні можливості коду.

Твердження 3.4. Коригувальний *R*-код має мінімальну кодову відстань d у тому і тільки у тому випадку, якщо ступінь надмірності R не менше добутку будь-яких $d-1$ основ заданої СЗК

$$R \geq \prod_{j=1}^{d-1} m_{q_j}, \text{ де } q_j = 1,2,...,m. \tag{3.8}$$

Доказ. Розділивши число M на ліву і праву частини нерівності (3.8), отримаємо наступний вираз:

$$L = \frac{M}{R} \leq \frac{M}{\prod_{j=1}^{d-1} m_{q_j}} = \prod_{j=1}^{m-d+1} m_{q_j}. \tag{3.9}$$

Число A, що відповідає будь-якому кодовому слову A за абсолютною величиною менше L і тому не може ділитися ні на який добуток $m-d+1$ модулів СЗК. Якщо число A ділиться на деякий модуль m_i, то відповідна компонента вектору A повинна дорівнювати нулю. Тому число нульових компонент вектору A не може бути більше $m-d$ і, отже, вага вектору A не менша, ніж d. Якщо усі числа A мають однакові знаки, то з твердження 3.3 витікає, що d є мінімальною кодовою відстанню коригувального коду у СЗК.

Припустимо тепер, що множина L містить L_1 від'ємних чисел. Розглянемо множину цілих додатних чисел B, що отримані шляхом додавання до кожного числа A величини L_1, тобто $B = A + L_1$. Відповідно до

приведеного вище доказу множина векторів *B* утворює коригувальний код, з мінімальною відстанню *d.* Але мінімальні відстані отриманого та вихідного кодів мають бути рівні по побудові. Тому навіть у разі різних по знаку чисел *A* теорема справедлива. Доведемо тепер необхідність умови (3.8). Припустимо, що добуток деяких $d-1$ основ СЗК більше, ніж *R.* Тоді

$$L => \prod_{j=1}^{m-d+1} p_{q_j} . \qquad (3.10)$$

Тому серед кодових слів знайдуться, принаймні, два вектори A_1 і A_2 такі, що

$$A_1 - A_2 = \prod_{j=1}^{m-d+1} p_{q_j} . \qquad (3.11)$$

Отже, вектор $A_1 - A_2$ містить $m-d+1$ нульових компонент, тобто вага його дорівнює $d-1$. Тому мінімальна відстань коду (у даному випадку відстань між векторами A_1 і A_2) менше d, що суперечить умові теореми. Отже, теорема доведена повністю.

Покажемо тепер, що *R*-код може виявляти і виправляти деяке число помилок більш високої кратності, ніж та, яка допускається, відповідно до тверджень 3.1, 3.2 і мінімальною відстанню коду. Припустимо, що мінімальна відстань коду дорівнює *d,* але у то же час є такі основи СЗК, число яких $d_1 \geq d$, що добуток цих модулів менший за R. Тоді будь-які помилки у цих модулях можна виявити. Дійсно, у векторі помилки Δ повинно бути не менше $m-d_1$ нульових залишків. Позначимо добуток модулів, яким відповідають спотворені символи (тобто ненульові складові вектору Δ) через $Q(d_1)$. Тоді число Δ кратне величині $M / Q(d_1) \geq M / R = L$ і, отже, задовольняє нерівності

$$M - L \geq \Delta \geq L. \qquad (3.12)$$

Неважко переконатися у тому, що сума будь-якого числа A і числа, що відповідає вектору помилки, не може належати множині L, тобто подібну помилку можна виявити. Проте навіть в тих випадках, коли добуток основ, що відповідають помилковим символам, більше R, серед помилок знайдуться такі, які задовольняють нерівності (3.12) і, отже, можуть бути виявлені. Число різних помилок, що відповідають довільним ($t \geq d$) основам СЗК, дорівнює $Q(t)-1$. Ці помилки відповідають числам, рівномірно розподіленим в інтервалі $(0, M)$ з кроком $M / Q(t)$. Якщо $Q(t) > R$, то знайдеться $[Q(t)-1/R]$ помилок, які не задовольняють нерівності (3.12). Доля таких помилок від загальної їх кількості не перевищує величини $1/R$. Тому можна стверджувати, що R-код дозволяє виявляти усі помилки кратності $d-1$ і меншій, а також велику частину $[(R-1)/R]$ помилок більш високої кратності.

Припустимо тепер, що коригувальний R-код з непарною мінімальною відстанню d використовується для виправлення помилок кратності k і нижче, де $k = (d-1)/2$. Нехай вектор A_1' утворений з кодового слова A_1 у результаті дії помилки, вага якої більша за k. Якщо на відстані $d \leq k$ від вектору A_1' знайдеться кодове слово A_2, то воно буде прийнято кодом за правильне значення початкового вектору. Помилку можна було б виявити, якби в межах відстані k від вектору A_1' знайшлося ще одне кодове слово A_3. Але такої ситуації бути не може. Так, як, в цьому випадку, відповідно до властивості метрики непозиційних кодових структур СЗК, кодова відстань між A_2 і A_3 виявилася б не більше, ніж $2k$, тобто менше мінімальної кодової відстані. Таким чином, для виявлення такої помилки необхідно щоб на відстані k від вектору A_1' не було жодного кодового слова. Відповідно, якщо ми хочемо виправити t-кратну помилку, де $t > k$, то серед усіх векторів, що

знаходяться на відстані $d \le t$ від вектору A_1', має бути лише одне кодове слово A_1.

У загальному випадку досить складно оцінити долю помилок довільної ваги t, які можна виявити або виправити за допомогою коду з мінімальною відстанню, меншою $d \le 2t+1$. Річ у тому, що навіть при досить грубих оцінках необхідно знати не лише величину R, але і величину кожного з модулів СЗК (під помилкою у модулі m_i надалі розуміється спотворення відповідного залишку a_i числа у СЗК). Наприклад, долю довільних помилок, які не можуть бути виявлені кодом, що виправляє k помилок при мінімальній відстані $d = 2k+1$, можна оцінити виходячи з таких міркувань. Кожен вектор простору M можна вважати геометричною точкою. Розглянемо безліч сфер радіусу k, центри яких знаходяться у точках, що відповідають різним кодовим словам. Жодна пара таких сфер не може мати загальних точок, оскільки інакше відстань між центрами таких сфер виявилася б менше мінімальної відстані коду. Кожна сфера містить однакове число точок V, рівне кількості різних векторів з вагою, що не перевищує k V можливо визначити суму всіх добутків з k чи меншого числа основ СЗК.

У цьому випадку доля векторів, які знаходяться на відстані $d > k$ від кодових слів, визначається як

$$(M - LV) / M = (R - V) / R. \qquad (3.13)$$

При довільних значеннях помилки і кодового слова A_1 вектор A_1' може потрапити з рівною імовірністю у будь-яку точку простору. Тому можна вважати, що вираження (3.13) визначає ймовірність того, що цей код зможе виявити довільну помилку. Приведена оцінка є не дуже точною, оскільки не враховує залежність між ймовірністю виявлення помилки і величиною t, що відповідає вазі самої помилки.

3.2 Дослідження коригувальних можливостей кодів у СЗК

Розглянемо деякий вектор $A=(a_1 \| a_2 \| ... \| a_n)$, компонентами якого є натуральні числа, що задовольняють умові: $0 \le a_i \le m_i - 1$, де $i = 1,2,...,n$; $m_1, ..., m_n$ – фіксовані натуральні числа. Очевидно, що число різних (тобто, що відрізняються хоча б однією компонентою) векторів такого типу дорівнює добутку $M = m_1 \cdot m_2 \cdot ... \cdot m_n$ (буквою M позначимо також безліч усіх векторів подібного виду, тобто $A \in M$). Таким чином, залежно від контексту під символом M розуміється або множина векторів *A*, або кількість елементів цієї множини.

З іншого боку, розглянемо множину *L*, що містить *L* цілих чисел *A*, таких, що якщо які-небудь два числа A_1 і A_2 належать множині *L*, то і будь-яке ціле число, що лежить між числами A_1 і A_2, також належить цій множині. Будемо вважати, що до складу множини *L* обов'язково входить нуль.

Як було показано у розділі 3.1, будь-яке число з множини *L* можна представити у системі залишкових класів із загальною основою, $M = [m_1, ..., m_n]$, якщо $L \le M$. Кожному числу $A \in L$, що представлене у даній СЗК, можна поставити у відповідність деякий вектор $A \in M$, але зворотне твердження справедливе, лише у тому випадку, якщо $M = L = M_0$. При дотриманні цієї умови будемо говорити про безнадмірне представлення чисел у СЗК [106].

Вочевидь, що якщо основи системи залишкових класів не є взаємно простими, то представлення чисел у такий СЗК завжди надмірне, оскільки $M < M_0$. Для системи зі взаємно простими основами $M = M_0$ і тому питання про надмірність представлення чисел залежить від співвідношення між *L* та M_0. Ступінню надмірності представлення чисел у СЗК назвемо величину $R = M_0 / L$. Надмірність представлення чисел у СЗК можна використати для виявлення та виправлення помилок, що виникають в процесі зберігання, передачі або перетворення інформації.

Коригувальним кодом у системі залишкових класів назвемо підмножину K множини M, що складається з L різних векторів A, кожному з яких відповідає одне і тільки одне число $A \in L$. Оскільки множини K і L містять однакове число елементів, кожному числу $A \in L$ відповідає один і тільки один вектор $A \in K$. Вектори, що належать коду, будемо називати також кодовими словами. Відповідність між векторами $A \in M$ і числами $A \in L$ можна встановити різними способами. Проте властивості кодів практично не залежать від вибору того або іншого способу, а в основному визначаються лише числами L, M та M_0.

Залежно від співвідношення між величинами L, M та M_0 у СЗК усі коригувальні коди можна розбити на три основні класи.

До першого класу відносяться коди, що відповідають СЗК зі взаємно простими основами. Ці коди найбільш придатні для використання у КСКОЦД. Такі коди надалі будемо називати R-кодами.

Кодам другого і третього класів відповідають співвідношення $L = M < M_0$ та $L < M < M_0$. У обох випадках основи системи залишкових класів не є взаємно простими. Перші з цих кодів назвемо L-кодами, а другі – RL-кодами. Нехай, наприклад, є СЗК, що задана основами 3, 4, 5. Якщо $L = 12$, то даній СЗК відповідає R-код, у якого $M = M_0 = 60$; $R = 5$. Класу лишків з основами 3, 4, 6 відповідає L-код, у якого $L = M = 12$; $M_0 = 72$. Нарешті, системі з основами 3, 4, 5, 6 відповідає RL-код ($L = 12$, $M = 60$, $M = 360$).

Розглянемо тепер деякі загальні поняття, характерні для усіх коригувальних кодів, у СЗК.

При оцінці ефективності будь-якого коригувального коду, необхідно знати зв'язок між надмірністю і можливостями виявляти і виправляти помилки. Для визначення цих можливостей найчастіше використовують поняття мінімальної кодової відстані $d_{\min}$, тобто найменшої відстані між двома будь-якими кодовими словами.

Кодовою відстанню d між будь-якими двома векторами (числами) A_1 і A_2 з множини M назвемо число компонент, в яких ці вектори відрізняються один від одного. Безпосередньо з визначення слідують такі властивості цієї кодової відстані :

$$\left.\begin{array}{ll} 1) & d(A_1, A_2) = d(A_2, A_1); \\ 2) & d(A_1, A_2) = 0 \quad \text{тоді і тільки тоді, коли } A_1 = A_2; \\ 3) & d(A_1, A_2) \geq 0; \\ 4) & d(A_1, A_2) \leq d(A_1, A_3) + d(A_2, A_3). \end{array}\right\} \qquad (3.14)$$

Відстань, що задовольняє перерахованим властивостям, часто називають метрикою, а множину елементів, в якій задана метрика – метричним простором. Величина відстані між різними векторами великої кількості M змінюється в межах від 1 до m. Цікаво відмітити, що двом сусіднім числам A_1 і A_2 (що відрізняється на одиницю) відповідають вектори A_1 і A_2, відстань між якими дорівнює m для будь-якої системи залишкових класів.

Визначимо операції додавання, віднімання і множення векторів у просторі M так само, як визначалися формальні модульні операції над числами, що представлені і СЗК. Вектори, яким відповідають числа, що представлені у СЗК, одночасно є скалярними величинами. Таким чином, операція множення вектору на скаляр не відрізняється від множення двох векторів. Кожному вектору з множини M можна присвоїти певну вагу. Вагою або ваговою функцією $W(A)$ вектору A назвемо число ненульових компонент цього вектору.

Очевидно, що відстань між двома векторами дорівнює вазі їх різниці, тобто

$$d(A_1, A_2) = W(A_1 - A_2) \qquad (3.15)$$

Приведемо тепер декілька корисних властивостей вагових функцій, які

безпосередньо витікають із співвідношень (3.14), що визначають метрику, і вирази (3.15):

$$W(A_1 \pm A_2) \le W(A_1) + W(A_2) \tag{3.16}$$

$$W(A_1 \pm A_2) \le W(A_2 \pm A_1) \tag{3.17}$$

$$W(A_1) = W(-A), \quad \text{где} \quad -A = 0 - A \tag{3.18}$$

$$W(A_1, A_2) \le \min(W(A_1), W(A_2)) \tag{3.19}$$

Поняття відстані і ваги, що введені вище, є дуже корисними при вивченні властивостей будь-яких коригувальних кодів.

Припустимо, що один з символів кодового слова A змінив своє значення у результаті дії якої-небудь завади. Отриманий у результаті новий (спотворений) вектор A' знаходиться на відстані, рівній одиниці від вектору A. Таку помилку можна виявити лише у тому випадку, якщо вектор A' не є кодовим словом. Тому усі кодові слова мають бути віддалені від вектору A на відстань, більшу одиниці. Чим більше відстань між кодовими словами, тим більше помилок може виявляти і виправляти такий код.

Під поодинокою (одноразовою) помилкою у СЗК будемо розуміти будь-яке спотворення одного залишку a_i числа $A = (a_1 \| a_2 \| \ldots \| a_n)$, що відноситься до якого-небудь одного модуля m_i. У той же час t-кратною помилкою у СЗК назвемо будь-які спотворення t залишків, що відповідають довільним t основам. Надалі будемо вважати, що помилки носять адитивний характер і однозначно визначаються вектором $\{\Delta\}_M$ помилки, вага якого дорівнює кратності помилки. Спотворений вектор A' отримується у результаті додавання (чи віднімання) кодового слова і вектору помилки, тобто $A' = A + \Delta A$ [104].

3.3 Метод варіювання коригувальними властивостями завадостійкого коду у СЗК при виконанні обчислювального процесу

Численні дослідження, обґрунтували можливість побудови КСКОЦД, в яких за рахунок спеціального кодування може бути створений імунітет проти найрізноманітніших спотворень інформації сигналів. Абсолютно чітко сформувалася точка зору, що боротьба за високу надійність передачі інформації, тобто за достовірність відновлення інформації на приймальному кінці лінії передачі, повинна вестись не стільки вдосконаленням технічних засобів передачі інформації, де будь-яке можливе підвищення надійності досягається дорогою ціною та іноді вимагає розробки складних захисних заходів, скільки застосуванням таких способів кодування інформації, які були б стійкі по відношенню до можливих випадкових спотворень інформації, розуміючи під цим здатність шляхом відповідної обробки прийнятої інформації, виключити внесені у неї збурення, очистити її від помилок і досягти повної відповідності того, що було відправлено з передавального кінець лінія.

У той час як підвищення надійності передачі інформації технічними засобами, навіть, якщо не зважати на економічну сторону питання, обмежене рівнем розвитку технічних засобів і будь-які досягнення в цій області вимагають нових технічних рішень, застосування для тієї ж мети спеціальних кодових систем не містить ніяких принципових обмежень. Більше того, при виборі відповідного коду, що має необхідну коригувальну здатність, можна помітно понизити вимоги до надійності самих ліній передачі інформації, зробити їх більш простішими і дешевшими.

Для обчислювальних засобів застосування методів спеціального кодування диктується насущною необхідністю. Адже будь-яка КСКОЦД являється сама по собі системою передачі і обробки інформації. У КСКОЦД постійно відбувається циркуляція інформації. Хоча у машині і немає довгих ліній передач, та зате по існуючих у ній, відносно коротким лініям,

інформація циркулює з величезною швидкістю та у великих кількостях. Якщо прийняти якусь умовну одиницю, наприклад проходження одним двійковим розрядом одного сантиметра шляху, то у цих умовних одиницях робота однієї обчислювальної машини середньої продуктивності за фіксований інтервал часу по передачі інформації, буде сумірна з роботою за такий же інтервал ряду великих ліній передачі.

Тому навіть з точки зору тільки передачі інформації при розробці обчислювальних засобів виникає важливе завдання забезпечення достовірності усього колосального потоку інформації. Адже у КСКОЦД, крім того, має бути забезпечена ще і достовірність арифметичної і логічної обробки інформації. Практично, без застосування методів спеціального кодування, забезпечення достовірності у КСКОЦД досягається подвійним прорахунком для виявлення правильності або неправильності результатів рішення задач і потрійним прорахунком у разі виявленої розбіжності для вибору правильного результату за даними, що збігаються. Такий шлях забезпечення достовірності зменшує фактичну продуктивність машини принаймні удвічі. Звідси ясно, що забезпечення достовірності якими-небудь методами, відмінними від вказаних повторних прорахунків, прямо і безпосередньо пов'язано зі збільшенням продуктивності КСКОЦД.

Для кожного спеціального коду, від якого потрібно, щоб він мав здатність до виявлення і корекції помилки, характерна наявність двох груп цифр – інформаційної і контрольної. До інформаційної групи входять цифри, що становлять числове значення закодованої величини, а в контрольну – цифри, що додатково вводяться для цілей виявлення і корекції можливих спотворень при передачі. Ці додаткові цифри є надмірними з точки зору числового значення величини і подовжують загальну протяжність коду, що, розуміється, дещо зменшує зрештою пропускну спроможність каналу при послідовній передачі і збільшує кількість каналів при паралельній передачі. Проте ці обставини повинні окупатися тими можливостями, які доставляють надмірні цифри для виявлення і виправлення помилок.

Позначимо через J_A і K_A відповідно інформаційну і контрольну частині коду *A*. Контрольна частина K_A є функцією інформаційної частини : $K_A = F(J_A)$.

Вид функції *F* і, отже, характер контрольних цифр, що вводяться у код, визначаються прийнятою системою кодування.

Нехай в цій системі передачі і обробки інформації прийнято n-розрядне двійкове позиційне представлення числових величин, тобто усі операції проводяться над числами (не враховуючи масштаби) у діапазоні $[0, 2^n)$. Ввівши у представлення ще m контрольних двійкових цифр, будемо оперувати з числами у діапазоні $[0, 2^{n+m})$. Проте, це розширення загального діапазону зовсім не збільшує діапазону, в якому можуть представлятися і оброблятися числові дані, оскільки введені розряди не несуть інформаційних функцій. Нехай увесь код *A* записується сукупністю двійкових цифр ε_j

$$A = \{\varepsilon_1, \varepsilon_2, ..., \tilde{\varepsilon}_{n+1}, \tilde{\varepsilon}_{n+2}, ..., \tilde{\varepsilon}_{n+m}\}.$$

Тут

$$J_A = \{\varepsilon_1, \varepsilon_2, ..., \varepsilon_n\};$$

$$K_A = \{\tilde{\varepsilon}_{n+1}, \tilde{\varepsilon}_{n+2}, ..., \tilde{\varepsilon}_{n+m}\}.$$

Основною особливістю усіх відомих до теперішнього часу спеціальних позиційних кодів є нерівноправність інформаційної та контрольної частин коду відносно арифметичних операцій.

Нехай J_A, K_A і J_B, K_B є інформаційні і відповідно контрольні частини кодів чисел A і B, та нехай над J_A і J_B має бути здійснена деяка арифметична операція $f(J_A, J_B)$. Обидві частини коду були б рівноправні,

якби операція f здійснювалася над повним кодом, тобто обчислювалася б величина

$$C = f(A, B), \tag{3.20}$$

причому

$$J_C = f(J_A, J_B).$$

Тоді, обчисливши $K_C^1 = F(J_C)$ і зіставивши його з K_C – фактичною контрольною частиною коду C, можна проконтролювати вірність виконання операції f. Ще більше рівноправність обох частин коду була б виражена, якби окрім (3.20) мала місце також і рівність

$$K_C = f(K_A, K_B).$$

Між тим, у відомих позиційних кодах операція f виконується не над повним кодом чисел A і B, а над J_A і J_B, тобто отримуємо $C^1 = f(J_A, J_B)$, а K_C обчислюється як $F(C^1)$, після чого складається повний код C, для якого $J_C = C^1$. Тут K_A і K_B у арифметичній операції не беруть участь, що не дає ніякої можливості по контрольних частинах компонентів арифметичної операції скласти контрольну частину результату, тобто виключається можливість контролю правильності виконання арифметичних операцій [70-72].

Саме ця властивість спеціальних позиційних кодів – їх неарифметичність – перешкоджає їх застосуванню у КСКОЦД, оскільки введені контрольні розряди не дозволяють контролювати результат арифметичної операції, у той час, коли цей контроль для КСКОЦД не менш

важливий, чим контроль передачі інформації [47, 107, 108].

У зв'язку з розробкою машинної арифметики у системі залишкових класів виникла можливість побудови непозиційних кодів, що виявляють і виправляють помилки, і у той же час є повністю арифметичними кодами, де інформаційна і контрольна частини абсолютно рівноправні відносно будь-якої операції.

Розглянемо систему з основами $m_1, m_2, ..., m_n$ і діапазоном $M = m_1 \cdot m_2 \cdot ... \cdot m_n$. Надалі діапазон M називатимемо робочим діапазоном системи. Введемо основу m_{n+1} взаємно просту з будь-якою з прийнятих основ і будемо представляти числа у системі з $n+1$ основ. Це означає, що будемо передавати числа і проводити операції над числами, що лежать у діапазоні $[0, M_0)$, який більш ширший за діапазон $[0, M)$, де $M_0 = M \cdot m_{n+1}$.

Надалі діапазон M_0 будемо називати повним діапазоном системи з однією контрольною основою.

Оскільки ми умовились, що усі числа, з якими оперує КСКОЦД, повинні лежати у діапазоні $[0, M)$, то очевидно, що якщо в результаті якої-небудь операції або при передачі числа виявилось, що отримане число A більше за M – це означає, що при проведенні операції виникла помилка. Будемо надалі числа, менші за M називати правильними, а більші за M – неправильними.

Таким чином, визначається можливість, побудови кодів, що виявляють і коригують помилки, у системі залишкових класів, а саме: будь-яке спотворення цифри по одному якому-небудь розряду перетворює це число на неправильне і тим самим дозволяє виявити наявність спотворення. Більше того, існує тільки одне-єдине значення цієї цифри, яке може перетворити неправильне число на правильне.

При цьому додатково введена контрольна основа m_{n+1} має бути більше будь-якої з основ системи.

3.4 Метод формування позиційної ознаки непозиційного коду у СЗК

Основна перевага непозиційної системи числення у класі лишків полягає у можливості організації процесу швидкої реалізації наступних модульних операцій: арифметичні операції додавання, віднімання і множення; операції логічного додавання, віднімання і множення по модулю два; ділення цілих чисел та ін. [109-111]. Проте у КСКОЦД загального призначення окрім вищеперерахованих арифметичних операцій необхідно здійснювати так звані у СЗК немодульні (позиційні) операції. До таких операцій в першу чергу відносяться наступні операції:

– арифметичне та алгебраїчне порівняння операндів та їх абсолютних величин;

– визначення знаку операнду;

– визначення наявності переповнювання розрядної сітки КСКОЦД;

– округлення величини результату операції;

– обчислення абсолютної величини числа;

– ділення і множення дробів;

– переведення даних з коду у СЗК в позиційну систему числення та навпаки;

– розширення вихідної СЗК (це інформаційний процес, коли по відомим залишкам $\{a_i\}$, що відповідають основам $\{m_i\}$, визначаються значення залишків цієї ж кодової структури по іншим додатковим основам);

– контроль та діагностика помилок та ін.

У загальному випадку усі позиційні операції зводяться до процедури визначення номера j числового інтервалу $[j \cdot m_i,\ (j+1) \cdot m_i)$ попадання (знаходження) числа $A = (a_1 \,||\, a_2 \,||\, ... \,||\, a_i \,||\, ... \,||\, a_n \,||\, a_{n+1})$. Для визначення номера j числового інтервалу знаходження числа A доцільно використовувати так звані позиційні ознаки непозиційної кодової структури (ПОНКС). З існуючих ПОНКС найчастіше у СЗК використовують наступні ознаки [112]:

– ознаки, що засновані на процедурі переводу числа з СЗК у ПСЧ;

– ознаки, що засновані на процедурі нульовизації (визначення значення γ_{n+1});

– ознаки, що засновані на процедурі розширення системи основ даної СЗК;

– ранг r числа A.

Основними недоліками вищеперерахованих ПОНКС є, по-перше, технічна і часова складність їх формування (розробка) для заданої кодової структури $A=(a_1 \| a_2 \| ... \| a_n \| a_{n+1})$ даних і, по-друге, значний час реалізації, за допомогою існуючих позиційних ознак, немодульних операцій у СЗК, зокрема, операції контролю даних.

Таким чином, необхідно проводити дослідження, присвячені розробці методів формування ПОНКС у СЗК, за допомогою яких оперативно реалізуються немодульні операції. Відмітимо, що будь-яка немодульна операція може бути реалізована за допомогою сукупності (послідовності) певних модульних і немодульних операцій, що реалізовуються за допомогою ПОНКС. Спочатку розглянемо основні вимоги до ПОНКС, на основі яких надалі буде розроблений метод підвищення оперативності контролю даних:

– за допомогою ПОНКС, що використана (вибрана, розроблена, сформована) необхідно достовірно визначити правильність або неправильність числа A у СЗК (визначити факт знаходження або незнаходження числа A в інформаційному числовому [0, M] інтервалі, де $M = \prod_{i=1}^{n} m_i$);

– простота формування ПОНКС для завдань кодової $A=(a_1 \| a_2 \| ... \| a_n \| a_{n+1})$ структури даних;

– простота використання сформованої ознаки для проведення контролю даних у СЗК (у загальному випадку для реалізації позиційних операцій);

– ознака повинна мати чіткий і зрозумілий фізичний сенс;

– аналітично ознака повинна описуватися не складним математичним

співвідношенням;

– за допомогою використання ПОНКС можливо технічно просто реалізувати систему контролю (СК) даних у СЗК;

– застосування вибраної ознаки непозиційного коду повинне забезпечити підвищення контролю даних у СЗК;

– використання ПОНКС повинне по можливості виключати найбільш складні позиційні операції з процедури контролю, діагностики та корекції помилок у СЗК.

Розглянемо метод формування ПОНКС, на основі непозиційної кодової структури $A=(a_1 \| a_2 \| ... \| a_i \| ... \| a_n \| a_{n+1})$ даних, представленою у СЗК основами $\{m_i\}$, $i=\overline{1,n+1}$ так званого однорядкового коду (ОК). У загальному вигляді ОК $K_N^{(n_A)}=\left\{Z_{N-1}^{(A)}\ Z_{N-1}^{(A)} ... Z_1^{(A)}\ Z_0^{(A)}\right\}$ є послідовністю двійкових $Z_K^{(A)}$ $(K=\overline{0,\ N-1})$ розрядів, що складається з одиниць і тільки одного нуля, що знаходиться на n_A-му місці (рахуючи справа, від розряду $Z_0^{(A)}$ наліво, до розряду $Z_{N-1}^{(A)}$). Математично ПОНКС n_A визначає номер j числового інтервалу $[j\cdot mi,\ (j+1)\cdot mi)$ знаходження числа A. Математично ПОНКС є натуральним n_A числом, яке вказує на місце розташування нульового двійкового розряду у записі ОК $K_N^{(n_A)}\left(Z_{n_A}^{(A)}=0\right)$.

Процедура формування ОК $K_N^{(n_A)}$ полягає в наступному. Для вибраної основи m_i СЗК за значенням залишку a_i числа $A=(a_1 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n \| a_{n+1})$ у блоці констант нульовизації (БКН) визначається константа виду $KH_{m_i}^{(A)}=\left(a_1' \| ... \| a_{i-1}', \| a_i \| a_{i+1}' \| ... \| a_{n+1}'\right)$.

Далі, за допомогою вибраної константи нульовизації $KH_{m_i}^{(A)}$ число A зміщуємо на лівий край інтервалу $[j\cdot m_i,\ (j+1)\cdot m_i)$ шляхом реалізації операції

$$A_{m_i}=A-KH_{m_i}^{(A)}=\left(a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_{n+1}\right)-$$

$$=\left(a_1' \| a_2' \| ... \| a_{i-1}', \| a_i \| a_{i+1}' \| ... \| a_{n+1}'\right)=\left[a_1^{(1)} \| a_2^{(1)} \| ... a_{i-1}^{(1)} \| 0 \| a_{i+1}^{(1)} \| ... \| a_{n+1}^{(1)}\right].$$

Очевидно, що число A_{m_i} кратно значенню модуля m_i СЗК.

Відомо, що правильність числа A у СЗК визначається попаданням або непопаданням його у числовий інформаційний [0, M) інтервал. Якщо число A знаходиться поза цим інтервалом ($A \geq M$), то воно вважається спотвореним (неправильним). У цьому випадку ПОНКС n_A повинен визначити факт попадання або непопадання вихідного числа A в інтервал [0, M). Щоб визначити факт знаходження числа в інформаційному [0, M) числовому інтервалі необхідно провести операцію виду $A_{m_i} - K_A \cdot m_i = Z_{K_A}^{(A)}$.

Ця операція проводитися одночасно і паралельно у часі за допомогою сукупності з N констант $K_A \cdot m_i \left(K_A = \overline{0, N-1}\right)$ де $N = \prod_{\substack{K=1 \\ K \neq i}}^{n+1} m_K$:

$$\begin{cases} A_{m_i} - 0 \cdot m_i = Z_0^{(A)}, \\ A_{m_i} - 1 \cdot m_i = Z_1^{(A)}, \\ A_{m_i} - 2 \cdot m_i = Z_2^{(A)}, \\ \quad \cdots \\ A_{m_i} - (N-2) \cdot m_i = Z_{N-2}^{(A)}, \\ A_{m_i} - (N-1) \cdot m_i = Z_{N-1}^{(A)}. \end{cases} \tag{3.21}$$

У цьому випадку ОК представиться у вигляді

$$K_N^{(n_A)} = \left\{ Z_{N-1}^{(A)} \; Z_{N-2}^{(A)} \; \ldots \; Z_1^{(A)} \; Z_0^{(A)} \right\}. \tag{3.22}$$

У сукупності аналітичних співвідношень існує єдине значення n_A для якого $Z_{K_A}^{(A)} = Z_{n_A}^{(A)} = 0 \quad (K_A = n_A)$, тобто $A_{m_i} - n_A \cdot m_i = 0$. Інші значення (3.21) рівні $Z_l^{(A)} = 1 \quad (A_{m_i} - l \cdot m_i \neq 0; \quad l \neq n_A)$. У загальному випадку кількість двійкових розрядів у записі ОК $K_N^{(n_A)}$ дорівнює значенню N [113-115].

Метод формування ПОНКС n_A у СЗК представлений на рис. 3.2.

Вибір інформаційних $\{m_i\}$, $i=\overline{1,n}$ і контрольного $m_k = m_n+1$ ($m_i < m_i+1$) основ СЗК для представлення даних $A=(a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n \| a_{n+1})$, НСД ($m_i$, m_j) = 1, $i \neq j$.

Вибір основи $m_i \in \{m_j\}$, $(j=\overline{1,n+1})$ по якій визначається номер j числового інтервалу $[j \cdot m_i, (j+1) \cdot m_i)$ знаходження числа A.

За значенням залишку a_i (по модулю m_i) числа A визначення константи нульовизації $KH_{m_i}^{(A)} = (t_1', t_2', ..., t_{i-1}', t_i, t_{i+1}', ..., t_n', t_{n+1}')$.

Визначення значення

$$A_{m_i} = A - KH_{m_i}^{(A)} = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n \| a_{n+1}) -$$

$$-(t_1' \| t_2' \| ... \| t_{i-1}' \| t_i \| t_{i+1}' \| ... \| t_n' \| t_{n+1}') = \left[a_1^{(1)} \| a_2^{(1)} \| ... \| a_{i-1}^{(1)} \| 0 \| a_{i+1}^{(1)} \| ... \| a_n^{(1)} \| a_{n+1}^{(1)} \right].$$

Визначення ОК $K_{N_i}^{(n_A)} = \left\{ Z_{N_i-1}^{(A)} \; Z_{N_i-2}^{(A)} \; ... \; Z_0^{(A)} \right\}$.

$$N = \prod_{\substack{K=1 \\ K \neq i}}^{n+1} m_K, \qquad N_i =]M / m_i[, \qquad M = \prod_{i=1}^{n} m_i.$$

$$A_{m_i} - K_A \cdot m_i = Z_{K_A}^{(A)}.$$

$$\begin{cases} A_{m_i} - 0 \cdot m_i = Z_0^{(A)}, \\ A_{m_i} - 1 \cdot m_i = Z_1^{(A)}, \\ \quad \dots \\ A_{m_i} - (N_i - 2) \cdot m_i = Z_{N_i-2}^{(A)}, \\ A_{m_i} - (N_i - 1) \cdot m_i = \quad Z_{N_i-1}^{(A)}. \end{cases}$$

Визначення ПОНКС n_A числа A, тобто числового значення n_A для якого $Z_{K_A}^{(A)} = Z_{n_A}^{(A)} = 0$, тобто $A_{m_i} - n_A \cdot m_i = 0$. При цьому $Z_l^{(A)} = 1$, $(A_{m_i} - l \cdot m_i \neq 0; l \neq n_A)$.

Рис. 3.1 Метод формування ПОНКС у СЗК

Висновки до розділу 3

У третьому розділі вирішено **третю** задачу досліджень.

1. З метою подальшої розробки методів підвищення оперативності контролю та діагностики помилок цілочислових даних, що представлені у СЗК, у розділі досліджені коригувальні властивості непозиційних кодових структур. Представлені основні положення і виводи теорії завадостійкого

кодування даних у СЗК. На підставі положень теорії завадостійкого кодування даних проведені дослідження коригувальних властивостей, і можливостей НКС при різних способах введення інформаційної надмірності, тобто при різній кількості і величині додаткових контрольних основ.

Це дало можливість створити процедуру варіювання можливими коригувальними здібностями завадостійкого коду у СЗК у ході обчислювального процесу (без основного рішення задачі).

2. З метою оперативної реалізації модульних і немодульних операцій у СЗК, зокрема, операцій контролю та діагностики помилок, у третьому розділі був розроблений метод формування позиційної ознаки НКС. Наявність і використання цієї ознаки дозволяє істотно підвищити оперативність процесів контролю та діагностики. Надалі позиційна ознака НКС буде використана для підвищення оперативності процедури контролю та діагностики даних у СЗК.

Основні положення цього розділу викладені у публікаціях автора [102, 107, 108, 111, 113-115].

РОЗДІЛ 4. МЕТОДИ ОПЕРАТИВНОГО КОНТРОЛЮ ДАНИХ У СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ

4.1 Формулювання принципів контролю непозиційних кодових структур у СЗК

Принципи контролю НКС у СЗК такі ж як і принципи контролю у ПСЧ, при цьому враховуючи принципи утворення СЗК і вплив властивостей СЗК на структуру КСКОЦД, відмітимо, у загальному вигляді, принципи контролю даних у НКС:

– принцип достовірності контролю;

– принцип безперервності контролю;

– принцип оперативності контролю.

Відмітимо так само, що кількість контрольної апаратури займає приблизно 20-25% від загальної кількості апаратних засобів.

При виборі методів контролю основна увага має бути звернена на здатність цього методу контролю до виявлення помилок, а також на об'єм апаратури і час, що витрачається на контроль.

Як відзначалося раніше програмні методи контролю правильності обчислень призначені для перевірки правильності реалізації обчислювального процесу в різних режимах роботи КСКОЦД та правильності функціонування усіх пристроїв КСКОЦД. Ці методи засновані на включенні у програмне забезпечення спеціальних контролюючих програм або додаткових співвідношень у загальний алгоритм.

Програмно-логічний контроль, заснований на використанні інформаційної надмірності та призначений для перевірки правильності реалізації обчислювального процесу. Інформаційна надмірність забезпечується за рахунок включення у загальний алгоритм додаткових співвідношень, що дозволяють виявляти і виправляти помилки, що виникають при обчисленнях.

Розглянемо найбільш поширені способи програмно-логічного контролю.

Спосіб подвійного прорахунку з порівнянням результатів. Основна його перевага – простота реалізації. Суть його полягає в тому, що уся робоча програма розбивається на окремі частини і після виконання якого-небудь етапу обчислень робиться контрольне підсумовування усіх команд, проміжних і кінцевих результатів етапу, що контролюється. Контрольна сума запам'ятовується і виконується повторне обчислення цього етапу з подальшим контрольним підсумовуванням. Обидві контрольні суми порівнюються. При порівнянні виконується наступний етап обчислень. У разі розбіжності робиться третій прорахунок цього етапу. При збігу третьої контрольної суми з однією з попередніх виконується наступний етап обчислень. Інакше подається сигнал про збої роботи у КСКОЦД. Цей спосіб має і недоліки: він збільшує час реалізації алгоритму, що допустимо лише за наявності надмірної швидкодії КСКОЦД і дозволяє виявляти та усувати лише випадкові помилки, викликані збоями у системі. При організації контролю способом подвійного прорахунку необхідно вірно зробити розбиття алгоритму на контрольовані етапи. В якості основного критерію при розбитті, слід прийняти забезпечення необхідної ймовірності виявлення помилки при мінімальній витраті часу на контроль. Дослідження показали, що існує оптимальне число контрольованих частин алгоритму, при якому час, що витрачається на контроль, є мінімальним.

Досвід експлуатації КСКОЦД показує, що потік випадкових збоїв можна прийняти простим. Позначимо інтенсивність потоку випадкових збоїв через λ, час рішення задачі – $T_з$, кількість контрольованих частин – N. Тоді час реалізації однієї контрольованої частини алгоритму визначиться як:

$$t = \frac{T_з}{N}.$$

Слід врахувати, що при організацій контролю способом подвійного прорахунку витрачається додатковий час $t_д$ на кожній частині задачі, що контролюється, на контрольне підсумовування, порівняння контрольних сум, ухвалення рішень на третій прорахунок або продовження обчислень.

Спосіб контрольних співвідношень дозволяє визначити не лише помилки, що з'являються за рахунок випадкових збоїв, але і помилки, що з'являються за рахунок відмов. Суть цього способу полягає в тому, що у загальний алгоритм включаються різні математичні співвідношення, що дозволяють перевірити правильність рішення основної задачі шляхом їх реалізації. При виконанні контрольних співвідношень із заданою точністю проводиться подальше рішення основної задачі. При невиконанні контрольних співвідношень або повторюється ця частина задачі, або зупиняють роботу КСКОЦД. Спосіб контрольних співвідношень може дати значний виграш у часі у порівнянні із способом подвійного прорахунку.

Спосіб "зрізаного" алгоритму дозволяє виявляти та усувати помилки за рахунок випадкових збоїв і систематичних відмов, якщо "зрізаний" алгоритм значно відрізняється від основного. Цей спосіб припускає наявність спрощеного алгоритму основної задачі. Спрощений алгоритм має бути менший за основний. Реалізація "зрізаного" алгоритму спільно з основним і збіг результатів у межах заданої точності дозволяють судити про правильність ходу обчислювального процесу.

Спосіб логічного аналізу результатів рішення дозволяє виявляти як випадкові, так і систематичні помилки. Суть його полягає в порівнянні деяких параметрів задачі та їх приростів, що обчислені у ході рішення задачі, із заздалегідь відомими межами їх зміни. Спосіб використовується у тому випадку, якщо заздалегідь відомі закони зміни деяких параметрів.

Спосіб підстановки полягає у тому, що після отримання ряду шуканих завдань, вирішується зворотне завдання. У якості вихідних даних вибираються знайдені значення невідомих та визначаються деякі величини, які при прямих обчисленнях використовувалися як вихідні дані. Потім

порівнюють ці величини з початковими даними при прямому обчисленні. Збіг в межах заданої точності свідчить про відсутність помилок в обчисленнях. Наприклад, при рішенні систем алгебричних рівнянь, в якості вихідних даних можуть бути прийняті корені $x_1 \| x_2 \| ... \| x_k$, ті, що отримані в обчисленні; в якості невідомих – які-небудь k - коефіцієнти, що визначаються при зворотному рішенні завдання. Порівняння отриманих коефіцієнтів з існуючими, в межах заданої точності, говорить про те, що система вирішена вірно. Аналогічним чином можна скористатися при рішенні систем диференціальних рівнянь.

При розробці загального алгоритму КСКОЦД необхідно використовувати найбільш ефективні способи контролю правильності обчислень, що дозволяють значно підвищити надійність обробки інформації з мінімальними витратами машинного часу.

Усі розглянуті способи контролю обчислень, є ефективними лише за умови правильності ходу реалізації програм КСКОЦД.

Контроль ходу виконання програм КСКОЦД: кожна програма, що реалізовує той або інший режим роботи КСКОЦД, складається з окремих підпрограм програмою-диспетчером. Правильність ходу виконання програми визначається: контролем послідовності включення підпрограм; контролем тривалості роботи підпрограм сформованої програми; контролем виконання переходів і переривань програми.

Контроль послідовності включення підпрограм: режим роботи КСКОЦД і системи забезпечується відповідною програмою, що складається з окремих підпрограм S_i, що виконуються по черзі. Спосіб контролю полягає в наступному. За час τ_i підпрограма S_i включається в роботу не менше ніж один раз і в результаті кожного виконання підпрограми S_i змінюється деякий параметр $R_i(t)$, що зберігається в оперативній пам'яті. Перевіркою співвідношення $R_i(t) \neq R_i(t+\tau_i)$ можна встановити, що підпрограма S_i виконувалася. Для кожного режиму роботи, що виконується КСКОЦД,

заздалегідь відомі зв'язки між окремими підпрограмами. Детермінованість зв'язків між підпрограмами використовується для контролю послідовності їх виконання. У цьому випадку кожна підпрограма при виконанні фіксує у певній комірці пам'яті заздалегідь закріплений за цією підпрограмою умовний код. Виконання наступної підпрограми починається лише після аналізу умовного коду, що записаний при виконанні попередньої підпрограми.

Контроль тривалості роботи підпрограм сформованої програми: припускає контроль тривалості роботи окремих частин програми і дозволяє виявляти порушення реалізації програм за рахунок зациклення та інших причин, що призводять до збільшення часу реалізації окремих підпрограм програми. Для цієї мети використовуються лічильники відносного часу, призначені для підрахунку тимчасових інтервалів. У цьому випадку накладаються певні обмеження на тривалість τ_i виконання підпрограми S_i. На початку кожної підпрограми у лічильник відносного часу спеціальною командою заноситься код, що відповідає допустимій відносній тривалості виконання цієї підпрограми. При кожній реалізації підпрограми S_i з вмісту лічильника відносного часу віднімається одиниця. За наявності у лічильнику відносного часу нуля, виробляється сигнал помилки, який викликає переривання програми і перехід до підпрограми аналізу помилок. Інакше відбувається перехід до виконання наступної підпрограми.

Контроль правильності виконання переходів і переривань програми здійснюється за допомогою команд умовної і безумовної передачі керування та заснований на програмному блокуванні сигналу помилки. Ідея цього контролю полягає в тому, що перед виконанням переходу спеціальною командою у ланцюг модифікації адреси та виконання переходу подається сигнал помилки, надходження якого може бути заблоковане за допомогою команд блокування, що розташовуються в усіх місцях програми, куди відбувається перехід.

При неправильному виконанні переходу сигнал помилки не буде заблокований і викличе при цьому переривання та включення в роботу підпрограми аналізу збоїв. Цей спосіб забезпечує високу імовірність виявлення як випадкових, так і систематичних помилок будь-якої кратності, але вимагає додаткового обладнання та спеціальних команд у програмі.

Переривання програми є характерною особливістю роботи КСКОЦД, що реалізовує свої алгоритми у реальному масштабі часу. У процесі роботи КСКОЦД, залежно від режиму роботи системи та об'єму інформації, що поступає і видається, робляться численні переривання програми, що налічують сотні переривань за секунду.

Для контролю правильності виконання переривань програми часто використовується розглянутий спосіб програмного блокування сигналу помилки. Відмінність полягає лише в тому, що формування сигналу помилки здійснюється схемним шляхом, а переривання може бути у будь-якому місці програми. Блокування сигналу помилки здійснюється однією з перших команд підпрограми, що уклинюється. Контроль переходу до основної програми після переривання здійснюється перевіркою правильності відновлення стану основних результатів регістрів і елементів пам'яті КСКОЦД, що використовувалися підпрограмою, що уклинюється. Для цієї мети застосовують метод багатократного зберігання змінної інформації у пам'яті машини і подальше її порівняння.

Сигнал помилки виробляється при незбіжності вмісту хоч би одного регістра або елементу пам'яті.

При апаратному контролі, який забезпечує контроль машини або окремих її пристроїв за допомогою додаткового обладнання, що включене у КСКОЦД, поширеним являється контроль по модулю. Цей контроль полягає у тому, що використовуються порівняння виду

$$x \equiv a \bmod m,$$

При такому контролі у якості надмірної інформації використовується величина контрольного коду a.

Розрізняють два види контролю по модулю: числовий та цифровий.

При цифровому контролі по модулю контрольний код утворюється, як залишок від ділення суми цифр числа x на модуль m. При числовому контролі по модулю, контрольний код утворюється як залишок від ділення числа x на модуль m.

Наприклад, якщо $m = 3$, то порівняння можна записати так:

при цифровому контролі	при числовому контролі
$x = 101010 \equiv 00 \bmod 3$	$x = 101010 \equiv 00 \bmod 3$
$x = 101001 \equiv 00 \bmod 3$	$x = 101001 \equiv 10 \bmod 3$
$x = 111010 \equiv 01 \bmod 3$	$x = 111010 \equiv 01 \bmod 3$

В якості контрольних кодів a тут фігурують коди 00, 00, 01, та 00, 10, 01.

При використанні двійкової системи числення для $m = 2$ цифровий контроль по модулю зводиться до контролю на парність (непарність). Проте цифровий контроль, наприклад, при перевірці правильності виконання операції додавання вимагає підрахунку одиниць перенесення. Внаслідок цього він використовується, головним чином, для контролю правильності передачі кодів і правильності зберігання інформації у пам'яті.

З теорії чисел відомо, що для числового контролю справедливі порівняння

$$\sum_{i=1}^{N} x_i \equiv \sum_{i=1}^{N} a_i \bmod m_i ,$$

$$\prod_{i=1}^{N} x_i \equiv \prod_{i=1}^{N} a_i \bmod m_i .$$

Приведені вирази дозволяють контролювати виконання операцій додавання та множення [116].

Апаратний контроль по модулю забезпечує отримання сигналів помилки, що виникають при неправильній роботі основного та контрольного обладнання. У цьому випадку фіксуються випадкові та систематичні помилки. Проте апаратний контроль не завжди забезпечує необхідну ступінь перевірки правильності функціонування КСКОЦД. Тому найбільш раціональною організацією системи контролю є комбінований метод контролю, що поєднує у собі апаратні та програмні методи контролю та задовольняє усім вимогам, що пред'являються до систем контролю. Основною проблемою використання комбінованого методу контролю є визначення оптимального співвідношення програмного та апаратного методів контролю, яке залежить від умов роботи та застосування КСКОЦД.

4.2 Основи контролю достовірності даних у СЗК

Усі операції, що виконуються в КСКОЦД над даними, представленими у СЗК, можна розбити на три основні групи [117, 118].

До першої групи відносяться такі операції, при виконанні яких помилка в одному залишку цього модуля не впливає (не поширюється) на значення залишків, що відповідають іншим модулям (основам) СЗК. До цієї групи входять модульні операції додавання, віднімання, множення (без округлення), а також операція пересилки чисел.

При виконанні операцій, що відносяться до другої групи, помилка, що виникла в одному залишку може поширюватися і спотворити залишки, що відповідають іншим основам СЗК. До таких операцій можна віднести обчислення позиційних характеристик, розширення системи основ, ділення, множення з округленням.

До третьої групи операцій відносяться такі операції, результати яких

вже не є числами, представленими у СЗК. Такими операціями є, наприклад переведення числа з СЗК у позиційну систему числення, визначення знаку, порівняння чисел за абсолютною величиною і т. д.

При виконанні операцій другої і третьої груп доводиться оцінювати величину чисел і, отже, обчислювати їх позиційні характеристики. Таким чином, у деяких випадках, з'являється можливість практично без додаткових тимчасових та апаратурних витрат контролювати правильність виконання позиційних операцій.

Якщо над результатами операцій, що відносяться до першої групи, досить часто виконуються операції немодульного типу, то немає необхідності спеціально контролювати правильність виконання кожної модульної операції, оскільки при цьому не відбувається (як відзначалося вище) поширення помилок. У той же час, коли у КСКОЦД упродовж тривалого часу виконуються тільки модульні операції, через певні проміжки часу для перевірки відсутності спотворень слід обчислювати вектор $\{\pi_N\}_{R_1}$. Якщо коригувальний код використовується не лише для контролю (виявлення), але і для виправлення помилок, то при виборі інтервалу часу між окремими перевірками слід враховувати можливість поширення помилок у деякій групі чисел.

Для того, щоб з'ясувати, чи являється деякий вектор *A* кодовим словом *R*-коду, необхідно визначити величину відповідного числа *A*. У загальному випадку, якщо число *A* належить множині *L*, то з певною ймовірністю можна вважати, що воно не є спотвореним. Якщо ж *A* не належить множині *L,* то напевно сталася помилка. Виходячи з цього очевидно, що базовою процедурою для процесу контролю даних у СЗК являється операція порівняння.

У теорії непозиційного завадостійкого кодування усі методи контролю можна розділити на три великі групи: методи, що засновані на використанні принципу безпосереднього порівняння, методи, що засновані на

використанні принципу нульовизації і методи, що засновані на використанні позиційних ознак непозиційного коду [16].

У цьому розділі розглянемо існуючі методи контролю даних у СЗК на основі застосування позиційних ознак $\pi_N(A)$. Для порівняння, величин значень A та L найзручніше скористатися позиційними ознаками (характеристиками) $\pi_N(A)$. Якщо $L = N$, то будь-яким кодовим словам відповідає тільки одне значення $\pi_N(A)$ рівне нулю. При значенні $L = 2N$ кодовим словам можуть відповідати два значення позиційної характеристики. Якщо $A < 0$, то $\pi_N(A) = R_1 - 1$, а додатним числам відповідає нульове значення характеристики.

У [104] показано, що позиційні характеристики непозиційного коду $\pi_N(A)$ обчислюються у ході виконання будь-якої немодульної операції. Отже, одночасно з виконанням будь-якої такої операції здійснюється контроль (виявлення) помилок. Якщо немодульні операції зустрічаються у ході рішення задачі досить часто, то немає необхідності вводити спеціальну операцію виявлення помилок, тобто у даному випадку для виявлення помилок не будуть потрібні додаткові витрати часу. Для діагностики та виправлення (корекції) помилок необхідно, передусім, визначити номери модулів СЗК, яким відповідають спотворені символи.

Розглянемо основні практичні методи контролю даних у СЗК, що засновані на використанні позиційних характеристик.

Перший метод контролю даних у СЗК полягає у наступному. Вилучимо з СЗК основу m_1 і визначимо величину числа, що відповідає вектору $\{A\}_{M/m_1}$. Якщо виявиться, що це число належить множині L, то можна стверджувати, що саме у вилученому модулі сталася помилка. Якщо число не потрапить до інтервалу L, то перейшовши до вектору $\{A\}_{M/m_2}$, будемо виконувати аналогічні дії до тих пір, поки не виявиться, що при виключенні основи m_i вектору $\{A\}_{M/p_i}$ відповідає число з множини L. Тим самим

помилка буде локалізована. Припустимо тепер, що, перебравши усі основи СЗК, ми не змогли локалізувати помилку. Це означає, що помилка не є поодинокою. Тоді почнемо виключати різні пари модулів, трійки і так далі (за умови, що мінімальна відстань коду досить велика). Якщо при вилученні якої-небудь комбінації з t модулів $(t \le k)$ число A потрапить в інтервал L, то можна стверджувати, що саме у цих модулях сталися помилки. Обчислення істинних значень спотворених символів здійснюється шляхом розширення скороченої системи основ СЗК до первинної величини.

Основний недолік розглянутого методу – значний час контролю, тобто низька оперативність процесу контролю даних. Це обумовлено у першу чергу тим, що для оцінки величини числа A у кожній із сукупностей наборів основ СЗК вимагається виконувати n модульних операцій.

З метою пошуку шляху підвищення оперативності контролю, розглянемо другий метод контролю даних у СЗК, що використовує деякі властивості позиційної ознаки $\pi_N(A)$. Для цього розглянемо результати доказів ряду відомих тверджень, що дозволяють виявити і використати властивості позиційної ознаки $\pi_N(A)$ для контролю даних.

Твердження 4.1. Нехай Q - добуток основ СЗК, які відповідають спотвореним залишкам кодового слова. Тоді, якщо $Q(\lambda+1) < R_1$, то повинна виконуватися наступна нерівність:

$$\left|(\pi_N(A') + \lambda)Q\right|_{R_1} < (\lambda+1)Q, \qquad (4.1)$$

де $\lambda = L/N$; $R_1 = M/N$; A' – число, що відповідає спотвореному кодовому слову.

Доказ. Припутимо $A' = A + \Delta$, де A – кодове слово, а Δ – вектор помилки. За умовою твердження усі ненульові складові вектору Δ відповідають тим основам СЗК, які входять в добуток Q. Тому $\Delta = qM/Q$, де q – ціле додатне число, що менше Q.

Отже, маємо, що

$$A = A' - qM / Q. \tag{4.2}$$

Розглянемо тепер різницю $A - |A'|_N$. Оскільки додатна величина $|A'|_N < N$, а число A лежить в інтервалі $(-(\lambda - 1)N, N)$, то ця різниця повинна задовольняти нерівності:

$$-\lambda N < A - |A'|_N < N. \tag{4.3}$$

Додамо до усіх частин цієї нерівності величину λN, отриманий вираз помножимо на Q / N і підставимо у цей добуток значення A з формули (4.2). Тоді:

$$0 < \left(\frac{A' |A'|_N}{N} + \lambda \right) Q - qR_1 < (\lambda + 1)Q. \tag{4.4}$$

Але за визначенням позиційної характеристики маємо, що $\pi_N(A') = [A' / N] = (A' - |A'|_N) / N$.

Тому, обчислюючи залишки від ділення усіх членів нерівності (4.4) на R_1 та враховуючи той факт, що $|(\lambda + 1)Q|_{R_1} = (\lambda + 1)Q$, у результаті прийдемо до шуканої нерівності (4.1). Що і вимагалося довести.

Твердження 4.2. Кожній позиційній характеристиці n_N відповідає один і тільки один вектор помилки з вагою, не більшою за $k = (d - 1) / 2$, якщо добуток контрольних модулів не менше добутку будь-яких $d - 1$ основ СЗК, помноженого на величину $\lambda + 1$, тобто

$$R_1 \geq (\lambda+1)\prod_{j=1}^{d-1} m_{q_j},\ q_j = 1,2,...,m. \qquad (4.5)$$

Доказ. Нехай одному значенню позиційної характеристики відповідають два вектори помилки, тобто знайдуться два таких кодових слова A_1 і A_2 і два вектори помилки Δ_1 і Δ_2, що

$$\pi_N(A_1') = \pi_N(A_2'), \text{ де } A_1' = A_1 + \Delta_1,\ A_2' = A_2 + \Delta_2.$$

Підставляючи ці значення A_1' і A_2' у вирази, що відповідають позиційним характеристикам, отримаємо наступну рівність:

$$(A_1' - |A_1'|_N + \Delta_1) / N = (A_2' - |A_2'|_N + \Delta_2) / N$$

чи

$$(A_1 - A_2) + (|A_2'|_N - |A_1'|_N) = \Delta_2 - \Delta_1 \qquad (4.6)$$

Права частина цієї рівності відповідає вектору $(\Delta_2 - \Delta_1)$, вага якого не перевищує величини $2k = d-1$. Тому

$$(\Delta_2 - \Delta_1) \geq \frac{M}{\prod_{j=1}^{d-1} m_{q_j}}.$$

Оцінимо тепер величину лівої частини виразу (4.6). Вочевидь, що різниця $(A_1 - A_2)$ лежить в інтервалі $(-\lambda N, \lambda N)$, а залишки $|A_2'|_N$ і $|A_1'|_N$ відповідають цілим додатним числам, меншим за N. Тому:

$$\left|A_1 - A_2 + \left|A_2'\right|_N - \left|A_1'\right|_N\right| < (\lambda + 1)N$$

Розділивши M на обидві частини виразу (4.5), отримаємо нерівність

$$M / (\lambda + 1)\prod_{j=1}^{d-1} p_{q_j} \geq M \big/ R_1$$

або

$$(\gamma + 1)N \leq \frac{M}{\prod_{j=1}^{d-1} m_{q_j}}.$$

Таким чином, ліва частина виразу (4.6) за абсолютною величиною свідомо менше за праву, тобто не можуть існувати два різні вектори Δ_1 і Δ_2, що відповідають одному значенню позиційної характеристики. Що і вимагалося довести.

Таким чином, суть другого контролю даних полягає у наступному. Для контролю (локалізації) помилок у СЗК досить послідовно перевіряти правдивість нерівності (4.1), спочатку при значенні $Q = m_i$, потім при значенні $Q = m_i m_j$ і так далі (де $i, j = 1,2,...,n;\ i \neq j$). Якщо для якого-небудь варіанту добутку основ СЗК ця нерівність виявиться правдивою, то слід визначити величину числа A, що представлене у скороченій СЗК, в якому відсутні модулі, що входять до складу цього добутку. При попаданні числа A до інтервалу L можна стверджувати, що у залишках саме по цих модулях сталися помилки та вірні значення спотворених залишків можна визначити, розширюючи СЗК до вихідної величини. Якщо ж число не потрапляє в інтервал L, то слід перейти до перевірки іншого варіанту комбінації добутків

основ. Перевірку нерівності (4.1) можна виконувати у СЗК з основою R_1 і, якщо у деякий добуток Q входять t модулів, то для такої перевірки знадобиться $t+1$ модульна операція, а не n операцій, як у попередньому випадку. У тих випадках, коли з будь-яких причин перехід до обчислень у скороченій СЗК небажаний, можна за рахунок деякого збільшення ступеня надмірності добитися того, щоб кожній позиційній характеристиці π_N відповідав тільки один вектор помилки.

Відмітимо деякі особливості практичного застосування другого методу контролю даних :

– якщо виконуються умови твердження 4.2, то для знаходження місця спотвореного залишку замість перебору різних основ СЗК за значенням позиційної характеристики, використовуючи для цього табличний метод обробки даних, можна відразу визначити вектор помилки;

– у випадки використання для процедури контролю табличного методу обробки даних виникає проблема захисту самої таблиці від помилок;

– при зміні мінімальної кодової відстані у СЗК за рахунок зменшення або збільшення співвідношення між числом контрольних та інформаційних модулів змінюється і відповідність між значеннями π_N і Δ позиційної ознаки, тобто для кожного набору інформаційних основ необхідно використати свою таблицю; у цьому випадку номери спотворених залишків доцільніше визначати за допомогою співвідношення (4.1);

– якщо виконуються умови твердження 4.1, то помилки зустрічаються, лише у контрольних модулях;

– якщо кожен з векторів $\{\pi_N\}_{R_1}$ і $\{\pi_N+1\}_{R_1}$ містить не менше $k+1$ не нульових компонент, то у залишках, що відповідають інформаційним основам, сталася, щонайменше, помилка в одному залишку;

– якщо в деякий добуток Q входять t модулів, то для такої перевірки знадобиться $t+1$ модульна операція, а не n операцій, як для першого методу контролю даних.

З перерахованих вище основних особливостей другого методу, відмітимо, що у деяких випадках (для якого-небудь варіанту добутку основ СЗК) цей метод контролю даних більш швидкодіючий, ніж перший. Проте, у загальному випадку, другий метод кардинально не вирішує питання підвищення оперативності контролю даних. Окрім цього, істотним недоліком методу є технічна складність організації процесу контролю даних.

Вище перелічені обставини обумовлюють необхідність удосконалення існуючих методів контролю даних і розробки нових оперативних методів контролю даних у СЗК.

Відмітимо, що при необхідності подальшої можливої корекції помилок, замість безпосереднього обчислення істинних значень спотворених символів за допомогою розширення вихідної системи основ можна скористатись іншим методом, а саме: по раніш визначеному значенню π_N обчислити ненульові компоненти вектору помилки і далі відняти цей вектор із спотвореного слова.

Нехай $A' = A + \Delta$ і $\pi_N = (A' - |A'|_N) / N$. Отже:

$$\Delta = \pi_N - (A - |A'|_N). \tag{4.7}$$

Помножимо і розділимо різницю $A - |A'|_N$ та добуток QN. Тоді:

$$\Delta = N\pi_N - \frac{(A - |A'|_N)Q}{N}\frac{N}{Q}.$$

Виконаємо ще одне еквівалентне перетворення цього виразу :

$$\Delta = N(\pi_N + \lambda) - \frac{(N\lambda + A - |A'|_N)Q}{N}\frac{N}{Q}.$$

Величина $N\lambda + A - |A'|_N$ свідомо додатна. Тому:

$$\frac{(N\lambda + A - |A'|_N)Q}{N} = |(\pi_N + \lambda)Q|_{R_1}.$$

Справедливість цієї рівності стане ясною, якщо згадати, що $|A'Q|_M = AQ$.

Отже, остаточний вираз для вектору помилки прийме вигляд:

$$\{\Delta\}_M = \{N(\pi_N - \lambda) - N / Q|(\pi_N + \lambda)Q|_{R_1}. \quad (4.8)$$

Іноді зручніше обчислювати помилку із оберненим знаком для того, щоб замість віднімання, додавати її до спотвореного числа. Тоді, позначивши $\delta = \pi_N + \lambda$, отримаємо наступне вираження:

$$\{-\Delta\}_M = \{N / Q|\delta Q|_{R_1} - \delta R\}_M. \quad (4.9)$$

Отже, для того, щоб визначити вектор помилок, спочатку слід обчислити усі залишки, що відповідають представленню величини $|\delta Q|_{R_1}$ у вихідному СЗК, з основою *M* за допомогою розширення системи з основою R_1. Для цього знадобиться *t* модульних операцій. Крім того, необхідно ще виконати операції віднімання і множення на константи.

Нехай $Q = Q_u Q_к$, де Q_u – добуток інформаційних модулів, яким відповідають помилки; $Q_к$ – добуток спотворених контрольних модулів. Тоді

$$|\delta Q|_{R_1} / Q = |\delta Q_u|_{R_1 / Q_к} / Q_u.$$

У цих випадках для обчислення вектору помилки слід у формулах (4.8) і (4.9) замінити Q на Q_u і R_1 на R_1 / $Q_к$.

Розглянемо окремі випадки застосування другого методу контролю.

Перший випадок. Так, у деяких випадках, знаючи вагу вектору $\{\pi_N\}_{R_1}$ можна оцінити число помилок, скориставшись результатами доказу наступного твердження.

Твердження 4.3. Якщо мінімальна відстань R–коду дорівнює d і вага одного з векторів $\{\pi_N\}_{R_1}$ або $\{\pi_N + 1\}_{R_1}$ дорівнює $t > k$, то число помилок, що спотворили кодове слово A, не менше, ніж $d - t$.

Доказ. Припустимо спочатку, що A є додатним числом. Тоді числу $\left|A - \left|A'\right|_N\right|$ відповідає кодове слово, вага якого не може бути менша, ніж d, якщо $A \neq (\left|A'\right|_N)$. З іншого боку, з формули (4.7) виходить, що:

$$W = (N\pi_N - \Delta) = W(A - \left|A'\right|_N) \geq d\ .$$

Скориставшись вираженням (4.7), отримаємо наступну нерівність:

$$W(\Delta) \geq W(N\pi_N - \Delta) - W(N\pi_N) \geq d - t$$

оскільки

$$W(N\pi_N) = W\{N\pi_N\}_{R_1}\ .$$

Якщо число A від'ємне, то величині $N + A - \left|A'\right|_N$ відповідає деяке кодове слово. Тому

$$W(\Delta) \geq W(N(\pi_N + 1) - \Delta) - W(N(\pi_N + 1)) \geq d - t.$$

Другий випадок. Якщо помилки сталися тільки в залишках по контрольних модулях, то процедура їх контролю і виправлення значно спрощується. В цьому випадку можна скористатися результатами наступного твердження.

Твердження 4.4. Нехай мінімальна відстань *R*-коду $d = 2k + 1$ і вага одного з векторів $\{\pi_N\}_{R_1}$ чи $\{\pi_N + 1\}_{R_1}$ не перевищує величини *k*. Тоді вектор помилки відповідно рівний або $\{\pi_N N\}_M$ або $\{(\pi_N + 1N)\}_M$.

Доказ. Використовуючи формулу (4.7) і очевидну рівність $W\{\pi_N\}_{R_1} = W\{\pi_N N\}_M$ отримаємо наступний вираз:

$$W\{\pi_N\}_{R_1} \geq W\{A - |A'|_N\}_M - W\{\Delta\}_M. \qquad (4.10)$$

Нехай *A* – додатне число. Тоді вектор $\{|A - |A'|_N|\}_M$ є кодовим словом і вага його не може бути менша, ніж $2k + 1$ окрім випадку, коли $A = |A'|_N$. Якщо $A \neq |A'|_N$, то права частина нерівності (4.10) строго більше *k*, оскільки $W\{\Delta\}_M \leq k$, а ліва частина за умовою не перевищує величини k.

Отже, $A = |A'|_N$ і відповідно до формули (4.7) $\{\Delta\}_M = \{\pi_N N\}_M$.

Припустимо тепер, що *A* – від'ємне число. Тоді:

$$W\{N + A - |A'|_N\}_M \geq 2k + 1.$$

Додаючи величину $(N - N)$ до правої частини виразу (4.7) і виконуючи еквівалентні перетворення, отримаємо:

$$\Delta = (\pi_N + 1)N - (N + A - |A'|_N).$$

З цього виразу виходить, що:

$$W\{\pi_N\}_{R_1} \geq W\{N + A - |A'|_N\}_M - W\{\Delta\}_M .$$

Так само як і у попередньому випадку, ця нерівність справедлива лише тоді, коли $N + A - |A'|_N = 0$. Тому $\{\Delta\}_M = \{(\pi_N + 1)N\}_M$. Твердження доведено.

Наведемо приклад контролю і корекції помилок за допомогою *R*-кодів.

Приклад 4.1. Нехай задана СЗК основами: $m_1 = 5$, $m_2 = 7$, $m_3 = 8$, $m_4 = 11$, $m_5 = 13$, $m_6 = 17$, $m_7 = 19$, $m_8 = 3$. При цьому $N = 280$, $R_1 = 135567$. Припустимо, що $L = 2N = 560$. Тоді мінімальна відстань коду дорівнює 5. При цьому задовольняються умови твердження 4.2.

Розглянемо кодове слово $\{A\}_M = \{-250\}_M = \{0,2,6,3,10,5,16,2\}_M$, у якого у символах, що відповідають модулям m_3 та m_7 сталися помилки $\Delta a_3 = 4$, $\Delta a_7 = 10$. Тоді $\{A'\}_M = \{0,2,2,3,10,5,7,2\}_M$. Передусім, визначимо позиційну характеристику $\{\pi_N\}_{R_1} = \{4,5,7,6,0\}_{R_1}$. Ваги векторів $\{\pi_N\}_{R_1}$ та $\{\pi_N + 1\}_{R_1}$ дорівнюють відповідно чотирьом та п'яти, тобто обоє більше за *k*. Тому, щонайменше, одна помилка сталася в інформаційному модулі. Обчислимо тепер вектор $\{\delta\}_{R_1} = \{\pi_N + 2\}_{R_1}$: $\{\delta\}_{R_1} = \{6,7,9,8,2\}_{R_1}$.

Далі перевіримо справедливість нерівності $\{\delta m_i\}_{R_1} < 3m_i$, де $i = 1, 2, 3$. У даному випадку величина δ множиться тільки на інформаційні основи, оскільки нам наперед відомо, що якщо помилка є поодинокою, то вона не може статися в якому-небудь з контрольних модулів.

Перевірку цієї нерівності виконаємо таким чином. Вичислимо величину $[|\delta m_i|_{R_1} / m_4] = \delta_1$. Якщо $\delta_1 \geq 3$, тоді нерівність не виконується, оскільки $m_4 / m_i > 1,3$. Якщо $\delta_1 < 2$, тоді можна вважати, що помилка виникає

у модулі m_i. Нарешті, якщо $\delta_1 = 2$, тоді слід визначити знак числа $\left|\delta m_i\right|_{R_1} - 3m_i$. Отже:

$$\{\delta 5\}_{R_1} = \{8,9,11,2,1\}_{R_1};\ \{\delta_1\}_{R_1/11} = \{6,8,4,1\}_{R_1/11};\ \{\delta 7\}_{R_1} = \{9,10,12,16,2\}_{R_1};$$

$$\{\delta_1\}_{R_1/11} = \{6,8,8,1\}_{R_1/11};\ \{\delta 8\}_{R_1} = \{4,4,4,7,1\}_{R_1};\ \{\delta_1\}_{R_1/11} = \{0,0,2,0\}_{R_1/11}.$$

Оскільки в усіх трьох випадках $\delta_1 > 3$ можна стверджувати, що у кодовому слові сталася подвійна помилка.

У загальному випадку далі слід перевіряти справедливість нерівностей $\left|\delta m_i m_j\right|_{R_1} < 3m_i m_j$, де $i, j = 1,...,m;\ i \neq j$. Проте ми можемо помітити, що у вектора $\{\delta_1\}_{R_1/11} = \{[\delta 8/11]\}_{R_1/11}$ є тільки одна ненульова компонента, що відповідає модулю $m_7 = 19$. Тому $\left|\delta_1\right|_{R_1/11\cdot 19} = 0 < 2$. Отже, можна стверджувати, що помилки сталися в основах m_3 і m_7. Для визначення вектору помилки скористаємось формулою (4.9), враховуючи той факт, що модуль m_7 є контрольним, тобто $Q = m_3$ і $\left|\delta Q\right|_{R_1} = \left|\delta 8\right|_{R_1/19}$. При цьому:

$$\left\{\left|\delta 8\right|_{R_1/19}\right\}_M = \{4,4,4,4,4,4,4,1\}_M;\ \{N/8\}_M = \{0,0,3,2,9,1,16,2\}_M;$$

$$\{\delta N\}_M = \{0,0,0,8,10,4,17,2\}_M;\ \{-\Delta\}_M = \{0,0,4,0,0,0,9,0\}_M.$$

Додаючи останню величину до вектору A', отримаємо вихідне кодове слово $\{A\}_M = \{0,2,6,3,10,5,16,2\}_M$.

Наведений приклад підтверджує можливість практичної реалізації розглянутих методів контролю даних у СЗК.

4.3 Метод контролю даних у СЗК на основі принципу порівняння

Усі методи контролю даних у СЗК засновані на порівнянні контрольованого числа $A=\left(a_1 \| a_2 \| \ldots \| a_n \| a_{n+1}\right)$ з інформаційним числовим діапазоном $[0, M=\prod_{i=1}^{n} m_i)$. При розгляді методу контролю даних у СЗК, заснованого на принципі порівняння, скористаємось результатами доказу відомого наукового твердження [44].

Твердження 4.5. Нехай СЗК з інформаційними $\{m_i\}$ $(i=\overline{1,n})$ і однією контрольною $m_к = m_n+1$ основами впорядковані ($m_i < m_i+1$), і нехай результат $A=(a_1 \| a_2 \| \ldots \| a_{i-1} \| a_i \| a_{i+1} \| \ldots \| a_n \| a_{n+1})$ виконання операції є правильним числом, тобто $A<M$ $(M=\prod_{i=1}^{n} m_i)$. Тоді можливо стверджувати, що число $\tilde{A}=(a_1 \| a_2 \| \ldots \| a_{i-1} \| \tilde{a}_i \| a_{i+1} \| \ldots \| a_n \| a_{n+1})$, у якому спотворений один залишок $\tilde{a}_i \neq a_i$ по модулю m_i, є неправильним, тобто $\tilde{A} \geq M$.

На основі принципу порівняння правильність числа A визначається виходячи із співвідношення $A<M=M_0 / m_{n+1}$ $(M_0=\prod_{i=1}^{n+1} m_i)$. З іншого боку очевидне виконання умови $M_0 / m_i > M_0 / m_{n+1}$ для впорядкованої СЗК при $i=\overline{1,n}$. У цьому випадку виконується наступна нерівність $A<M_0 / m_i$. Відмітимо, що залишок $a_i \equiv A(\mathrm{mod}\, m_i)$ числа A по модулю m_i може набувати тільки значення $a_i=\overline{0, m_i-1}$. Відповідно до умови твердження $\tilde{a}_i \neq a_i$, і враховуючи, те що інші значення залишків a_j ($j=\overline{1, n+1}$ та $i \neq j$) невірного $\tilde{A}$ числа залишаються без змін, то у числовому інтервалі [0, M_0 / m_i) не можуть одночасно знаходиться обидва числа A і $\tilde{A}$. Тоді, оскільки число $A < M_0 / m_n+1$ правильне (знаходиться в інформаційному числовому [0, M] інтервалі), то число $\tilde{A}$ знаходиться поза інтервалом [0, M_0 / m_i), і тим більше знаходиться поза інтервалом [0, M) (рис. 4.1, 4.2).

У цьому випадку число $\tilde{A}$, для якого виконується умова $\tilde{A} \geq M$, є неправильним. Таким чином, показано, що число $A = (a_1 \| a_2 \| \ldots \| a_{i-1} \| \tilde{a}_i \| a_{i+1} \| \ldots \| a_n \| a_{n+1})$ є спотвореним.

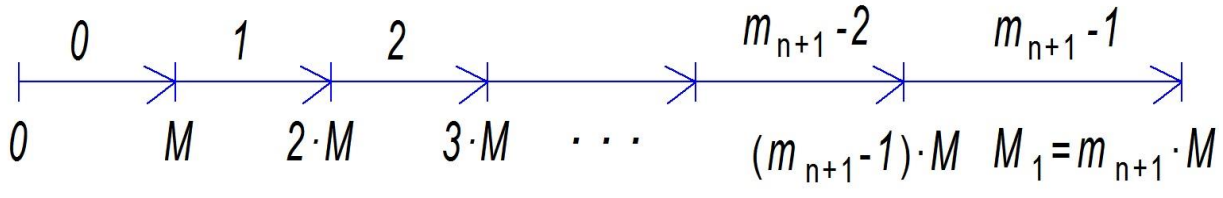

Рис. 4.1 Числові інтервали для довільного модуля m_i СЗК

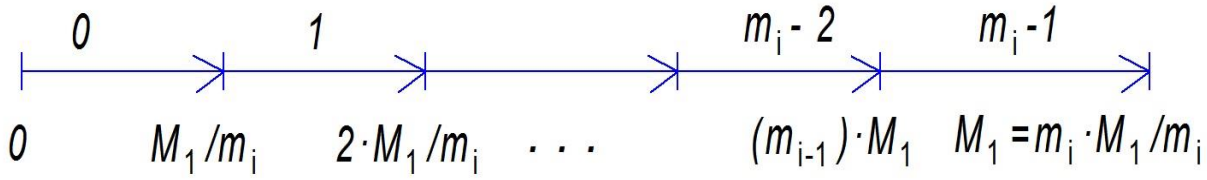

Рис. 4.2 Числові інтервали для $m_к = m_n+1$

Розглянемо метод контролю даних у СЗК, що ґрунтується на результатах і виводах розглянутого наукового твердження. В основі контролю лежить базова операція – порівняння результату операції A з числом $M = M_0/m_n+1$. Для порівняння чисел $A = (a_1 \| a_2 \| \ldots \| a_n \| a_{n+1})$ і M необхідно перевести значення A у ПСЧ. Для цього можна використати ортогональні базиси B_i $(i = \overline{1, n+1})$, які представляються у вигляді:

$$\begin{cases} B_1 = (1,0,\ldots,0,\ldots,0,0), \\ B_2 = (0,1,\ldots,0,\ldots,0,0), \\ \quad \bullet\bullet\bullet \\ B_i = (0,0,\ldots,1,\ldots,0,0), \\ \quad \bullet\bullet\bullet \\ B_n = (0,0,\ldots,0,\ldots,1,0), \\ B_{n+1} = (0,0,\ldots,0,\ldots,0,1). \end{cases}$$

Ортогональні базиси B_i визначаються для кожного СЗК відповідно до виразу

$$B_i = \bar{m}_i \cdot M_0 / m_i \equiv 1 (\mathrm{mod}\, m_i) \tag{4.11}$$

Значення ваги $\bar{m}_i$ ортогонального базису B_i визначається як одне з рішень системи порівнянь :

$$\begin{cases} \bar{m}_i = 1, & 1 \cdot M_i \equiv \rho_1 (\mathrm{mod}\, m_i), \\ \bar{m}_i = 2, & 2 \cdot M_i \equiv \rho_2 (\mathrm{mod}\, m_i), \\ & \bullet \; \bullet \; \bullet \\ \bar{m}_i = m_i - 2, & (m_i - 2) \cdot M_i \equiv \rho_{m_i - 2} (\mathrm{mod}\, m_i), \\ \bar{m}_i = m_i - 1, & (m_i - 1) \cdot M_i \equiv \rho_{m_i - 1} (\mathrm{mod}\, m_i). \end{cases} \tag{4.12}$$

Значення $\bar{m}_i$ для якого виконується умова (4.11), визначається шляхом підстановки можливих значень $\bar{m}_i = \overline{1, m_i - 1}$ методом простого перебору. Значення $A_{ПСЧ}$ у ПСЧ визначається відповідно до відомої формули

$$A_{ПСЧ} = (\sum_{i=1}^{n+1} a_i \cdot B_i) \bmod M_0 \tag{4.13}$$

У загальному вигляді метод контролю у СЗК представлений на рис. 4.3.

Наведемо приклади реалізації методу контролю даних у СЗК. Для однобайтової ($l = 1$) розрядної сітки КСКОЦД у СЗК може бути задана інформаційними $m_1 = 3,\ m_2 = 4,\ m_3 = 5,\ m_4 = 7$ і контрольним $m_k = m_5 = 11$ основами. Дана СЗК забезпечує інформаційний числовий інтервал [0, M) для однобайтової КСКОЦД, де $M = \prod_{i=1}^{4} m_i = 420$.

Повний числовий інтервал представлення чисел у СЗК визначається як $[0, M_0)$, де $M_0 = M \cdot m_{n+1} = 4620$ (рис. 4.4).

1	Вибір основ $m_i \ (i = \overline{1, n+\kappa})$ СЗК
	Визначається сукупність $\{m_i\}$ можливих основ, з подальшою оптимізацією набору основ СЗК.
2	Визначення значень $M_i \ (i = \overline{1, n+\kappa})$ СЗК
	$M_0 = m_1 \cdot m_2 \cdot ... \cdot m_{i-1} \cdot m_i \cdot m_{i+1} \cdot ... \cdot m_{n+\kappa-1} \cdot m_{n+\kappa},$ • • • $M_i = m_1 \cdot m_2 \cdot ... \cdot m_{i-1} \cdot m_{i+1} \cdot ... \cdot m_{n+\kappa-1} \cdot m_{n+\kappa},$ • • • $M_{n+\kappa} = M_0 / m_{n+\kappa} = m_1 \cdot m_2 \cdot ... \cdot m_i \cdot ... \cdot m_{n+\kappa-1}.$
3	Визначення ваги $\bar{m}_i \ (i = \overline{1, n+\kappa})$ ортогональних B_i базисів СЗК
	$\bar{m}_i = 1, \quad 1 \cdot M_i \equiv \rho_1 (\mathrm{mod}\, m_i),$ • • • $\bar{m}_i = m_i - 2, \ (m_i - 2) \cdot M_i \equiv \rho_{m_i-2} (\mathrm{mod}\, m_i),$ $\bar{m}_i = m_i - 1, \ (m_i - 1) \cdot M_i \equiv \rho_{m_i-1} (\mathrm{mod}\, m_i).$
4	Визначення ортогональних *Bi* базисів СЗК
	$B_i = \bar{m}_i \cdot M_0 / m_i = \bar{m}_i \cdot M_i = 1 (\mathrm{mod}\, m_i).$ $\begin{cases} B_1 = (1,0,...,0,...,0,0), \\ \quad \bullet \bullet \bullet \\ B_i = (0,0,...,1,...,0,0), \\ \quad \bullet \bullet \bullet \\ B_{n+\kappa} = (0,0,...,0,...,0,1). \end{cases}$
5	Контроль даних $A = (a_1 \,\|\| \, a_2 \,\|\| ... \,\|\| \, a_{n+\kappa})$ у СЗК
	1. Визначення значення $A_{ПСЧ} = \left(\sum_{i=1}^{n+\kappa} a_i \cdot B_i \right) \mathrm{mod}\, M_0.$ 2. Порівняння величин $A_{ПСЧ}$ і $M = \prod_{i=1}^{n} m_i$. 3. Якщо $A_{ПСС} < M$, те число A правильне. 4. Якщо $A_{ПСС} \geq$ M, то число A неправильне

Рис. 4.3 Метод контролю даних у СЗК, що заснований на принципі порівняння

У табл. 4.1÷4.5 представлені відповідно до (4.12) процедури визначення значень $\bar{m}_i$ $(i=\overline{1,5})$, а у табл. 4.6 приведені розраховані значення ортогональних базисів B_i $(i=\overline{1,5})$ для даної СЗК.

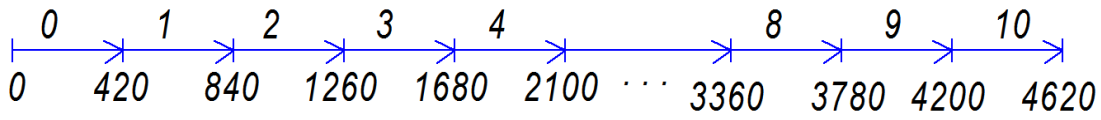

Рис. 4.4 Числові інтервали для l = 1 ($m_k = m_{n+1} = 11$)

Таблиця 4.1

Процедура визначення $\bar{m}_1$

$m_1=3,\quad M_1=4\cdot5\cdot7\cdot11=1540$	
$\bar{m}_1=1$	$\bar{m}_1\cdot M_1=1540\equiv1(\mathrm{mod}\,m_1)$
$\bar{m}_2=2$	$\bar{m}_1\cdot M_1=3080\equiv2(\mathrm{mod}\,m_1)$
$\bar{m}_1=1,\quad B_1=(1,0,0,0,0)=1540$	

Таблиця 4.2

Процедура визначення $\bar{m}_2$

$m_2=4,\quad M_2=3\cdot5\cdot7\cdot11=1155$	
$\bar{m}_2=1$	$1\cdot M_2=1155\equiv3(\mathrm{mod}\,m_2)$
$\bar{m}_2=2$	$2\cdot M_2=2310\equiv2(\mathrm{mod}\,m_2)$
$\bar{m}_2=3$	$3\cdot M_2=3465\equiv1(\mathrm{mod}\,m_2)$
$\bar{m}_2=3,\quad B_2=(0,1,0,0,0)=3465$	

Таблиця 4.3

Процедура визначення $\bar{m}_3$

$m_3=5,\quad M_3=3\cdot4\cdot7\cdot11=924$	
$\bar{m}_3=1$	$1\cdot M_3=924\equiv4(\mathrm{mod}\,m_3)$
$\bar{m}_3=2$	$2\cdot M_3=1848\equiv3(\mathrm{mod}\,m_3)$
$\bar{m}_3=3$	$3\cdot M_3=2772\equiv2(\mathrm{mod}\,m_3)$
$\bar{m}_3=4$	$4\cdot M_2=3696\equiv1(\mathrm{mod}\,m_3)$
$\bar{m}_3=4,\quad B_3=(0,0,1,0,0)=3696$	

Таблиця 4.4

Процедура визначення $\bar{m}_4$

$m_4=7,\quad M_4=3\cdot4\cdot5\cdot11=660$	
$\bar{m}_4=1$	$1\cdot M_4=660\equiv2(\mathrm{mod}\,m_4)$
$\bar{m}_4=2$	$2\cdot M_4=1320\equiv4(\mathrm{mod}\,m_4)$
$\bar{m}_4=3$	$3\cdot M_4=1980\equiv6(\mathrm{mod}\,m_4)$
$\bar{m}_4=4$	$4\cdot M_4=2640\equiv1(\mathrm{mod}\,m_4)$
$\bar{m}_4=5$	$5\cdot M_4=3300\equiv3(\mathrm{mod}\,m_4)$
$\bar{m}_4=6$	$6\cdot M_4=3960\equiv5(\mathrm{mod}\,m_4)$
$\bar{m}_4=4,\quad B_4=(0,0,0,1,0)=2640$	

Таблиця 4.5

Процедура визначення $\bar{m}_5$

$m_5=11,\quad M_5=3\cdot4\cdot5\cdot7=420$	
$\bar{m}_5=1$	$1\cdot M_5=420\equiv2(\mathrm{mod}\,m_5)$
$\bar{m}_5=2$	$2\cdot M_5=840\equiv4(\mathrm{mod}\,m_5)$
$\bar{m}_5=3$	$3\cdot M_5=1260\equiv6(\mathrm{mod}\,m_5)$
$\bar{m}_5=4$	$4\cdot M_5=1680\equiv8(\mathrm{mod}\,m_5)$
$\bar{m}_5=5$	$5\cdot M_5=2100\equiv10(\mathrm{mod}\,m_5)$
$\bar{m}_5=6$	$6\cdot M_5=2520\equiv1(\mathrm{mod}\,m_5)$
$\bar{m}_5=7$	$7\cdot M_5=2940\equiv3(\mathrm{mod}\,m_5)$
$\bar{m}_5=8$	$8\cdot M_5=3360\equiv5(\mathrm{mod}\,m_5)$
$\bar{m}_5=9$	$9\cdot M_5=3780\equiv7(\mathrm{mod}\,m_5)$
$\bar{m}_5=10$	$10\cdot M_5=4200\equiv9(\mathrm{mod}\,m_5)$
$\bar{m}_5=6,\quad B_5=(0,0,0,0,1)=2520$	

Таблиця 4.6

Ортогональні базиси B_i СЗК

$B_1 = (1 \| 0 \| 0 \| 0 \| 0) = 1540, \quad \bar{m}_1 = 1$
$B_2 = (0 \| 1 \| 0 \| 0 \| 0) = 3465, \quad \bar{m}_2 = 3$
$B_3 = (0 \| 0 \| 1 \| 0 \| 0) = 3696, \quad \bar{m}_3 = 4$
$B_4 = (0 \| 0 \| 0 \| 1 \| 0) = 2640, \quad \bar{m}_4 = 4$
$B_5 = (0 \| 0 \| 0 \| 0 \| 1) = 2520, \quad \bar{m}_5 = 6$

Розглянемо приклади реалізації методу контролю даних у СЗК. Нехай задане правильне (A = 400 < M = 420) число $A = (1 \| 0 \| 0 \| 1 \| 4)$ у СЗК.

Приклад 4.2. Визначити правильність отриманого числа $\tilde{A} = (\tilde{0} \| 0 \| 0 \| 1 \| 4)$, що спотворене за основою $m_1 = 3$ ($\tilde{a}_1 = 0$).

Проведемо контроль цього числа $\tilde{A}$. Переводимо число $\tilde{A}$ у ПСЧ і порівнюємо його з величиною M = 420. Отримаємо наступний вираз:

$$\tilde{A} = (\sum_{i=1}^{n+1} a_i \cdot B_i) \bmod M_0 = (\sum_{i=1}^{5} a_i \cdot B_i) \bmod 4620 =$$

$$= (1540 \cdot 0 + 3465 \cdot 0 + 3696 \cdot 0 + 2640 \cdot 1 +$$

$$+2520 \cdot 4) \bmod 4620 = 12720 \bmod (4620) = 3480 > 420.$$

Висновок. Таким чином, операнд $\tilde{A}$ – неправильний і містить помилку в якомусь одному з п'яти залишків числа.

Приклад 4.3. Нехай число $A = (1 \| 0 \| 0 \| 1 \| 4)$ неспотворене. У цьому випадку отримаємо:

$$A = (1540 \cdot 1 + 3465 \cdot 0 + 3696 \cdot 0 + 2640 \cdot 1 +$$

$$+2520 \cdot 4) \bmod 4620 = 14260 (\bmod 4620) = 400 < 420.$$

Висновок. Число A – правильне, тобто знаходиться в інформаційному [0, 420) числовому інтервалі [47].

4.4 Методи контролю даних у СЗК на основі принципу нульовизації

Як відомо, основною перевагою використання СЗК, порівняно з ПСЧ, являється можливість організації у СЗК процесу швидкої реалізації цілочислових арифметичних операцій додавання, віднімання та множення [119-125]. Проте у процесі рішення конкретної обчислювальної задачі виникає необхідність реалізації контролю результату операцій, тобто виникає необхідність використання процедури нульовизації (ПН) НКС. Застосування процедури нульовизації, яка складає до 90% часу контролю даних у СЗК, вимагає значних часових витрат, що позбавляє СЗК її основної переваги [126]. Таким чином, розробка процедури швидкої нульовизації чисел, є дуже актуальною.

4.4.1 Метод послідовного віднімання

Розглянемо процедуру нульовизації з точки зору часу її реалізації. Суть першої (Н1), базової у теорії СЗК, процедури нульовизації (процедура послідовної нульовизації (ППН)) складається з послідовності операцій віднімання виду

$$A^{(i+1)} = A^{(i)} - KH^{(i)}, \tag{4.13}$$

за допомогою сукупності констант нульовизації (КН) виду (4.14)

$$KH^{(0)} = [t_1^{(0)} \| t_2^{(0)} \| t_3^{(0)} \| \ldots \| t_{i-1}^{(0)} \| t_i^{(0)} \| t_{i+1}^{(0)} \| \ldots \| t_{n-3}^{(0)} \| t_{n-2}^{(0)} \| t_{n-1}^{(0)} \| t_n^{(0)} \| t_{n+1}^{(0)}],$$

$$t_1^{(0)} = a_1^{(0)},\ t_1^{(0)} = \overline{0, m_1 - 1};$$

$$KH^{(1)} = [0 \| t_2^{(1)} \| t_3^{(1)} \| \ldots \| t_{i-1}^{(1)} \| t_i^{(1)} \| t_{i+1}^{(1)} \| \ldots \| t_{n-3}^{(1)} \| t_{n-2}^{(1)} \| t_{n-1}^{(1)} \| t_n^{(1)} \| t_{n+1}^{(1)}],$$

$$t_2^{(1)} = a_2^{(1)},\ t_2^{(1)} = \overline{0, m_2 - 1};$$

$$KH^{(2)} = [0 \| 0 \| t_3^{(2)} \| \ldots \| t_{i-1}^{(2)} \| t_i^{(2)} \| t_{i+1}^{(2)} \| \ldots \| t_{n-3}^{(2)} \| t_{n-2}^{(2)} \| t_{n-1}^{(2)} \| t_n^{(2)} \| t_{n+1}^{(2)}],$$

$$t_3^{(2)} = a_3^{(2)},\ t_3^{(2)} = \overline{0, m_3 - 1};$$

$$KH^{(i-1)} = [0 \| 0 \| 0 \| \ldots \| 0 \| t_i^{(i-1)} \| t_{i+1}^{(i-1)} \| \ldots \| t_{n-3}^{(i-1)} \| t_{n-2}^{(i-1)} \| t_{n-1}^{(i-1)} \| t_n^{(i-1)} \| t_{n+1}^{(i-1)}],$$

$$t_i^{(i-1)} = a_i^{(i-1)},\ t_i^{(i-1)} = \overline{0, m_i - 1};$$

$$KH^{(n-2)} = [0 \| 0 \| 0 \| \ldots \| 0 \| 0 \| 0 \| \ldots \| 0 \| 0 \| t_{n-1}^{(n-2)} \| t_n^{(n-2)} \| t_{n+1}^{(n-2)}]\ ,$$

$$t_{n-1}^{(n-2)} = a_{n-1}^{(n-2)},\ t_{n-1}^{(n-2)} = \overline{0, m_{n-1} - 1};$$

$$KH^{(n-1)} = [0 \| 0 \| 0 \| \ldots \| 0 \| 0 \| 0 \| \ldots \| 0 \| 0 \| 0 \| t_n^{(n-1)} \| t_{n+1}^{(n-1)}],$$

$$t_n^{(n-1)} = a_n^{(n-1)},\ t_n^{(n-1)} = \overline{0, m_n - 1}, \qquad (4.14)$$

з відповідних чисел

$$A^{(0)} = [a_1^{(0)} \| a_2^{(0)} \| a_3^{(0)} \| \ldots \| a_{i-1}^{(0)} \| a_i^{(0)} \| a_{i+1}^{(0)} \| \ldots \| a_{n-3}^{(0)} \| a_{n-2}^{(0)} \| a_{n-1}^{(0)} \| a_n^{(0)} \| a_{n+1}^{(0)}],$$

$$A^{(1)} = [0 \| a_2^{(1)} \| a_3^{(1)} \| \ldots \| a_{i-1}^{(1)} \| a_i^{(1)} \| a_{i+1}^{(1)} \| \ldots \| a_{n-3}^{(1)} \| a_{n-2}^{(1)} \| a_{n-1}^{(1)} \| a_n^{(1)} \| a_{n+1}^{(1)}],$$

$$A^{(2)} = [0 \| 0 \| a_3^{(2)} \| \ldots \| a_{i-1}^{(2)} \| a_i^{(2)} \| a_{i+1}^{(2)} \| \ldots \| a_{n-3}^{(2)} \| a_{n-2}^{(2)} \| a_{n-1}^{(2)} \| a_n^{(2)} \| a_{n+1}^{(2)}],$$

$A^{(i-1)} = [0 \| 0 \| 0 \| \ldots \| 0 \| a_i^{(i-1)} \| a_{i+1}^{(i-1)} \| \ldots \| a_{n-3}^{(i-1)} \| a_{n-2}^{(i-1)} \| a_{n-1}^{(i-1)} \| a_n^{(i-1)} \| a_{n+1}^{(i-1)}]$ і так далі.

Наприклад: виконання першої операції віднімання

$$A^{(1)} = A^{(0)} - KH^{(0)} = [a_1^{(0)} \| a_2^{(0)} \| a_3^{(0)} \| \ldots \| a_{i-1}^{(0)} \| a_i^{(0)} \| a_{i+1}^{(0)} \| \ldots$$

$$\ldots \| a_{n-3}^{(0)} \| a_{n-2}^{(0)} \| a_{n-1}^{(0)} \| a_n^{(0)} \| a_{n+1}^{(0)}] - [t_1^{(0)} \| t_2^{(0)} \| t_3^{(0)} \| \ldots \| t_{i-1}^{(0)} \| t_i^{(0)} \| t_{i+1}^{(0)} \| \ldots$$

$$\ldots \| t_{n-3}^{(0)} \| t_{n-2}^{(0)} \| t_{n-1}^{(0)} \| t_n^{(0)} \| t_{n+1}^{(0)}] = \{[a_1^{(0)} - t_1^{(0)}] \bmod m_1 \| [a_2^{(0)} - t_2^{(0)}] \bmod m_2 \|$$

$$\| [a_3^{(0)} - t_3^{(0)}] \bmod m_3 \| \ldots \| [a_{i-1}^{(0)} - t_{i-1}^{(0)}] \bmod m_{i-1} \| [a_i^{(0)} - t_i^{(0)}] \bmod m_i \|$$

$$\| [a_{i+1}^{(0)} - t_{i+1}^{(0)}] \bmod m_{i+1} \| \ldots \| [a_{n-3}^{(0)} - t_{n-3}^{(0)}] \bmod m_{n-3} \| [a_{n-2}^{(0)} - t_{n-2}^{(0)}] \bmod m_{n-2} \|$$

$$\| [a_{n-1}^{(0)} - t_{n-1}^{(0)}] \bmod m_{n-1} \| [a_n^{(0)} - t_n^{(0)}] \bmod m_n \| [a_{n+1}^{(0)} - t_{n+1}^{(0)}] \bmod m_{n+1} \} =$$

$$= [0 \| a_2^{(1)} \| a_3^{(1)} \| \ldots \| a_{i-1}^{(1)} \| a_i^{(1)} \| a_{i+1}^{(1)} \| \ldots \| a_{n-3}^{(1)} \| a_{n-2}^{(1)} \| a_{n-1}^{(1)} \| a_n^{(1)} \| a_{n+1}^{(1)}];$$

виконання другої операції віднімання

$$A^{(2)} = A^{(1)} - KH^{(1)} =$$

$$= [0 \| a_2^{(1)} \| a_3^{(1)} \| \ldots \| a_{i-1}^{(1)} \| a_i^{(1)} \| a_{i+1}^{(1)} \| \ldots \| a_{n-3}^{(1)} \| a_{n-2}^{(1)} \| a_{n-1}^{(1)} \| a_n^{(1)} \| a_{n+1}^{(1)}] -$$

$$-[0 \| t_2^{(1)} \| t_3^{(1)} \| \ldots \| t_{i-1}^{(1)} \| t_i^{(1)} \| t_{i+1}^{(1)} \| \ldots \| t_{n-3}^{(1)} \| t_{n-2}^{(1)} \| t_{n-1}^{(1)} \| t_n^{(1)} \| t_{n+1}^{(1)}] =$$

$$= \{0 \| [a_2^{(1)} - t_2^{(1)}] \bmod m_2 \| [a_3^{(1)} - t_3^{(1)}] \bmod m_3 \| \ldots \| [a_{i-1}^{(1)} - t_{i-1}^{(1)}] \bmod m_{i-1} \|$$

$$\| [a_i^{(1)} - t_i^{(1)}] \bmod m_i \| [a_{i+1}^{(1)} - t_{i+1}^{(1)}] \bmod m_{i+1} \| \ldots \| [a_{n-3}^{(1)} - t_{n-3}^{(1)}] \bmod m_{n-3} \|$$

$$\| [a_{n-2}^{(1)} - t_{n-2}^{(1)}] \bmod m_{n-2} \| [a_{n-1}^{(1)} - t_{n-1}^{(1)}] \bmod m_{n-1} \| [a_n^{(1)} - t_n^{(1)}] \bmod m_n \|$$

$$\| [a_{n+1}^{(1)} - t_{n+1}^{(1)}] \bmod m_{n+1} \} =$$

$$= [0 \| 0 \| a_3^{(2)} \| \ldots \| a_{i-1}^{(2)} \| a_i^{(2)} \| a_{i+1}^{(2)} \| \ldots \| a_{n-3}^{(2)} \| a_{n-2}^{(2)} \| a_{n-1}^{(2)} \| a_n^{(2)} \| a_{n+1}^{(2)}];$$

виконання третьої операції віднімання

$$A^{(3)} = A^{(2)} - KH^{(2)} =$$

$$= [0 \| 0 \| a_3^{(2)} \| \ldots \| a_{i-1}^{(2)} \| a_i^{(2)} \| a_{i+1}^{(2)} \| \ldots \| a_{n-3}^{(2)} \| a_{n-2}^{(2)} \| a_{n-1}^{(2)} \| a_n^{(2)} \| a_{n+1}^{(2)}] -$$

$$-[0 \| 0 \| t_3^{(2)} \| \ldots \| t_{i-1}^{(2)} \| t_i^{(2)} \| t_{i+1}^{(2)} \| \ldots \| t_{n-3}^{(2)} \| t_{n-2}^{(2)} \| t_{n-1}^{(2)} \| t_n^{(2)} \| t_{n+1}^{(2)}] =$$

$$= \{0 \| 0 \| [a_3^{(2)} - t_3^{(2)}] \bmod m_3 \| \ldots \| [a_{i-1}^{(2)} - t_{i-1}^{(2)}] \bmod m_{i-1} \| [a_i^{(2)} - t_i^{(2)}] \bmod m_i \|$$

$$\| [a_{i+1}^{(2)} - t_{i+1}^{(2)}] \bmod m_{i+1} \| \ldots \| [a_{n-3}^{(2)} - t_{n-3}^{(2)}] \bmod m_{n-3} \| [a_{n-2}^{(2)} - t_{n-2}^{(2)}] \bmod m_{n-2} \|$$

$$\| [a_{n-1}^{(2)} - t_{n-1}^{(2)}] \bmod m_{n-1} \| [a_n^{(2)} - t_n^{(2)}] \bmod m_n \| [a_{n+1}^{(2)} - t_{n+1}^{(2)}] \bmod m_{n+1} \} =$$

$$= [0 \| 0 \| 0 \| a_4^{(3)} \| a_5^{(3)} \| \ldots \| a_{i-1}^{(3)} \| a_i^{(3)} \| a_{i+1}^{(3)} \| \ldots \| a_{n-3}^{(3)} \| a_{n-2}^{(3)} \| a_{n-1}^{(3)} \| a_n^{(3)} \| a_{n+1}^{(3)}],$$ і так далі.

Алгоритм виконання процедури ПН представлений у табл. 4.7. Відповідно до цього алгоритму вихідне число $A = A^{(0)} = (a_1^{(0)} \| a_2^{(0)} \| \ldots \| a_i^{(0)} \| \| a_{i+1}^{(0)} \| \ldots \| a_n^{(0)} \| a_{n+1}^{(0)})$ за формулою (4.13) послідовно зводиться до виду $A^{(H)} = (0 \| 0 \| \ldots \| 0 \| \gamma_{n+1})$ за допомогою такої послідовності операцій віднімання, яка не приведе до виходу числового значення числа $A^{(0)}$ за

робочий діапазон $[0, M)$ СЗК. У цьому випадку вихідне число $A = A^{(0)} = (a_1^{(0)} \| a_2^{(0)} \| ... \| a_i^{(0)} \| a_{i+1}^{(0)} \| ... \| a_n^{(0)} \| a_{n+1}^{(0)})$ послідовно зводиться до виду *A,* тобто $A = A^{(0)} = (a_1^{(0)} \| a_2^{(0)} \| ... \| a_i^{(0)} \| a_{i+1}^{(0)} \| ... \| a_n^{(0)} \| a_{n+1}^{(0)})$, $A^{(1)} = (0 \| a_2^{(1)} \| a_3^{(1)} \| ... \| a_n^{(1)} \| a_{n+1}^{(1)})$, $A^{(2)} = (0 \| 0 \| a_3^{(2)} \| ... \| a_n^{(2)} \| a_{n+1}^{(2)})$ і так далі.

Продовжуючи віднімання *n* разів, отримаємо значення $A^{(H)} = (0 \| 0 \| ... \| 0 \| a_{n+1}^{(n)})$ або $A^{(H)} = (0 \| 0 \| ... \| 0 \| \gamma_{n+1})$, де $\gamma_{n+1} = a_{n+1}^{(n)}$. Процедура ПН представлена на рис. 4.5.

Таблиця 4.7

Алгоритм процедури послідовного віднімання

№ операції	Зміст операції
1	Звернення по значенню $a_1^{(0)}$ числа $A^{(0)}$ у $БКН_0$ за $КН^{(0)}$.
2	Виконання операції віднімання $A^{(1)} = A^{(0)} - КН^{(0)}$.
3	Звернення по значенню $a_2^{(1)}$ числа $A^{(1)}$ у $БКН_1$ за $КН^{(1)}$.
4	Виконання операції віднімання $A^{(2)} = A^{(1)} - КН^{(1)}$.
5	Звернення по значенню $a_3^{(2)}$ числа $A^{(2)}$ у $БКН_2$ за $КН^{(2)}$.
6	Виконання операції віднімання $A^{(3)} = A^{(2)} - КН^{(2)}$.
7	Звернення по значенню $a_4^{(3)}$ числа $A^{(3)}$ у $БКН_3$ за $КН^{(3)}$.
8	Виконання операції віднімання $A^{(4)} = A^{(3)} - КН^{(3)}$.
⋮	…
$2n-3$	Звернення по значенню $a_{n-1}^{(n-2)}$ числа $A^{(n-2)}$ у $БКН_{n-2}$ за $КН^{(n-2)}$.
$2n-2$	Виконання операції віднімання $A^{(n-1)} = A^{(n-2)} - КН^{(n-2)}$.
$2n-1$	Звернення по значенню $a_n^{(n-1)}$ числа $A^{(n-1)}$ у $БКН_{n-1}$ за $КН^{(n-1)}$.
$2n$	Виконання операції віднімання $A^{(n)} = A^{(n-1)} - КН^{(n-1)}$. Отримання нульовизованого числа $A^{(H)} = A^{(n)} = [0 \| 0 \| ... \| 0 \| ... \| 0 \| 0 \| \gamma_{n+1} = a_{n+1}^{(n)}]$.

№ операції (такту)	Зміст операції
1	Звернення по значенню залишку $a_1^{(0)}$ числа $A = A^{(0)} = [a_1^{(0)} \| a_2^{(0)} \| \| a_3^{(0)} \| \ldots \| a_{i-1}^{(0)} \| a_i^{(0)} \| a_{i+1}^{(0)} \| \ldots \| a_{n-3}^{(0)} \| a_{n-2}^{(0)} \| a_{n-1}^{(0)} \| a_n^{(0)} \| a_{n+1}^{(0)}]$ у $БКН_0$ за константою нульвизації $КН^{(0)} = [t_1^{(0)} \| t_2^{(0)} \| t_3^{(0)} \| \ldots \| t_{i-1}^{(0)} \| t_i^{(0)} \| t_{i+1}^{(0)} \| \ldots \ldots \| t_{n-3}^{(0)} \| t_{n-2}^{(0)} \| t_{n-1}^{(0)} \| t_n^{(0)} \| t_{n+1}^{(0)}]$; $t_1^{(0)} = a_1^{(0)}$; $t_1^{(0)} = \overline{0, m_1 - 1}$.
2	Виконання операції віднімання $A^{(1)} = A^{(0)} - КН^{(0)} = [a_1^{(0)} \| a_2^{(0)} \| \| a_3^{(0)} \| \ldots \| a_{i-1}^{(0)} \| a_i^{(0)} \| a_{i+1}^{(0)} \| \ldots \| a_{n-3}^{(0)} \| a_{n-2}^{(0)} \| a_{n-1}^{(0)} \| a_n^{(0)} \| a_{n+1}^{(0)}] - [t_1^{(0)} \| t_2^{(0)} \| t_3^{(0)} \| \ldots \| t_{i-1}^{(0)} \| t_i^{(0)} \| t_{i+1}^{(0)} \| \ldots \| t_{n-3}^{(0)} \| t_{n-2}^{(0)} \| t_{n-1}^{(0)} \| t_n^{(0)} \| t_{n+1}^{(0)}] = \{[a_1^{(0)} - t_1^{(0)}] \bmod m_1 \| [a_2^{(0)} - t_2^{(0)}] \bmod m_2 \| [a_3^{(0)} - t_3^{(0)}] \bmod m_3 \| \ldots \ldots \| [a_{i-1}^{(0)} - t_{i-1}^{(0)}] \bmod m_{i-1} \| [a_i^{(0)} - t_i^{(0)}] \bmod m_i \| [a_{i+1}^{(0)} - t_{i+1}^{(0)}] \bmod m_{i+1} \| \ldots \ldots \| [a_{n-3}^{(0)} - t_{n-3}^{(0)}] \bmod m_{n-3} \| [a_{n-2}^{(0)} - t_{n-2}^{(0)}] \bmod m_{n-2} \| [a_{n-1}^{(0)} - t_{n-1}^{(0)}] \bmod m_{n-1} \| \| [a_n^{(0)} - t_n^{(0)}] \bmod m_n \| [a_{n+1}^{(0)} - t_{n+1}^{(0)}] \bmod m_{n+1}\} = [0 \| a_2^{(1)} \| a_3^{(1)} \| \ldots \| a_{i-1}^{(1)} \| a_i^{(1)} \| \| a_{i+1}^{(1)} \| \ldots \| a_{n-3}^{(1)} \| a_{n-2}^{(1)} \| a_{n-1}^{(1)} \| a_n^{(1)} \| a_{n+1}^{(1)}]$.
3	Звернення по значенню залишку $a_2^{(1)}$ числа $A^{(1)} = [0 \| a_2^{(1)} \| a_3^{(1)} \| \ldots \ldots \| a_{i-1}^{(1)} \| a_i^{(1)} \| a_{i+1}^{(1)} \| \ldots \| a_{n-3}^{(1)} \| a_{n-2}^{(1)} \| a_{n-1}^{(1)} \| a_n^{(1)} \| a_{n+1}^{(1)}]$ у $БКН_1$ за константою нульвизації $КН^{(1)} = [0 \| t_2^{(1)} \| t_3^{(1)} \| \ldots \| t_{i-1}^{(1)} \| t_i^{(1)} \| t_{i+1}^{(1)} \| \ldots \| t_{n-3}^{(1)} \| t_{n-2}^{(1)} \| \| t_{n-1}^{(1)} \| t_n^{(1)} \| t_{n+1}^{(1)}]$; $t_2^{(1)} = a_2^{(1)}$; $t_2^{(1)} = \overline{0, m_2 - 1}$.
4	Виконання операції віднімання $A^{(2)} = A^{(1)} - КН^{(1)} = \left[0 \| a_2^{(1)} \| a_3^{(1)} \| \ldots \ldots \| a_{i-1}^{(1)} \| a_i^{(1)} \| a_{i+1}^{(1)} \| \ldots \| a_{n-3}^{(1)} \| a_{n-2}^{(1)} \| a_{n-1}^{(1)} \| a_n^{(1)} \| a_{n+1}^{(1)}\right] - \left[0 \| t_2^{(1)} \| t_3^{(1)} \| \ldots \| t_{i-1}^{(1)} \| t_i^{(1)} \| t_{i+1}^{(1)} \| \ldots \| t_{n-3}^{(1)} \| t_{n-2}^{(1)} \| t_{n-1}^{(1)} \| t_n^{(1)} \| t_{n+1}^{(1)}\right] = \{0 \| [a_2^{(1)} - t_2^{(1)}] \bmod m_2 \| \| [a_3^{(1)} - t_3^{(1)}] \bmod m_3 \| \ldots \| [a_{i-1}^{(1)} - t_{i-1}^{(1)}] \bmod m_{i-1} \| [a_i^{(1)} - t_i^{(1)}] \bmod m_i \| \| [a_{i+1}^{(1)} - t_{i+1}^{(1)}] \bmod m_{i+1} \| \ldots \| [a_{n-3}^{(1)} - t_{n-3}^{(1)}] \bmod m_{n-3} \| [a_{n-2}^{(1)} - t_{n-2}^{(1)}] \bmod m_{n-2} \| \| [a_{n-1}^{(1)} - t_{n-1}^{(1)}] \bmod m_{n-1} \| [a_n^{(1)} - t_n^{(1)}] \bmod m_n \| [a_{n+1}^{(1)} - t_{n+1}^{(1)}] \bmod m_{n+1}\} = [0 \| 0 \| a_3^{(2)} \| \ldots \| a_{i-1}^{(2)} \| a_i^{(2)} \| a_{i+1}^{(2)} \| \ldots \| a_{n-3}^{(2)} \| a_{n-2}^{(2)} \| a_{n-1}^{(2)} \| a_n^{(2)} \| a_{n+1}^{(2)}]$.

Рис. 4.5 Процедура ПН чисел у СЗК

5	Звернення по значенню залишку $a_3^{(2)}$ числа $A^{(2)} = [0 \| 0 \| a_3^{(2)} \| \dots$ $\dots \| a_{i-1}^{(2)} \| a_i^{(2)} \| a_{i+1}^{(2)} \| \dots \| a_{n-3}^{(2)} \| a_{n-2}^{(2)} \| a_{n-1}^{(2)} \| a_n^{(2)} \| a_{n+1}^{(2)}]$ у $БКН_2$ за константою нульвизації $KH^{(2)} = [0 \| 0 \| t_3^{(2)} \| \dots \| t_{i-1}^{(2)} \| t_i^{(2)} \| t_{i+1}^{(2)} \| \dots \| t_{n-3}^{(2)} \| t_{n-2}^{(2)} \| t_{n-1}^{(2)} \|$ $\| t_n^{(2)} \| t_{n+1}^{(2)}]$; $t_3^{(2)} = a_3^{(2)}$; $t_3^{(2)} = \overline{0, m_3 - 1}$.
6	Виконання операції віднімання $A^{(3)} = A^{(2)} - KH^{(2)} = [0 \| 0 \| a_3^{(2)} \| \dots$ $\dots \| a_{i-1}^{(2)} \| a_i^{(2)} \| a_{i+1}^{(2)} \| \dots \| a_{n-3}^{(2)} \| a_{n-2}^{(2)} \| a_{n-1}^{(2)} \| a_n^{(2)} \| a_{n+1}^{(2)}] - [0 \| 0 \| t_3^{(2)} \| \dots \| t_{i-1}^{(2)} \|$ $\| t_i^{(2)} \| t_{i+1}^{(2)} \| \dots \| t_{n-3}^{(2)} \| t_{n-2}^{(2)} \| t_{n-1}^{(2)} \| t_n^{(2)} \| t_{n+1}^{(2)}] = \{0 \| 0 \| [a_3^{(2)} - t_3^{(2)}] \bmod m_3 \| \dots$ $\dots \| [a_{i-1}^{(2)} - t_{i-1}^{(2)}] \bmod m_{i-1} \| [a_i^{(2)} - t_i^{(2)}] \bmod m_i \| [a_{i+1}^{(2)} - t_{i+1}^{(2)}] \bmod m_{i+1} \| \dots$ $\dots \| [a_{n-3}^{(2)} - t_{n-3}^{(2)}] \bmod m_{n-3} \| [a_{n-2}^{(2)} - t_{n-2}^{(2)}] \bmod m_{n-2} \| [a_{n-1}^{(2)} - t_{n-1}^{(2)}] \bmod m_{n-1} \|$ $\| [a_n^{(2)} - t_n^{(2)}] \bmod m_n \| [a_{n+1}^{(2)} - t_{n+1}^{(2)}] \bmod m_{n+1} \} =$ $= [0 \| 0 \| 0 \| a_4^{(3)} \| a_5^{(3)} \| \dots \| a_{i-1}^{(3)} \| a_i^{(3)} \| a_{i+1}^{(3)} \| \dots \| a_{n-3}^{(3)} \| a_{n-2}^{(3)} \| a_{n-1}^{(3)} \| a_n^{(3)} \| a_{n+1}^{(3)}]$.
7	Звернення по значенню залишку $a_4^{(3)}$ числа $A^{(3)} = [0 \| 0 \| 0 \| a_4^{(3)} \|$ $\| a_5^{(3)} \| \dots \| a_{i-1}^{(3)} \| a_i^{(3)} \| a_{i+1}^{(3)} \| \dots \| a_{n-3}^{(3)} \| a_{n-2}^{(3)} \| a_{n-1}^{(3)} \| a_n^{(3)} \| a_{n+1}^{(3)}]$ у $БКН_3$ за константою нульвизації $KH^{(3)} = [0 \| 0 \| 0 \| t_4^{(3)} \| t_5^{(3)} \| \dots \| t_{i-1}^{(3)} \| t_i^{(3)} \| t_{i+1}^{(3)} \| \dots$ $\| t_{n-3}^{(3)} \| t_{n-2}^{(3)} \| t_{n-1}^{(3)} \| t_n^{(3)} \| t_{n+1}^{(3)}]$; $t_4^{(3)} = a_4^{(3)}$; $t_4^{(3)} = \overline{0, m_4 - 1}$.
8	Виконання операції віднімання $A^{(4)} = A^{(3)} - KH^{(3)} = [0 \| 0 \| 0 \| a_4^{(3)} \|$ $\| a_5^{(3)} \| \dots \| a_{i-1}^{(3)} \| a_i^{(3)} \| a_{i+1}^{(3)} \| \dots \| a_{n-3}^{(3)} \| a_{n-2}^{(3)} \| a_{n-1}^{(3)} \| a_n^{(3)} \| a_{n+1}^{(3)}] - [0 \| 0 \| 0 \| t_4^{(3)} \|$ $\| t_5^{(3)} \| \dots \| t_{i-1}^{(3)} \| t_i^{(3)} \| t_{i+1}^{(3)} \| \dots \| t_{n-3}^{(3)} \| t_{n-2}^{(3)} \| t_{n-1}^{(3)} \| t_n^{(3)} \| t_{n+1}^{(3)}] =$ $= \{0 \| 0 \| 0 \| [a_4^{(3)} - t_4^{(3)}] \bmod m_4 \| [a_5^{(3)} - t_5^{(3)}] \bmod m_5 \| \dots \| [a_{i-1}^{(3)} - t_{i-1}^{(3)}] \bmod m_{i-1} \|$ $\| [a_i^{(3)} - t_i^{(3)}] \bmod m_i \| [a_{i+1}^{(3)} - t_{i+1}^{(3)}] \bmod m_{i+1} \| \dots \| [a_{n-3}^{(3)} - t_{n-3}^{(3)}] \bmod m_{n-3} \|$ $\| [a_{n-2}^{(3)} - t_{n-2}^{(3)}] \bmod m_{n-2} \| [a_{n-1}^{(3)} - t_{n-1}^{(3)}] \bmod m_{n-1} \| [a_n^{(3)} - t_n^{(3)}] \bmod m_n \|$ $\| [a_{n+1}^{(3)} - t_{n+1}^{(3)}] \bmod m_{n+1} \} = [0 \| 0 \| 0 \| 0 \| a_5^{(4)} \| \dots \| a_{i-1}^{(4)} \| a_i^{(4)} \| a_{i+1}^{(4)} \| \dots$ $\dots \| a_{n-3}^{(4)} \| a_{n-2}^{(4)} \| a_{n-1}^{(4)} \| a_n^{(4)} \| a_{n+1}^{(4)}]$.

Рис. 4.5, аркуш 2

Для значення $A^{(i)}$	Звернення по значенню залишку $a_i^{(i-1)}$ числа $A^{(i-1)}=[0\|\|0\|\|0\|\|\ldots\|\|0\|\|$ $\|\|a_i^{(i-1)}\|\|a_{i+1}^{(i-1)}\|\|\ldots\|\|a_{n-3}^{(i-1)}\|\|a_{n-2}^{(i-1)}\|\|a_{n-1}^{(i-1)}\|\|a_n^{(i-1)}\|\|a_{n+1}^{(i-1)}]$ у $БКН_{i-1}$ за константою нульвизації $KH^{(i-1)}=[0\|\|0\|\|0\|\|\ldots\|\|0\|\|t_i^{(i-1)}\|\|t_{i+1}^{(i-1)}\|\|\ldots\|\|t_{n-3}^{(i-1)}\|\|t_{n-2}^{(i-1)}\|\|t_{n-1}^{(i-1)}\|\|$ $\|\|t_n^{(i-1)}\|\|t_{n+1}^{(i-1)}]$; $t_i^{(i-1)}=a_i^{(i-1)}$; $t_i^{(i-1)}=\overline{0,m_i-1}$.
	Виконання операції віднімання $A^{(i)}=A^{(i-1)}-KH^{(i-1)}=[0\|\|0\|\|0\|\|\ldots$ $\ldots\|\|0\|\|a_i^{(i-1)}\|\|a_{i+1}^{(i-1)}\|\|\ldots\|\|a_{n-3}^{(i-1)}\|\|a_{n-2}^{(i-1)}\|\|a_{n-1}^{(i-1)}\|\|a_n^{(i-1)}\|\|a_{n+1}^{(i-1)}]-[0\|\|0\|\|0\|\|\ldots\|\|0\|\|$ $\|\|t_i^{(i-1)}\|\|t_{i+1}^{(i-1)}\|\|\ldots\|\|t_{n-3}^{(i-1)}\|\|t_{n-2}^{(i-1)}\|\|t_{n-1}^{(i-1)}\|\|t_n^{(i-1)}\|\|t_{n+1}^{(i-1)}]=\{0\|\|0\|\|0\|\|\ldots\|\|0\|\|$ $\|[a_i^{(i-1)}-t_i^{(i-1)}]\bmod m_i\|[a_{i+1}^{(i-1)}-t_{i+1}^{(i-1)}]\bmod m_{i+1}\|\ldots\|[a_{n-3}^{(i-1)}-t_{n-3}^{(i-1)}]\bmod m_{n-3}\|$ $\|[a_{n-2}^{(i-1)}-t_{n-2}^{(i-1)}]\bmod m_{n-2}\|[a_{n-1}^{(i-1)}-t_{n-1}^{(i-1)}]\bmod m_{n-1}\|[a_n^{(i-1)}-t_n^{(i-1)}]\bmod m_n\|$ $\|[a_{n+1}^{(i-1)}-t_{n+1}^{(i-1)}]\bmod m_{n+1}\}=[0\|\|0\|\|0\|\|\ldots\|\|0\|\|0\|\|a_{i+1}^{(i)}\|\|\ldots\|\|a_{n-3}^{(i)}\|\|a_{n-2}^{(i)}\|\|a_{n-1}^{(i)}\|\|$ $\|a_n^{(i)}\|\|a_{n+1}^{(i)}]$.
$2n-3$	Звернення по значенню залишку $a_{n-1}^{(n-2)}$ і числа $A^{(n-2)}=[0\|\|0\|\|0\|\|\ldots$ $\ldots\|\|0\|\|0\|\|0\|\|\ldots\|\|0\|\|0\|\|a_{n-1}^{(n-2)}\|\|a_n^{(n-2)}\|\|a_{n+1}^{(n-2)}]$ у $БКН_{n-2}$ за константою нульвизації $KH^{(n-2)}=[0\|\|0\|\|0\|\|\ldots\|\|0\|\|0\|\|0\|\|\ldots\|\|0\|\|0\|\|t_{n-1}^{(n-2)}\|\|t_n^{(n-2)}\|\|$ $\|\|t_{n+1}^{(n-2)}]$; $t_{n-1}^{(n-2)}=a_{n-1}^{(n-2)}$; $t_{n-1}^{(n-2)}=\overline{0,m_{n-1}-1}$.
$2n-2$	Виконання операції віднімання $A^{(n-1)}=A^{(n-2)}-KH^{(n-2)}=[0\|\|0\|\|0\|\|\ldots$ $\ldots\|\|0\|\|0\|\|0\|\|\ldots\|\|0\|\|0\|\|a_{n-1}^{(n-2)}\|\|a_n^{(n-2)}\|\|a_{n+1}^{(n-2)}]-[0\|\|0\|\|0\|\|\ldots\|\|0\|\|0\|\|0\|\|\ldots$ $\ldots\|\|0\|\|0\|\|t_{n-1}^{(n-2)}\|\|t_n^{(n-2)}\|\|t_{n+1}^{(n-2)}]=\{0\|\|0\|\|0\|\|\ldots\|\|0\|\|0\|\|0\|\|\ldots\|\|0\|\|0\|\|$ $\|[a_{n-1}^{(n-2)}-t_{n-1}^{(n-2)}]\bmod m_{n-1}\|[a_n^{(n-2)}-t_n^{(n-2)}]\bmod m_n\|$ $\|[a_{n+1}^{(n-2)}-t_{n+1}^{(n-2)}]\bmod m_{n+1}\}=[0\|\|0\|\|0\|\|\ldots\|\|0\|\|0\|\|0\|\|\ldots\|\|0\|\|0\|\|0\|\|a_n^{(n-1)}\|\|$ $\|a_{n+1}^{(n-1)}]$.
$2n-1$	Звернення по значенню залишку $a_n^{(n-1)}$ числа $A^{(n-1)}=[0\|\|0\|\|0\|\|\ldots$ $\ldots\|\|0\|\|0\|\|0\|\|\ldots\|\|0\|\|0\|\|0\|\|a_n^{(n-1)}\|\|a_{n+1}^{(n-1)}]$ у $БКН_{n-1}$ за константою нульвизації $KH^{(n-1)}=[0\|\|0\|\|0\|\|\ldots\|\|0\|\|0\|\|0\|\|\ldots\|\|0\|\|0\|\|0\|\|$ $\|\|t_n^{(n-1)}\|\|t_{n+1}^{(n-1)}]$; $t_n^{(n-1)}=a_n^{(n-1)}$; $t_n^{(n-1)}=\overline{0,m_n-1}$.

Рис. 4.5, аркуш 3

$2n$	Отримання нульовизованого числа $A^{(H)} = A^{(n)} = A^{(n-1)} - KH^{(n-1)} =$ $= [0 \| 0 \| 0 \| \ldots \| 0 \| 0 \| 0 \| \ldots \| 0 \| 0 \| 0 \| a_n^{(n-1)} \| a_{n+1}^{(n-1)}] - [0 \| 0 \| 0 \| \ldots \| 0 \| 0 \| 0 \| \ldots$ $\ldots \| 0 \| 0 \| 0 \| t_n^{(n-1)} \| t_{n+1}^{(n-1)}] = \{0 \| 0 \| 0 \| \ldots \| 0 \| 0 \| 0 \| \ldots \| 0 \| 0 \| 0 \|$ $\| [a_n^{(n-1)} - t_n^{(n-1)}] \bmod m_n \| [a_{n+1}^{(n-1)} - t_{n+1}^{(n-1)}] \bmod m_{n+1}\} = [0 \| 0 \| 0 \| \ldots \| 0 \| 0 \| 0 \| \ldots$ $\ldots \| 0 \| 0 \| 0 \| 0 \| a_{n+1}^{(n)}]$, де $a_{n+1}^{(n)} = \gamma_{n+1}$.
$T_{H1} = 2 \cdot n \cdot \tau_{сл}$	

Рис. 4.5, аркуш 4

Позначивши час вибірки КН з відповідного БКН КСКОЦД, що функціонує у СЗК, як t_1, а час віднімання з числа $A^{(i-1)}$ константи $KH^{(i-1)}$, тобто виконання операції $A^{(i)} = A^{(i-1)} - KH^{(i-1)}$ – як t_2, отримаємо загальний час T_{H1} виконання процедури нульовизації для першого $H1$ методу

$$T_{H1} = n\,(t_1 + t_2). \qquad (4.15)$$

При реалізації БН у табличному варіанті можна вважати, що практично $t_1 = t_2 = \tau_{сл}$. У цьому випадку для процедури ПН час нульовизації дорівнює значенню $T_{H1} = 2n\tau_{сл}$, де: $\tau_{сл}$ – час віднімання з числа $A^{(i)}$ константи нульовизації $KH^{(i)}$; n – кількість інформаційних основ СЗК. Окрім цього для реалізації процедури нульовизації за першим методом $H1$ у БН необхідно зберігати $K_{H1} = \sum_{i+1}^{n} m_i - n$ констант нульовизації. При цьому кількість N_{H1} двійкових розрядів констант нульовизації, яке посередньо визначає кількість обладнання (ємність) БКН КСКОЦД, визначається виразом $N_{H1} = \left(\sum_{i+1}^{n} m_i - 1 \right)(n-i)$. Очевидно, що розглянута базова процедура ПН не

вичерпує можливості підвищення швидкодії реалізації процедури нульовизації чисел, оскільки виконання операції віднімання $A^{(i+1)} = A^{(i)} - KH^{(i)}$ і вибірки чергової КН рознесені у часі. Це обумовлено тим, що доки не закінчена операція віднімання, заздалегідь невідомий залишок числа, по якому має бути вибрана КН для наступного етапу процедури нульовизації [127-129].

4.4.2 Метод паралельного віднімання

Суть запропонованого методу паралельного віднімання (МПВ) полягає у тому, що процедура нульовизації здійснюється паралельно у часі по двох основах. Для n – парного числа маємо $a_i^{(i-1)}$, $a_{n-i+1}^{(i-1)}$ ($i = \overline{1, n/2}$), а саме $a_1^{(0)}$, $a_n^{(0)}$; $a_2^{(1)}$, $a_{n-1}^{(1)}$; $a_3^{(2)}$, $a_{n-2}^{(2)}$; ... $a_{n/2}^{(n/2)}$, $a_{n/2+1}^{(n)/2)}$ (рис. 4.6). Для n – непарного числа маємо, що $a_1^{(0)}$, $a_n^{(0)}$; $a_2^{(1)}$, $a_{n-1}^{(1)}$; $a_3^{(2)}$, $a_{n-2}^{(2)}$; ... $a_{(n+1)/2}^{((n+1)/2-1)}$ (рис. 4.7). У цьому випадку для довільного значення i KH для відповідного числа мають наступний вигляд

$$A^{(i)} = [\overbrace{0\|0\|\ldots\|0}^{i-\text{нулей}}\|a_{i+1}^{(i)}\|a_{i+2}^{(i)}\|\ldots\|a_{n-i-1}^{(i)}\|a_{n-i}^{(i)}\|\overbrace{0\|\ldots\|0\|0}^{i-\text{нулей}}\|a_{n+1}^{(i)}],$$

$$KH^{(i)} = [0\|0\|\ldots\|0\|t_{i+1}^{(i)}\|t_{i+2}^{(i)}\|\ldots\|t_{n-i-1}^{(i)}\|t_{n-i}^{(i)}\|0\|\ldots\|0\|0\|t_{n+1}^{(i)}];$$

$$t_{i+1}^{(i)} = \overline{0, m_{i+1}},\ t_{n-i}^{(i)} = \overline{0, m_{n-i}};\ t_{i+1}^{(i)} = a_{i+1}^{(i)},\ t_{n-i}^{(i)} = a_{n-i}^{(i)}.$$

Для довільного значення i маємо, що

$$A^{(i+1)} = A^{(i)} - KH^{(i)} =$$

$$= [0\|0\|\ldots\|0\|a_{i+1}^{(i)}\|a_{i+2}^{(i)}\|a_{i+3}^{(i)}\|\ldots\|a_{n-i-2}^{(i)}\|a_{n-i-1}^{(i)}\|a_{n-i}^{(i)}\|0\|\ldots\|0\|a_{n+1}^{(i)}] -$$

$$-[0\|0\|\ldots\|0\|t_{i+1}^{(i)}\|t_{i+2}^{(i)}\|t_{i+3}^{(i)}\|\ldots\|t_{n-i-2}^{(i)}\|t_{n-i-1}^{(i)}\|t_{n-1}^{(i)}\|0\|\ldots\|0\|t_{n+1}^{(i)}] =$$

$$= \{0\|0\|\ldots\|0\|[a_{i+1}^{(i)} - t_{i+1}^{(i)}] \bmod m_{i+1}\|[a_{i+2}^{(i)} - t_{i+2}^{(i)}] \bmod m_{i+2}\|[a_{i+3}^{(i)} - t_{i+3}^{(i)}] \bmod m_{i+3}\|\ldots$$

$$\ldots \| [a_{n-i-2}^{(i)} - t_{n-i-2}^{(i)}] \bmod m_{n-i-2} \| [a_{n-i-1}^{(i)} - t_{n-i-1}^{(i)}] \bmod m_{n-i-1} \|$$

$$\| [a_{n-i}^{(i)} - t_{n-i}^{(i)}] \bmod m_{n-i} \| 0 \| \ldots \| 0 \| [a_{n+1}^{(i)} - t_{n+1}^{(i)}] \bmod m_{n+1} \} =$$

$$= [0 \| 0 \| \ldots \| 0 \| 0 \| a_{i+2}^{(i+1)} \| a_{i+3}^{(i+1)} \| \ldots \| a_{n-i-2}^{(i+1)} \| a_{n-i-1}^{(i+1)} \| 0 \| 0 \| \ldots \| 0 \| 0 \| a_{n+1}^{(i+1)}].$$

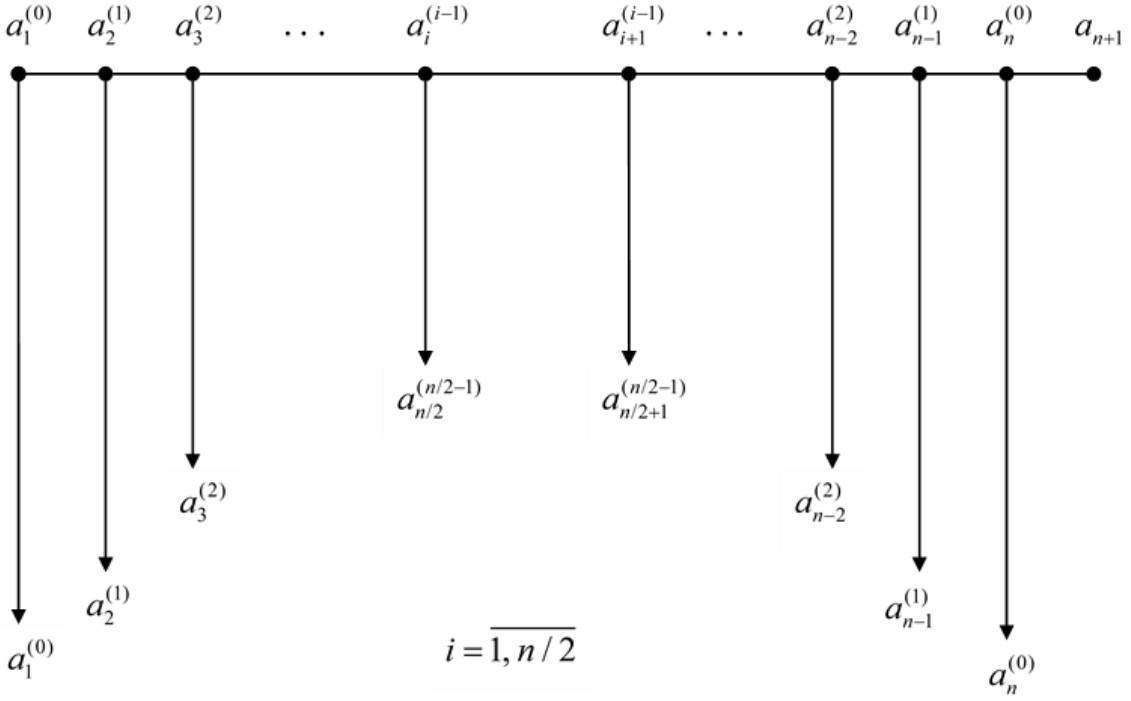

Рис. 4.6 Схема вибірки КН для МПВ (n – парне число)

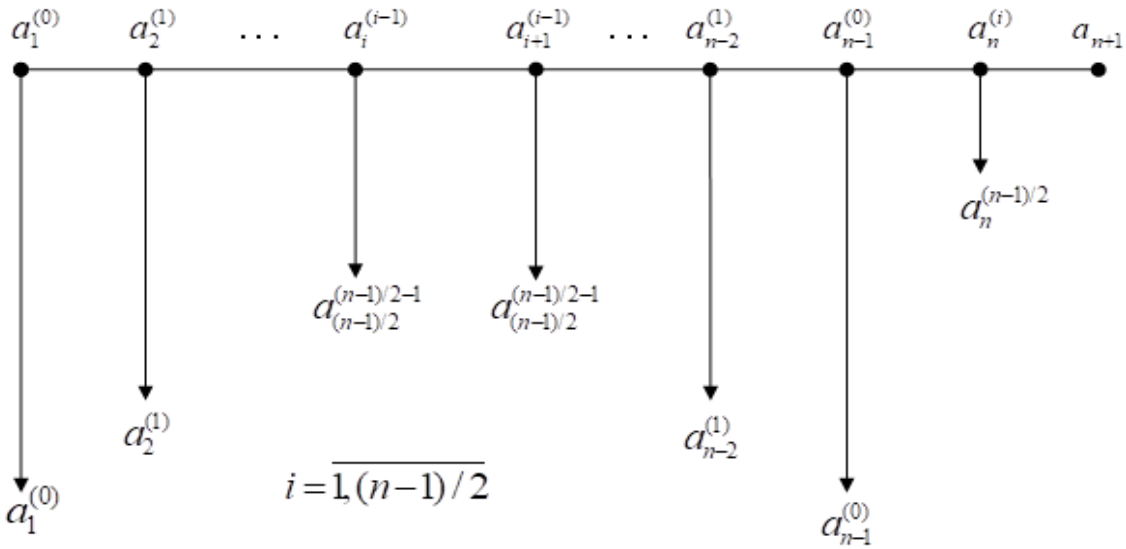

Рис. 4.7 Схема вибірки КН для МПВ (n – непарне число)

Алгоритм виконання процедури нульовизації за МПВ представлений у табл. 4.8.

Перед набуттям значення $\gamma_{n+1} = a_{n+1}^{(n/2)}$ для n – парного числа, маємо, що

$$A^{(n/2-1)} = [\overbrace{0 \| 0 \| \ldots \| 0}^{n/2-1\text{нулів}} \| a_{n/2}^{(n/2-1)} \| a_{n/2+1}^{(n/2-1)} \| \overbrace{0 \| \ldots \| 0 \| 0}^{n/2-1\text{нулів}} \| a_{n+1}^{(n/2-1)}].$$

$$KH^{(n/2-1)} = [\overbrace{0 \| 0 \| \ldots \| 0}^{n/2-1\text{нулів}} \| t_{n/2}^{(n/2-1)} \| t_{n/2+1}^{(n/2-1)} \| \overbrace{0 \| \ldots \| 0 \| 0}^{n/2-1\text{нулів}} \| t_{n+1}^{(n/2-1)}],$$

$$t_{n/2}^{(n/2-1)} = \overline{0, m_{n/2}},\ t_{n/2+1}^{(n/2-1)} = \overline{0, m_{n/2+1}},\ t_{n/2}^{(n/2-1)} = a_{n/2}^{(n/2-1)},\ t_{n/2+1}^{(n/2-1)} = a_{n/2+1}^{(n/2-1)}.$$

$$A^{(H)} = A^{(n/2)} = A^{(n/2-1)} - KH^{(n/2-1)} = \left\{0 \| 0 \| \ldots \| 0 \| \left[a_{n/2}^{(n/2-1)} - t_{n/2}^{(n/2-1)} \right] \bmod m_{n/2} \right\|$$

$$\| \left[a_{n/2+1}^{(n/2-1)} - t_{n/2+1}^{(n/2-1)} \right] \bmod m_{n/2+1} \| 0 \| 0 \| \ldots \| 0 \| 0 \| \left[a_{n+1}^{(n/2-1)} - t_{n+1}^{(n/2-1)} \right] \bmod m_{n+1} \} =$$

$$= \left[0 \| 0 \| \ldots \| 0 \| 0 \| 0 \| \ldots \| 0 \| 0 \| a_{n+1}^{(n/2)} \right], \text{ де } \gamma_{n+1} = a_{n+1}^{(n/2)}.$$

Перед набуттям значення $\gamma_{n+1} = a_{n+1}^{(n/2)}$ для n – непарного числа, маємо, що

$$A^{((n+1)/2-1)} = [\overbrace{0 \| 0 \| \ldots \| 0}^{\frac{n+1}{2}-1\text{ нулів}} \| a_{(n+1)/2}^{((n+1)/2-1)} \overbrace{\| 0 \| \ldots \| 0}^{\frac{n+1}{2}-1\text{ нулів}} \| a_{n+1}^{((n+1)/2-1)}].$$

$$KH^{((n+1)/2-1)} = [0 \| 0 \| \ldots \| 0 \| t_{(n+1)/2}^{((n+1)/2-1)} \| 0 \| \ldots \| 0 \| t_{n+1}^{((n+1)/2-1)}],$$

$$t_{(n+1)/2}^{((n+1)/2-1)} = \overline{0, m_{(n+1)/2}};\ t_{(n+1)/2}^{((n+1)/2-1)} = a_{(n+1)/2}^{((n+1)/2-1)}.$$

$$A^{(H)} = A^{(n+1)/2} = A^{((n+1)/2-1)} - KH^{((n+1)/2-1)} =$$

$$= \left\{0 \| 0 \| \ldots \| 0 \| \left[a_{(n+1)/2}^{((n+1)/2-1)} - t_{(n+1)/2}^{((n+1)/2-1)} \right] \bmod m_{(n+1)/2} \| 0 \| ...0 \| 0 \| \ldots \| 0 \| 0 \| \right.$$

$$\left. \| \left[a_{n+1}^{((n+1)/2-1)} - t_{n+1}^{((n+1)/2-1)} \right] \bmod m_{n+1} \right\} = \left[0 \| 0 \| \ldots \| 0 \| \ldots \| 0 \| 0 \| a_{n+1}^{(n+1)/2} \right], \text{ де } \gamma_{n+1} = a_{n+1}^{(n+1)/2}.$$

Метод паралельного віднімання представлений на рис. 4.8.

Таблиця 4.8

Алгоритм виконання процедури паралельного віднімання

№ операції	Зміст операції
1	Звернення по значеннях залишків $a_1^{(0)}$ і $a_n^{(0)}$ числа $A^{(0)}$ у $БКН_0$ за $КН^{(0)}$.
2	Виконання операції віднімання $A^{(1)} = A^{(0)} - KH^{(0)}$.
3	Звернення по значеннях залишків $a_2^{(1)}$ і $a_{n-1}^{(1)}$ числа $A^{(1)}$ у $БКН_1$ за $КН^{(1)}$.
4	Виконання операції віднімання $A^{(2)} = A^{(1)} - KH^{(1)}$.
5	Звернення по значеннях залишків $a_2^{(2)}$ і $a_{n-2}^{(2)}$ числа $A^{(2)}$ у $БКН_2$ за $КН^{(2)}$.
6	Виконання операції віднімання $A^{(3)} = A^{(2)} - KH^{(2)}$.
…	…
i	Виконання операції віднімання $A^{(i)} = A^{(i-1)} - KH^{(i-1)}$.
$i+1$	Звернення по значеннях залишків $a_{i+1}^{(i)}$ і $a_{n-i}^{(i)}$ числа $A^{(i)}$ у $БКН_i$ за $КН^{(i)}$.
$i+2$	Виконання операції віднімання $A^{(i+1)} = A^{(i)} - KH^{(i)}$.
…	…
$n-3$	Звернення по значеннях залишків $a_{n/2-1}^{(n/2-2)}$ і $a_{n/2+2}^{(n/2-2)}$ числа $A^{(n/2-2)}$ у $БКН_{n/2-2}$ за $КН^{(n/2-2)}$.
$n-2$	Виконання операції віднімання $A^{(n/2-1)} = A^{(n/2-2)} - KH^{(n/2-2)}$.
$n-1$	Звернення по значеннях залишків $a_{n/2}^{(n/2-1)}$ і $a_{n/2+1}^{(n/2-1)}$ числа $A^{(n/2-1)}$ у $БКН_{n/2-1}$ за $КН^{(n/2-1)}$.
n	Виконання операції віднімання $A^{(n/2)} = A^{(n/2-1)} - KH^{(n/2-1)}$. Отримання нульовизованого $A^{(H)}$ числа $A^{(H)} = A^{(n/2)} = [0 \| 0 \| ... \| 0 \| ... \| 0 \| 0 \| \gamma_{n+1} = a_{n+1}^{(n/2)}]$.

№ операції (такту)	Зміст операції
1	Звернення по значеннях залишків $a_1^{(0)}$ і $a_n^{(0)}$ числа $A = A^{(0)} = [a_1^{(0)} \| \| a_2^{(0)} \| a_3^{(0)} \| \ldots \| a_{i-1}^{(0)} \| a_i^{(0)} \| a_{i+1}^{(0)} \| \ldots \| a_{n-3}^{(0)} \| a_{n-2}^{(0)} \| a_{n-1}^{(0)} \| a_n^{(0)} \| a_{n+1}^{(0)}]$ у $БКН_0$ за константою нульвизації $КН^{(0)} = [t_1^{(0)} \| t_2^{(0)} \| t_3^{(0)} \| \ldots \| t_{i-1}^{(0)} \| t_i^{(0)} \| t_{i+1}^{(0)} \| \ldots \| t_{n-3}^{(0)} \| t_{n-2}^{(0)} \| t_{n-1}^{(0)} \| t_n^{(0)} \| t_{n+1}^{(0)}]$; $t_1^{(0)} = a_1^{(0)}$, $t_n^{(0)} = a_n^{(0)}$; $t_1^{(0)} = \overline{0, m_1 - 1}$, $t_n^{(0)} = \overline{0, m_n - 1}$
2	Виконання операції віднімання $A^{(1)} = A^{(0)} - КН^{(0)} = [a_1^{(0)} \| a_2^{(0)} \| \| a_3^{(0)} \| \ldots \| a_{i-1}^{(0)} \| a_i^{(0)} \| a_{i+1}^{(0)} \| \ldots \| a_{n-3}^{(0)} \| a_{n-2}^{(0)} \| a_{n-1}^{(0)} \| a_n^{(0)} \| a_{n+1}^{(0)}] - [t_1^{(0)} \| t_2^{(0)} \| \| t_3^{(0)} \| \ldots \| t_{i-1}^{(0)} \| t_i^{(0)} \| t_{i+1}^{(0)} \| \ldots \| t_{n-3}^{(0)} \| t_{n-2}^{(0)} \| t_{n-1}^{(0)} \| t_n^{(0)} \| t_{n+1}^{(0)}] =$ $= \{[a_1^{(0)} - t_1^{(0)}] \bmod m_1 \| [a_2^{(0)} - t_2^{(0)}] \bmod m_2 \| [a_3^{(0)} - t_3^{(0)}] \bmod m_3 \| \ldots$ $\ldots \| [a_{i-1}^{(0)} - t_{i-1}^{(0)}] \bmod m_{i-1} \| [a_i^{(0)} - t_i^{(0)}] \bmod m_i \| [a_{i+1}^{(0)} - t_{i+1}^{(0)}] \bmod m_{i+1} \| \ldots$ $\ldots \| [a_{n-3}^{(0)} - t_{n-3}^{(0)}] \bmod m_{n-3} \| [a_{n-2}^{(0)} - t_{n-2}^{(0)}] \bmod m_{n-2} \| [a_{n-1}^{(0)} - t_{n-1}^{(0)}] \bmod m_{n-1} \| \ldots$ $\ldots \| [a_n^{(0)} - t_n^{(0)}] \bmod m_n \| [a_{n+1}^{(0)} - t_{n+1}^{(0)}] \bmod m_{n+1}\} = [0 \| a_2^{(1)} \| a_3^{(1)} \| \ldots$ $\ldots \| a_{i-1}^{(1)} \| a_i^{(1)} \| a_{i+1}^{(1)} \| \ldots \| a_{n-3}^{(1)} \| a_{n-2}^{(1)} \| a_{n-1}^{(1)} \| 0 \| a_{n+1}^{(1)}]$.
3	Звернення по значеннях залишків $a_2^{(1)}$ і $a_{n-1}^{(1)}$ числа $A^{(1)} = [0 \| a_2^{(1)} \| \| a_3^{(1)} \| \ldots \| a_{i-1}^{(1)} \| a_i^{(1)} \| a_{i+1}^{(1)} \| \ldots \| a_{n-3}^{(1)} \| a_{n-2}^{(1)} \| a_{n-1}^{(1)} \| 0 \| a_{n+1}^{(1)}]$ у $БКН_1$ за константою нульвизації $КН^{(1)} = [0 \| t_2^{(1)} \| t_3^{(1)} \| \ldots \| t_{i-1}^{(1)} \| t_i^{(1)} \| t_{i+1}^{(1)} \| \ldots \| t_{n-3}^{(1)} \| t_{n-2}^{(1)} \| t_{n-1}^{(1)} \| 0 \| t_{n+1}^{(1)}]$; $t_2^{(1)} = a_2^{(1)}$, $t_{n-1}^{(1)} = a_{n-1}^{(1)}$; $t_2^{(1)} = \overline{0, m_2 - 1}$, $t_{n-1}^{(1)} = \overline{0, m_{n-1} - 1}$.

Рис. 4.8 МПВ у СЗК

4	Виконання операції віднімання $A^{(2)} = A^{(1)} - KH^{(1)} = [0 \| a_2^{(1)} \| \| a_3^{(1)} \| \ldots \| a_{i-1}^{(1)} \| a_i^{(1)} \| a_{i+1}^{(1)} \| \ldots \| a_{n-3}^{(1)} \| a_{n-2}^{(1)} \| a_{n-1}^{(1)} \| 0 \| a_{n+1}^{(1)}] - [0 \| t_2^{(1)} \| t_3^{(1)} \| \ldots \| t_{i-1}^{(1)} \| t_i^{(1)} \| t_{i+1}^{(1)} \| \ldots \| t_{n-3}^{(1)} \| t_{n-2}^{(1)} \| t_{n-1}^{(1)} \| 0 \| t_{n+1}^{(1)}] = \{0 \| [a_2^{(1)} - t_2^{(1)}] \bmod m_2 \| \| [a_3^{(1)} - t_3^{(1)}] \bmod m_3 \| [a_4^{(1)} - t_4^{(1)}] \bmod m_4 \| \ldots \| [a_{i-1}^{(1)} - t_{i-1}^{(1)}] \bmod m_{i-1} \| \| [a_i^{(1)} - t_i^{(1)}] \bmod m_i \| [a_{i+1}^{(1)} - t_{i+1}^{(1)}] \bmod m_{i+1} \| \ldots \| [a_{n-3}^{(1)} - t_{n-3}^{(1)}] \bmod m_{n-3} \| \| [a_{n-2}^{(1)} - t_{n-2}^{(1)}] \bmod m_{n-2} \| [a_{n-1}^{(1)} - t_{n-1}^{(1)}] \bmod m_{n-1} \| 0 \| [a_{n+1}^{(1)} - t_{n+1}^{(1)}] \bmod m_{n+1} \} = = [0 \| 0 \| a_3^{(2)} \| a_4^{(2)} \| \ldots \| a_{i-1}^{(2)} \| a_i^{(2)} \| a_{i+1}^{(2)} \| \ldots \| a_{n-3}^{(2)} \| a_{n-2}^{(2)} \| 0 \| 0 \| a_{n+1}^{(2)}]$.
5	Звернення по значеннях залишків $a_3^{(2)}$ і $a_{n-2}^{(2)}$ числа $A^{(2)} = [0 \| 0 \| \| a_3^{(2)} \| \ldots \| a_{i-1}^{(2)} \| a_i^{(2)} \| a_{i+1}^{(2)} \| \ldots \| a_{n-3}^{(2)} \| a_{n-2}^{(2)} \| 0 \| 0 \| a_{n+1}^{(2)}]$ у $БКН_2$ за константою нульвизації $KH^{(2)} = [0 \| 0 \| t_3^{(2)} \| \ldots \| t_{i-1}^{(2)} \| t_i^{(2)} \| t_{i+1}^{(2)} \| \ldots \| t_{n-3}^{(2)} \| t_{n-2}^{(2)} \| \| 0 \| 0 \| t_{n+1}^{(2)}]$, $t_3^{(2)} = a_3^{(2)}$, $t_{n-2}^{(2)} = a_{n-2}^{(2)}$; $t_3^{(2)} = \overline{0, m_3 - 1}$, $t_{n-2}^{(2)} = \overline{0, m_{n-2} - 1}$.
6	Виконання операції віднімання $A^{(3)} = A^{(2)} - KH^{(2)} = [0 \| 0 \| a_3^{(2)} \| \ldots \| a_{i-1}^{(2)} \| a_i^{(2)} \| a_{i+1}^{(2)} \| \ldots \| a_{n-3}^{(2)} \| a_{n-2}^{(2)} \| 0 \| 0 \| a_{n+1}^{(2)}] - [0 \| 0 \| t_3^{(2)} \| \ldots \| t_{i-1}^{(2)} \| t_i^{(2)} \| t_{i+1}^{(2)} \| \ldots \| t_{n-3}^{(2)} \| t_{n-2}^{(2)} \| 0 \| 0 \| t_{n+1}^{(2)}] = \{0 \| 0 \| [a_3^{(2)} - t_3^{(2)}] \bmod m_3 \| \| [a_4^{(2)} - t_4^{(2)}] \bmod m_4 \| \ldots \| [a_{i-1}^{(2)} - t_{i-1}^{(2)}] \bmod m_{i-1} \| [a_i^{(2)} - t_i^{(2)}] \bmod m_i \| \| [a_{i+1}^{(2)} - t_{i+1}^{(2)}] \bmod m_{i+1} \| \ldots \| [a_{n-3}^{(2)} - t_{n-3}^{(2)}] \bmod m_{n-3} \| [a_{n-2}^{(2)} - t_{n-2}^{(2)}] \bmod m_{n-2} \| \| 0 \| 0 \| [a_{n+1}^{(2)} - t_{n+1}^{(2)}] \bmod m_{n+1} \} = [0 \| 0 \| 0 \| a_4^{(3)} \| a_5^{(2)} \| \ldots \| a_{i-1}^{(3)} \| a_i^{(3)} \| a_{i+1}^{(3)} \| \ldots \| a_{n-4}^{(3)} \| a_{n-3}^{(3)} \| 0 \| 0 \| 0 \| a_{n+1}^{(3)}]$.
...	...

Рис. 4.8, аркуш 2

Для значення $A^{(i)}$	Звернення по значеннях залишків $a_i^{(i-1)}$ і $a_{n-i+1}^{(i-1)}$ числа $A^{(i-1)} = [0 \| \| 0 \| \| \ldots \| \| 0 \| \| a_i^{(i-1)} \| \| a_{i+1}^{(i-1)} \| \| a_{i+2}^{(i-1)} \| \| \ldots \| \| a_{n-i-3}^{(i-1)} \| \| a_{n-i}^{(i-1)} \| \| a_{n-i+1}^{(i-1)} \| \| 0 \| \| 0 \| \| \ldots \| \| 0 \| \| a_{n+1}^{(i-1)}]$ у $БКН_{i-1}$ за константою нульовизації $KH^{(i-1)} = [0 \| \| 0 \| \| \ldots \| \| 0 \| \| t_i^{(i-1)} \| \| t_{i+1}^{(i-1)} \| \| t_{i+2}^{(i-1)} \| \| \ldots \| \| t_{n-i-1}^{(i-1)} \| \| t_{n-i}^{(i-1)} \| \| t_{n-i+1}^{(i-1)} \| \| 0 \| \| 0 \| \| \ldots \| \| 0 \| \| t_{n+1}^{(i-1)}]$; $t_i^{(i-1)} = a_i^{(i-1)}$, $t_{n-i+1}^{(i-1)} = a_{n-i+1}^{(i-1)}$; $t_i^{(i-1)} = \overline{0, m_i - 1}$, $t_{n-i+1}^{(i-1)} = \overline{0, m_{n-i+1} - 1}$.
	Виконання операції віднімання $A^{(i)} = A^{(i-1)} - KH^{(i-1)} = [0 \| \| 0 \| \| 0 \| \| \ldots \| \| 0 \| \| a_i^{(i-1)} \| \| a_{i+1}^{(i-1)} \| \| \ldots \| \| 0 \| \| 0 \| \| a_{n+1}^{(i-1)}] - [0 \| \| 0 \| \| 0 \| \| \ldots \| \| 0 \| \| t_i^{(i-1)} \| \| t_{i+1}^{(i-1)} \| \| \ldots \| \| 0 \| \| 0 \| \| t_{n+1}^{(i-1)}] = \{0 \| \| 0 \| \| \ldots \| \| 0 \| \| [a_i^{(i-1)} - t_i^{(i-1)}] \bmod m_i \| \| [a_{i+1}^{(i-1)} - t_{i+1}^{(i-1)}] \bmod m_{i+1} \| \| [a_{i+2}^{(i-1)} - t_{i+2}^{(i-1)}] \bmod m_{i+2} \| \| \ldots \| \| [a_{n-i-1}^{(i-1)} - t_{n-i-1}^{(i-1)}] \bmod m_{n-i-1} \| \| [a_{n-i}^{(i-1)} - t_{n-i}^{(i-1)}] \bmod m_{n-i} \| \| [a_{n-i+1}^{(i-1)} - t_{n-i+1}^{(i-1)}] \bmod m_{n-i+1} \| \| 0 \| \| 0 \| \| \ldots \| \| 0 \| \| [a_{n+1}^{(i-1)} - t_{n+1}^{(i-1)}] \bmod m_{n+1}\} = [0 \| \| 0 \| \| \ldots \| \| 0 \| \| 0 \| \| a_{i+1}^{(i)} \| \| a_{i+2}^{(i)} \| \| a_{i+3}^{(i)} \| \| \ldots \| \| a_{n-i-1}^{(i)} \| \| a_{n-i}^{(i)} \| \| 0 \| \| 0 \| \| \ldots \| \| 0 \| \| a_{n+1}^{(i)}]$.
Для значення $A^{(i+1)}$	Звернення по значеннях залишків $a_{i+1}^{(i)}$ і $a_{n-i}^{(i)}$ числа $A^{(i)} = [0 \| \| 0 \| \| 0 \| \| \ldots \| \| 0 \| \| 0 \| \| a_{i+1}^{(i)} \| \| \ldots \| \| a_{n-i-1}^{(i)} \| \| a_{n-i}^{(i)} \| \| 0 \| \| 0 \| \| a_{n+1}^{(i)}]$ у $БКН_i$ за константою нульовизації $KH^{(i)} = [0 \| \| 0 \| \| 0 \| \| \ldots \| \| 0 \| \| 0 \| \| t_{i+1}^{(i)} \| \| \ldots \| \| t_{n-i-1}^{(i)} \| \| t_{n-i}^{(i)} \| \| 0 \| \| 0 \| \| t_{n+1}^{(i)}]$; $t_{i+1}^{(i)} = a_{i+1}^{(i)}$, $t_{n-i}^{(i)} = a_{n-i}^{(i)}$; $t_{i+1}^{(i)} = \overline{0, m_{i+1} - 1}$, $t_{n-i}^{(i)} = \overline{0, m_{n-i} - 1}$.
	Виконання операції віднімання $A^{(i+1)} = A^{(i)} - KH^{(i)} = [0 \| \| 0 \| \| \ldots \| \| 0 \| \| a_{i+1}^{(i)} \| \| a_{i+2}^{(i)} \| \| a_{i+3}^{(i)} \| \| \ldots \| \| a_{n-i-2}^{(i)} \| \| a_{n-i-1}^{(i)} \| \| a_{n-i}^{(i)} \| \| 0 \| \| \ldots \| \| 0 \| \| a_{n+1}^{(i)}] - [0 \| \| 0 \| \| \ldots \| \| 0 \| \| t_{i+1}^{(i)} \| \| t_{i+2}^{(i)} \| \| t_{i+3}^{(i)} \| \| \ldots \| \| t_{n-i-2}^{(i)} \| \| t_{n-i-1}^{(i)} \| \| t_{n-1}^{(i)} \| \| 0 \| \| \ldots \| \| 0 \| \| t_{n+1}^{(i)}] = \{0 \| \| 0 \| \| \ldots \| \| 0 \| \| [a_{i+1}^{(i)} - t_{i+1}^{(i)}] \bmod m_{i+1} \| \| [a_{i+2}^{(i)} - t_{i+2}^{(i)}] \bmod m_{i+2} \| \| [a_{i+3}^{(i)} - t_{i+3}^{(i)}] \bmod m_{i+3} \| \| \ldots \| \| [a_{n-i-2}^{(i)} - t_{n-i-2}^{(i)}] \bmod m_{n-i-2} \| \| [a_{n-i-1}^{(i)} - t_{n-i-1}^{(i)}] \bmod m_{n-i-1} \| \| [a_{n-i}^{(i)} - t_{n-i}^{(i)}] \bmod m_{n-i} \| \| 0 \| \| \ldots \| \| 0 \| \| [a_{n+1}^{(i)} - t_{n+1}^{(i)}] \bmod m_{n+1}\} = [0 \| \| 0 \| \| \ldots \| \| 0 \| \| 0 \| \| a_{i+2}^{(i+1)} \| \| a_{i+3}^{(i+1)} \| \| \ldots \| \| a_{n-i-2}^{(i+1)} \| \| a_{n-i-1}^{(i+1)} \| \| 0 \| \| 0 \| \| \ldots \| \| 0 \| \| 0 \| \| a_{n+1}^{(i+1)}]$.
…	…

Рис. 4.8, аркуш 3

$n-1$	Надалі для n – парного і n – непарного чисела отримаємо. Для n парного числа. Звернення по значеннях залишків $a_{n/2}^{(n/2-1)}$ і $a_{n/2+1}^{(n/2-1)}$ числа $A^{(n/2-1)}=[0\|\|0\|\|\ldots\|\|0\|\|a_{n/2}^{(n/2-1)}\|\|a_{n/2+1}^{(n/2-1)}\|\|0\|\|\ldots\|\|0\|\|0\|\|a_{n+1}^{(n/2-1)}]$ у $БКН_{n/2-1}$ за константою нульвизації $КН^{(n/2-1)}=[0\|\|0\|\|\ldots\|\|0\|\|t_{n/2}^{(n/2-1)}\|\|t_{n/2+1}^{(n/2-1)}\|\|0\|\|\ldots\|\|0\|\|0\|\|t_{n+1}^{(n/2-1)}]$; $t_{n/2}^{(n/2-1)}=a_{n/2}^{(n/2-1)}$, $t_{n/2+1}^{(n/2-1)}=a_{n/2+1}^{(n/2-1)}$; $t_{n/2}^{(n/2-1)}=\overline{0,m_{n/2}-1}$, $t_{n/2+1}^{(n/2-1)}=\overline{0,m_{n/2+1}-1}$. Для n непарного числа. Звернення за значенням залишку $a_{(n+1)/2}^{((n+1)/2-1)}$ числа $A^{((n+1)/2-1)}=[0\|\|0\|\|\ldots\|\|0\|\|a_{(n+1)/2}^{((n+1)/2-1)}\|\|0\|\|\ldots\|\|0\|\|a_{n+1}^{((n+1)/2-1)}]$ у $БКН_{(n+1)/2-1}$ за константою нульвизації $КН^{((n+1)/2-1)}=[0\|\|0\|\|\ldots\|\|0\|\|t_{(n+1)/2}^{((n+1)/2-1)}\|\|0\|\|\ldots\|\|0\|\|t_{n+1}^{((n+1)/2-1)}]$, $t_{(n+1)/2}^{((n+1)/2-1)}=a_{(n+1)/2}^{((n+1)/2-1)}$; $t_{(n+1)/2}^{((n+1)/2-1)}=\overline{0,m_{(n+1)/2}-1}$.
n	Для n – парного і n – непарного чисел отримаємо наступне значення нульвизованого числа $A^{(H)}$. Для n парного числа. Отримання нульвизованого $A^{(H)}$ числа: $A^{(H)}=A^{(n/2)}=A^{(n/2-1)}-$ $-КН^{(n/2-1)}=[0\|\|0\|\|\ldots\|\|0\|\|a_{n/2}^{(n/2-1)}\|\|a_{n/2+1}^{(n/2-1)}\|\|0\|\|\ldots\|\|0\|\|0\|\|a_{n+1}^{(n/2-1)}]-$ $-[0\|\|0\|\|\ldots\|\|0\|\|t_{n/2}^{(n/2-1)}\|\|t_{n/2+1}^{(n/2-1)}\|\|0\|\|\ldots\|\|0\|\|0\|\|t_{n+1}^{(n/2-1)}]=\{0\|\|0\|\|\ldots\|\|0\|\|$ $\|[a_{n/2}^{(n/2-1)}-t_{n/2}^{(n/2-1)}]\bmod m_{n/2}\|[a_{n/2+1}^{(n/2-1)}-t_{n/2+1}^{(n/2-1)}]\bmod m_{n/2+1}\|0\|\|\ldots\|\|0\|\|0\|\|$ $\|[a_{n+1}^{(n/2-1)}-t_{n+1}^{(n/2-1)}]\bmod m_{n+1}\}=\left[0\|\|0\|\|\ldots\|\|0\|\|0\|\|0\|\|\ldots\|\|0\|\|0\|\|a_{n+1}^{(n/2)}\right]$, де $\gamma_{n+1}=a_{n+1}^{(n/2)}$. Для n непарного числа. Отримання нульвизованого $A^{(H)}$ числа: $A^{(H)}=A^{(n+1/2)}=A^{((n+1/2-1)}-$ $КН^{((n+1)/2-1)}=[0\|\|0\|\|\ldots\|\|0\|\|a_{(n+1)/2}^{((n+1)/2-1)}\|\|0\|\|\ldots\|\|0\|\|a_{n+1}^{((n+1)/2-1)}]-[0\|\|0\|\|\ldots$ $\ldots\|\|0\|\|t_{(n+1)/2}^{((n+1)/2-1)}\|\|0\|\|\ldots\|\|0\|\|t_{n+1}^{((n+1)/2-1)}]=\{0\|\|0\|\|\ldots\|\|0\|\|$ $\|[a_{(n+1)/2}^{((n+1)/2-1)}-t_{(n+1)/2}^{((n+1)/2-1)}]\bmod m_{(n+1)/2}\|0\|\|\ldots\|\|0\|\|$ $\|[a_{n+1}^{((n+1)/2-1)}-t_{n+1}^{((n+1)/2-1)}]\bmod m_{n+1}\}=[0\|\|0\|\|\ldots\|\|0\|\|\ldots\|\|0\|\|0\|\|a_{n+1}^{((n+1)/2)}]$, де $\gamma_{n+1}=a_{n+1}^{((n+1)/2)}$.
$T_{H3}=n\cdot\tau$	

Рис. 4.8, аркуш 4

Час T_{H3} виконання процедури нульовизації для цього МПВ визначається як

$$T_{H3} = n \cdot \tau_{сл}. \qquad (4.16)$$

При реалізації процедури нульовизації для описаного ($H3$) методу у БКН обчислювача у СЗК необхідно мати $K_{H3} = \sum_{i=1}^{\left[\frac{n}{2}\right]} (m_i \cdot m_{n-i+1} - 1)$ констант нульовизації. При цьому кількість N_{H3} двійкових розрядів констант нульовизації БКН визначається виразом $N_{H3} = \sum_{i=1}^{\left[\frac{n}{2}\right]} (m_i \cdot m_{n-i+1} - 1) \cdot (n - 2i + 1)$.

4.4.3 Метод послідовного віднімання з попереднім аналізом подальшого залишку непозиційної кодової структури у СЗК

Розглянемо процедуру ($H2$) нульовизації – процедуру послідовної нульовизації з визначенням подальшого залишку (ПН ВПЗ), яка усуває недолік описаний при виконанні процедури ($H1$). Використання цієї процедури дозволяє зменшити, у порівнянні з ($H1$) процедурою, час контролю даних у СЗК. Суть процедури полягає в тому, що доки робиться вибірка константи нульовизації

$$KH^{(i)} = [0 \| 0 \| 0 \| \ldots \| 0 \| t_{i+1}^{(i)} \| t_{i+2}^{(i)} \| \ldots \| t_{n-3}^{(i)} \| t_{n-2}^{(i)} \| t_{n-1}^{(i)} \| t_n^{(i)} \| t_{n+1}^{(i)}]$$

для числа

$$A^{(i)} = [0 \| \ \| 0 \| 0 \| \ldots \| a_{i+1}^{(i)} \| a_{i+2}^{(i)} \| \ldots \| a_{n-3}^{(i)} \| a_{n-2}^{(i)} \| a_{n-1}^{(i)} \| a_n^{(i)} \| a_{n+1}^{(i)}]$$

по значенню залишку $a_{i+1}^{(i)}$ по основі m_{i+1} у обчислювальному тракті (ОТ)

КСКОЦД, що функціонує по основі m_{i+2} може бути сформоване значення залишку $a_{i+2}^{(i+1)}$ по якому на наступному етапі нульвизації робитиметься вибірка наступної константи нульвизації

$$KH^{(i+1)} = [0 \| 0 \| 0 \| \ldots \| 0 \| t_{i+2}^{(i+1)} \| t_{i+3}^{(i+1)} \| \ldots \| t_{n-3}^{(i+1)} \| t_{n-2}^{(i+1)} \| t_{n-1}^{(i+1)} \| t_{n}^{(i+1)} \| t_{n+1}^{(i+1)}].$$

Значення величини Δa_{i+2}, яке буде відніматись зі значення $a_{i+2}^{(i)}$, щоб отримати значення залишку $a_{i+2}^{(i+1)}$, визначається тільки значенням залишку $a_{i+1}^{(i)}$. Аналітично це визначається наступним співвідношенням

$$a_{i+2}^{(i+1)} = \left[a_{i+2}^{(i)} - \Delta a_{i+2} \right] \bmod m_{i+2}. \qquad (4.17)$$

У процесі вибірки $KH^{(i)}$ по значенню залишку $a_{i+1}^{(i)}$ числа $A^{(i)}$, цей же залишок одночасно буде переданий у обчислювальний тракт КСКОЦД по основі m_{i+2}. У цьому випадку з відповідних, заздалегідь складених двовходових таблиць $F\left\{a_{i+2}^{(i+1)}\right\} = \left[a_{i+1}^{(i)};\ a_{i+2}^{(i)} \right]$, по значеннях $a_{i+1}^{(i)}$ і $a_{i+2}^{(i)}$ вибирається значення $a_{i+2}^{(i+1)}$. Алгоритм виконання процедури ПН ВПЗ представлений у табл. 4.9. Число додавань для процедури ПН ВПЗ дорівнює n, оскільки нульвизація проводиться по усім n інформаційним основам СЗК. Проте після кожних двох додавань потрібен один додатковий такт для утворення чергової адреси і звернення у БН. У зв'язку з цим на кожні два такти віднімання доводиться один такт, вільний від операції віднімання з числа операцій вибірки чергової константи нульвизації. Таким чином, загальна кількість тактів, вільних від операції віднімання, під час яких робиться звернення у БКН КСКОЦД та утворення чергової адреси, визначається величиною $[n/2]$. Процедура ПН ВПЗ представлена на рис. 4.9.

Таблиця 4.9

Алгоритм виконання процедури ПН ВПЗ

№ оп.	Зміст операції	
1	Звернення по значенню залишку $a_1^{(0)}$ числа $A^{(0)}$ у $БКН_0$ за $КН^{(0)}$.	Утворення значення залишку $a_2^{(1)}$ числа $A^{(1)}$ у вигляді $a_2^{(1)} = t_2^{(1)} = \left[a_2^{(0)} - a_1^{(0)} \right] \bmod m_2$.
2	Виконання операції віднімання $A^{(1)} = A^{(0)} - КН^{(0)}$.	Звернення по значенню залишку $a_2^{(1)}$ числа $A^{(1)}$ у $БКН_1$ за $КН^{(1)}$.
3	Виконання операції віднімання $A^{(2)} = A^{(1)} - КН^{(1)}$.	Утворення значення залишку $a_3^{(2)}$ числа $A^{(2)}$ у вигляді $a_3^{(2)} = t_3^{(2)} = \left[a_3^{(1)} - a_2^{(1)} \right] \bmod m_3$.
4	Звернення по значенню залишку $a_3^{(2)}$ числа $A^{(2)}$ у $БКН_2$ за $КН^{(2)}$.	Утворення значення залишку $a_4^{(3)}$ числа $A^{(3)}$ у вигляді $a_4^{(3)} = t_4^{(3)} = \left[a_4^{(2)} - a_3^{(2)} \right] \bmod m_4$.
5	Виконання операції віднімання $A^{(3)} = A^{(2)} - КН^{(2)}$.	Звернення по значенню залишку $a_4^{(3)}$ числа $A^{(3)}$ у $БКН_3$ за $КН^{(3)}$.
6	Виконання операції віднімання $A^{(4)} = A^{(3)} - КН^{(3)}$.	Утворення значення залишку $a_5^{(4)}$ числа $A^{(4)}$ у вигляді $a_5^{(4)} = t_5^{(4)} = \left[a_5^{(3)} - a_4^{(3)} \right] \bmod m_5$.
⋮	…	…
i	Виконання операції віднімання $A^{(i)} = A^{(i-1)} - КН^{(i-1)}$.	Звернення по значеннях залишку $a_{i+1}^{(i)}$ числа $A^{(i)}$ у $БКН_i$ за $КН^{(i)}$.
$i+1$	Виконання операції віднімання $A^{(i+1)} = A^{(i)} - КН^{(i)}$.	Утворення значення залишку $a_{i+2}^{(i+1)}$ числа $A^{(i+1)}$ у вигляді $a_{i+2}^{(i+1)} = t_{i+2}^{(i+1)} = \left[a_{i+2}^{(i)} - a_{i+1}^{(i)} \right] \bmod m_{i+2}$.
$i+2$	Звернення по значенню залишку $a_{i+2}^{(i+1)}$ числа $A^{(i+1)}$ у $БКН_{i+1}$ за $КН^{(i+1)}$.	Утворення значення залишку $a_{i+3}^{(i+2)}$ числа $A^{(i+2)}$ у вигляді $a_{i+3}^{(i+2)} = t_{i+3}^{(i+2)} = \left[a_{i+3}^{(i+1)} - a_{i+2}^{(i+1)} \right] \bmod m_{i+3}$.
⋮	…	…
$k-2$	Звернення по значенню залишку $a_{n-1}^{(n-2)}$ числа $A^{(n-2)}$ у $БКН_{n-2}$ за $КН^{(n-2)}$.	Утворення значення залишку $a_n^{(n-1)}$ числа $A^{(n-1)}$ у вигляді $a_n^{(n-1)} = t_n^{(n-1)} = \left[a_n^{(n-2)} - a_{n-1}^{(n-2)} \right] \bmod m_n$.
$k-1$	Виконання операції віднімання $A^{(n-1)} = A^{(n-2)} - КН^{(n-2)}$.	Звернення по значенню залишку $a_n^{(n-1)}$ числа $A^{(n-1)}$ у $БКН_{n-1}$ за $КН^{(n-1)}$.
k	Виконання операції віднімання $A^{(n)} = A^{(n-1)} - КН^{(n-1)}$. Отримання нульовизованого $A^{(H)}$ числа $A^{(H)} = A^{(n)} = [0 \,\|\, 0 \,\|\, \ldots \,\|\, 0 \,\|\, \ldots \,\|\, 0 \,\|\, 0 \,\|\, (\gamma_{n+1} = a_{n+1}^{(n)})]$.	

№ операції (такту)	Зміст операцій	
1	Звернення по значенню залишку $a_1^{(0)}$ числа $A = A^{(0)} = [a_1^{(0)} \| a_2^{(0)} \| \| a_3^{(0)} \| \ldots \| a_{i-1}^{(0)} \| a_i^{(0)} \| a_{i+1}^{(0)} \| \ldots \| a_{n-3}^{(0)} \| \| a_{n-2}^{(0)} \| a_{n-1}^{(0)} \| a_n^{(0)} \| a_{n+1}^{(0)}]$ у $БКН_0$ за константою нульвизації $КН^{(0)} = = [t_1^{(0)} \| t_2^{(0)} \| t_3^{(0)} \| \ldots \| t_{i-1}^{(0)} \| t_i^{(0)} \| t_{i+1}^{(0)} \| \ldots \ldots \| t_{n-3}^{(0)} \| t_{n-2}^{(0)} \| t_{n-1}^{(0)} \| t_n^{(0)} \| t_{n+1}^{(0)}]$.	Утворення значення залишку $a_2^{(1)}$ числа $A^{(1)} = [0 \| a_2^{(1)} \| \| a_3^{(1)} \| \ldots \| a_{i-1}^{(1)} \| a_i^{(1)} \| a_{i+1}^{(1)} \| \ldots \ldots \| a_{n-3}^{(1)} \| a_{n-2}^{(1)} \| a_{n-1}^{(1)} \| a_n^{(1)} \| a_{n+1}^{(1)}]$ у вигляді $a_2^{(1)} = t_2^{(1)} = \left[a_2^{(0)} - a_1^{(0)}\right] \bmod m_2$.
2	Виконання операції віднімання $A^{(1)} = A^{(0)} - КН^{(0)} = [a_1^{(0)} \| a_2^{(0)} \| \| a_3^{(0)} \| \ldots \| a_{i-1}^{(0)} \| a_i^{(0)} \| a_{i+1}^{(0)} \| \ldots \ldots \| a_{n-3}^{(0)} \| a_{n-2}^{(0)} \| a_{n-1}^{(0)} \| a_n^{(0)} \| a_{n+1}^{(0)}] - -[t_1^{(0)} \| t_2^{(0)} \| t_3^{(0)} \| \ldots \| t_{i-1}^{(0)} \| t_i^{(0)} \| t_{i+1}^{(0)} \| \ldots \ldots \| t_{n-3}^{(0)} \| t_{n-2}^{(0)} \| t_{n-1}^{(0)} \| t_n^{(0)} \| t_{n+1}^{(0)}] = = \{[a_1^{(0)} - t_1^{(0)}] \bmod m_1 \| \| [a_2^{(0)} - t_2^{(0)}] \bmod m_2 \| \| [a_3^{(0)} - t_3^{(0)}] \bmod m_3 \| \ldots \ldots \| [a_{i-1}^{(0)} - t_{i-1}^{(0)}] \bmod m_{i-1} \| \| [a_i^{(0)} - t_i^{(0)}] \bmod m_i \| \| [a_{i+1}^{(0)} - t_{i+1}^{(0)}] \bmod m_{i+1} \| \ldots \ldots \| [a_{n-3}^{(0)} - t_{n-3}^{(0)}] \bmod m_{n-3} \| \| [a_{n-2}^{(0)} - t_{n-2}^{(0)}] \bmod m_{n-2} \| \| [a_{n-1}^{(0)} - t_{n-1}^{(0)}] \bmod m_{n-1} \| \| [a_n^{(0)} - t_n^{(0)}] \bmod m_n \| \| [a_{n+1}^{(0)} - t_{n+1}^{(0)}] \bmod m_{n+1}\} = [0 \| a_2^{(1)} \| \| a_3^{(1)} \| \ldots \| a_{i-1}^{(1)} \| a_i^{(1)} \| a_{i+1}^{(1)} \| \ldots \| a_{n-3}^{(1)} \| \| a_{n-2}^{(1)} \| a_{n-1}^{(1)} \| a_n^{(1)} \| a_{n+1}^{(1)}]$.	Звернення по значенню залишку $a_2^{(1)}$ числа $A^{(1)} = [0 \| \| a_2^{(1)} \| a_3^{(1)} \| \ldots \| a_{i-1}^{(1)} \| a_i^{(1)} \| \| a_{i+1}^{(1)} \| \ldots \| a_{n-3}^{(1)} \| a_{n-2}^{(1)} \| a_{n-1}^{(1)} \| \| a_n^{(1)} \| a_{n+1}^{(1)}]$ у $БКН_1$ за константою нульвизації $КН^{(1)} = [0 \| t_2^{(1)} \| t_3^{(1)} \| \ldots \| t_{i-1}^{(1)} \| \| t_i^{(1)} \| t_{i+1}^{(1)} \| \ldots \| t_{n-3}^{(1)} \| t_{n-2}^{(1)} \| t_{n-1}^{(1)} \| \| t_n^{(1)} \| t_{n+1}^{(1)}]$.

Рис. 4.9 – Метод ПН ВПЗ

3	Виконання операції віднімання $A^{(2)} = A^{(1)} - KH^{(1)} = [0 \| a_2^{(1)} \| a_3^{(1)} \| ...$ $... \| a_{i-1}^{(1)} \| a_i^{(1)} \| a_{i+1}^{(1)} \| ... \| a_{n-3}^{(1)} \| a_{n-2}^{(1)} \|$ $\| a_{n-1}^{(1)} \| a_n^{(1)} \| a_{n+1}^{(1)}] - [0 \| t_2^{(1)} \| t_3^{(1)} \| ...$ $... \| t_{i-1}^{(1)} \| t_i^{(1)} \| t_{i+1}^{(1)} \| \ldots \| t_{n-3}^{(1)} \| t_{n-2}^{(1)} \| t_{n-1}^{(1)} \|$ $\| t_n^{(1)} \| t_{n+1}^{(1)}] = \{0 \| [a_2^{(1)} - t_2^{(1)}] \bmod m_2 \|$ $\| [a_3^{(1)} - t_3^{(1)}] \bmod m_3 \| ...$ $... \| [a_{i-1}^{(1)} - t_{i-1}^{(1)}] \bmod m_{i-1} \|$ $\| [a_i^{(1)} - t_i^{(1)}] \bmod m_i \|$ $\| [a_{i+1}^{(1)} - t_{i+1}^{(1)}] \bmod m_{i+1} \| ...$ $... \| [a_{n-3}^{(1)} - t_{n-3}^{(1)}] \bmod m_{n-3} \|$ $\| [a_{n-2}^{(1)} - t_{n-2}^{(1)}] \bmod m_{n-2} \|$ $\| [a_{n-1}^{(1)} - t_{n-1}^{(1)}] \bmod m_{n-1} \|$ $\| [a_n^{(1)} - t_n^{(1)}] \bmod m_n \|$ $\| [a_{n+1}^{(1)} - t_{n+1}^{(1)}] \bmod m_{n+1} \} = [0 \| 0 \| a_3^{(2)} \| ...$ $... \| a_{i-1}^{(2)} \| a_i^{(2)} \| a_{i+1}^{(2)} \| \ldots \| a_{n-3}^{(2)} \| a_{n-2}^{(2)} \|$ $\| a_{n-1}^{(2)} \| a_n^{(2)} \| a_{n+1}^{(2)}]$.	Утворення значення залишку $a_3^{(2)}$ числа $A^{(2)} = [0 \| 0 \| a_3^{(2)} \| ...$ $... \| a_{i-1}^{(2)} \| a_i^{(2)} \| a_{i+1}^{(2)} \| \ldots \| a_{n-3}^{(2)} \|$ $\| a_{n-2}^{(2)} \| a_{n-1}^{(2)} \| a_n^{(2)} \| a_{n+1}^{(2)}]$ у вигляді $a_3^{(2)} = t_3^{(2)} = \left[a_3^{(1)} - a_2^{(1)} \right] \bmod m_3$.
4	Звернення по значенню залишку $a_3^{(2)}$ числа $A^{(2)} = [0 \| 0 \| a_3^{(2)} \| ...$ $... \| a_{i-1}^{(2)} \| a_i^{(2)} \| a_{i+1}^{(2)} \| ... \| a_{n-3}^{(2)} \| a_{n-2}^{(2)} \|$ $\| a_{n-1}^{(2)} \| a_n^{(2)} \| a_{n+1}^{(2)}]$ у $БКН_2$ за константою нульовизації $KH^{(2)}$.	Утворення значення залишку $a_4^{(3)}$ числа $A^{(3)} = [0 \| 0 \| 0 \| ...$ $... \| a_{i-1}^{(3)} \| a_i^{(3)} \| a_{i+1}^{(3)} \| ... \| a_{n-3}^{(3)} \|$ $\| a_{n-2}^{(3)} \| a_{n-1}^{(3)} \| a_n^{(3)} \| a_{n+1}^{(3)}]$ у вигляді $a_4^{(3)} = t_4^{(3)} = \left[a_4^{(2)} - a_3^{(2)} \right] \bmod m_4$.

Рис. 4.9, аркуш 2

5	Виконання операції віднімання $A^{(3)} = A^{(2)} - KH^{(2)} = [0 \| 0 \| a_3^{(2)} \| \dots$ $\dots \| a_{i-1}^{(2)} \| a_i^{(2)} \| a_{i+1}^{(2)} \| \dots \| a_{n-3}^{(2)} \| a_{n-2}^{(2)} \|$ $\| a_{n-1}^{(2)} \| a_n^{(2)} \| a_{n+1}^{(2)}] - [0 \| 0 \| t_3^{(2)} \| \dots$ $\dots \| t_{i-1}^{(2)} \| t_i^{(2)} \| t_{i+1}^{(2)} \| \dots \| t_{n-3}^{(2)} \| t_{n-2}^{(2)} \| t_{n-1}^{(2)} \|$ $\| t_n^{(2)} \| t_{n+1}^{(2)}] = \{0 \| 0 \|$ $\| [a_3^{(2)} - t_3^{(2)}] \bmod m_3 \| \dots$ $\dots \| [a_{i-1}^{(2)} - t_{i-1}^{(2)}] \bmod m_{i-1} \|$ $\| [a_i^{(2)} - t_i^{(2)}] \bmod m_i \|$ $\| [a_{i+1}^{(2)} - t_{i+1}^{(2)}] \bmod m_{i+1} \| \dots$ $\dots \| [a_{n-3}^{(2)} - t_{n-3}^{(2)}] \bmod m_{n-3} \|$ $\| [a_{n-2}^{(2)} - t_{n-2}^{(2)}] \bmod m_{n-2} \|$ $\| [a_{n-1}^{(2)} - t_{n-1}^{(2)}] \bmod m_{n-1} \|$ $\| [a_n^{(2)} - t_n^{(2)}] \bmod m_n \|$ $\| [a_{n+1}^{(2)} - t_{n+1}^{(2)}] \bmod m_{n+1}\} = [0 \| 0 \| 0 \|$ $\| a_4^{(3)} \| a_5^{(3)} \| \dots \| a_{i-1}^{(3)} \| a_i^{(3)} \| a_{i+1}^{(3)} \| \dots$ $\dots \| a_{n-3}^{(3)} \| a_{n-2}^{(3)} \| a_{n-1}^{(3)} \| a_n^{(3)} \| a_{n+1}^{(3)}]$.	Звернення по значенню залишку $a_4^{(3)}$ числа $A^{(3)} = [0 \|$ $\| 0 \| 0 \| \dots \| a_{i-1}^{(3)} \| a_i^{(3)} \| a_{i+1}^{(3)} \| \dots$ $\dots \| a_{n-3}^{(3)} \| a_{n-2}^{(3)} \| a_{n-1}^{(3)} \| a_n^{(3)} \| a_{n+1}^{(3)}]$ у $БКН_3$ за константою нульовизації $KH^{(3)} = [0 \| 0 \|$ $\| 0 \| \dots \| t_{i-1}^{(3)} \| t_i^{(3)} \| t_{i+1}^{(3)} \| \dots \| t_{n-3}^{(3)} \|$ $\| t_{n-2}^{(3)} \| t_{n-1}^{(3)} \| t_n^{(3)} \| t_{n+1}^{(3)}]$.

Рис. 4.9, аркуш 3

6	Виконання операції віднімання $A^{(4)} = A^{(3)} - KH^{(3)} = [0 \| 0 \| 0 \| \ldots$ $\ldots \| a_{i-1}^{(3)} \| a_i^{(3)} \| a_{i+1}^{(3)} \| \ldots \| a_{n-3}^{(3)} \| a_{n-2}^{(3)} \|$ $\| a_{n-1}^{(3)} \| a_n^{(3)} \| a_{n+1}^{(3)}] - [0 \| 0 \| 0 \| \ldots \| t_{i-1}^{(3)} \|$ $\| t_i^{(3)} \| t_{i+1}^{(3)} \| \ldots \| t_{n-3}^{(3)} \| t_{n-2}^{(3)} \| t_{n-1}^{(3)} \| t_n^{(3)} \|$ $\| t_{n+1}^{(3)}] = \{0 \| 0 \| 0 \| [a_4^{(3)} - t_4^{(3)}] \bmod m_4 \|$ $\| [a_5^{(3)} - t_5^{(3)}] \bmod m_5 \| \ldots$ $\ldots \| [a_{i-1}^{(3)} - t_{i-1}^{(3)}] \bmod m_{i-1} \|$ $\| [a_i^{(3)} - t_i^{(3)}] \bmod m_i \|$ $\| [a_{i+1}^{(3)} - t_{i+1}^{(3)}] \bmod m_{i+1} \| \ldots$ $\ldots \| [a_{n-3}^{(3)} - t_{n-3}^{(3)}] \bmod m_{n-3} \|$ $\| [a_{n-2}^{(3)} - t_{n-2}^{(3)}] \bmod m_{n-2} \|$ $\| [a_{n-1}^{(3)} - t_{n-1}^{(3)}] \bmod m_{n-1} \|$ $\| [a_n^{(3)} - t_n^{(3)}] \bmod m_n \|$ $\| [a_{n+1}^{(3)} - t_{n+1}^{(3)}] \bmod m_{n+1} \} = [0 \| 0 \| 0 \| 0 \|$ $\| a_5^{(4)} \| \ldots \| a_{i-1}^{(4)} \| a_i^{(4)} \| a_{i+1}^{(4)} \| \ldots \| a_{n-3}^{(4)} \|$ $\| a_{n-2}^{(4)} \| a_{n-1}^{(4)} \| a_n^{(4)} \| a_{n+1}^{(4)}]$.	Утворення значення залишку $a_5^{(4)}$ числа $A^{(4)} = [0 \| 0 \| 0 \| \ldots$ $\ldots \| a_{i-1}^{(4)} \| a_i^{(4)} \| a_{i+1}^{(4)} \| \ldots \| a_{n-3}^{(4)} \|$ $\| a_{n-2}^{(4)} \| a_{n-1}^{(4)} \| a_n^{(4)} \| a_{n+1}^{(4)}]$ у вигляді $a_5^{(4)} = t_5^{(4)} = \left[a_5^{(3)} - a_4^{(3)} \right] \bmod m_5$.
⋮	…	…

Рис. 4.9, аркуш 4

Для значення $A^{(i)}$	Виконання операції віднімання $A^{(i)} = A^{(i-1)} - KH^{(i-1)} = [0 \| 0 \| 0 \| \dots$ $\dots \| 0 \| a_i^{(i-1)} \| a_{i+1}^{(i-1)} \| \dots \| a_{n-3}^{(i-1)} \| a_{n-2}^{(i-1)} \|$ $\| a_{n-1}^{(i-1)} \| a_n^{(i-1)} \| a_{n+1}^{(i-1)}] - [0 \| 0 \| 0 \| \dots$ $\dots \| 0 \| t_i^{(i-1)} \| t_{i+1}^{(i-1)} \| \dots \| t_{n-3}^{(i-1)} \| t_{n-2}^{(i-1)} \|$ $\| t_{n-1}^{(i-1)} \| t_n^{(i-1)} \| t_{n+1}^{(i-1)}] = \{0 \| 0 \| 0 \| \dots \| 0 \|$ $\| [a_i^{(i-1)} - t_i^{(i-1)}] \bmod m_i \|$ $\| [a_{i+1}^{(i-1)} - t_{i+1}^{(i-1)}] \bmod m_{i+1} \| \dots$ $\dots \| [a_{n-3}^{(i-1)} - t_{n-3}^{(i-1)}] \bmod m_{n-3} \|$ $\| [a_{n-2}^{(i-1)} - t_{n-2}^{(i-1)}] \bmod m_{n-2} \|$ $\| [a_{n-1}^{(i-1)} - t_{n-1}^{(i-1)}] \bmod m_{n-1} \|$ $\| [a_n^{(i-1)} - t_n^{(i-1)}] \bmod m_n \|$ $\| [a_{n+1}^{(i-1)} - t_{n+1}^{(i-1)}] \bmod m_{n+1} \} = [0 \| 0 \| 0 \| \dots$ $\dots \| 0 \| 0 \| a_{i+1}^{(i)} \| \dots \| a_{n-3}^{(i)} \| a_{n-2}^{(i)} \| a_{n-1}^{(i)} \|$ $\| a_n^{(i)} \| a_{n+1}^{(i)}]$.	Звернення по значеннях залишку $a_{i+1}^{(i)}$ числа $A^{(i)} = [0 \| 0 \|$ $\| 0 \| \dots \| 0 \| 0 \| a_{i+1}^{(i)} \| \dots \| a_{n-3}^{(i)} \|$ $\| a_{n-2}^{(i)} \| a_{n-1}^{(i)} \| a_n^{(i)} \| a_{n+1}^{(i)}]$ у $БКН_i$ за константою нульовизації $KH^{(i)} = [0 \| 0 \| 0 \| \dots \| 0 \| 0 \|$ $\| t_{i+1}^{(i)} \| \dots \| t_{n-3}^{(i)} \| t_{n-2}^{(i)} \| t_{n-1}^{(i)} \| t_n^{(i)} \|$ $\| t_{n+1}^{(i)}]$.
Для значення $A^{(i+1)}$	Виконання операції віднімання $A^{(i+1)} = A^{(i)} - KH^{(i)} = [0 \| 0 \| 0 \| \dots \| 0 \|$ $\| 0 \| a_{i+1}^{(i)} \| \dots \| a_{n-3}^{(i)} \| a_{n-2}^{(i)} \| a_{n-1}^{(i)} \| a_n^{(i)} \|$ $\| a_{n+1}^{(i)}] - [0 \| 0 \| 0 \| \dots \| 0 \| 0 \| t_{i+1}^{(i)} \| \dots$ $\dots \| t_{n-3}^{(i)} \| t_{n-2}^{(i)} \| t_{n-1}^{(i)} \| t_n^{(i)} \| t_{n+1}^{(i)}]$.	Утворення значення залишку $a_{i+2}^{(i+1)}$ числа $A^{(i+1)} = [0 \| 0 \| 0 \| \dots \| 0 \| 0 \|$ $\| 0 \| \dots \| a_{n-3}^{(i+1)} \| a_{n-2}^{(i+1)} \| a_{n-1}^{(i+1)} \|$ $\| a_n^{(i+1)} \| a_{n+1}^{(i+1)}]$ у вигляді $a_{i+2}^{(i+1)} =$ $= t_{i+2}^{(i+1)} = [a_{i+2}^{(i)} - a_{i+1}^{(i)}] \bmod m_{i+2}$
	Звернення по значенню залишку $a_{i+2}^{(i+1)}$ числа $A^{(i+1)} = [0 \| 0 \| 0 \| \dots \| 0 \|$ $\| 0 \| 0 \| \dots \| a_{n-3}^{(i+1)} \| a_{n-2}^{(i+1)} \| a_{n-1}^{(i+1)} \| a_n^{(i+1)} \|$ $\| a_{n+1}^{(i+1)}]$ у $БКН_{i+1}$ за константою нульовизації $KH^{(i+1)} = [0 \| 0 \| 0 \| \dots$ $\dots \| 0 \| 0 \| 0 \| \dots \| t_{n-3}^{(i+1)} \| t_{n-2}^{(i+1)} \| t_{n-1}^{(i+1)} \|$ $\| t_n^{(i+1)} \| t_{n+1}^{(i+1)}]$.	Утворення значення залишку $a_{i+3}^{(i+2)}$ числа $A^{(i+2)} = [0 \| 0 \| 0 \| \dots$ $\dots \| 0 \| 0 \| 0 \| \dots \| a_{n-3}^{(i+2)} \| a_{n-2}^{(i+2)} \|$ $\| a_{n-1}^{(i+2)} \| a_n^{(i+2)} \| a_{n+1}^{(i+2)}]$ у вигляді $a_{i+3}^{(i+2)} = t_{i+3}^{(i+2)} =$ $= [a_{i+3}^{(i+1)} - a_{i+2}^{(i+1)}] \bmod m_{i+3}$.
⋮	…	…

Рис. 4.9, аркуш 5

$k-2$	Звернення по значенню залишку $a_{n-1}^{(n-2)}$ числа $A^{(n-2)}=[0\|\|0\|\|0\|\|\dots$ $\dots\|\|0\|\|0\|\|0\|\|\dots\|\|0\|\|0\|\|a_{n-1}^{(n-2)}\|\|a_n^{(n-2)}\|$ $\|\|a_{n+1}^{(n-2)}]$ у $БКН_{n-2}$ за константою нульовизації $КН^{(n-2)}=[0\|\|0\|\|0\|\|\dots$ $\dots\|\|0\|\|0\|\|0\|\|\dots\|\|0\|\|0\|\|t_{n-1}^{(n-2)}\|$ $\|t_n^{(n-2)}\|t_{n+1}^{(n-2)}]$.	Утворення значення залишку $a_n^{(n-1)}$ числа $A^{(n-1)}=[0\|\|0\|\|0\|\|\dots$ $\dots\|\|0\|\|0\|\|0\|\|\dots\|\|0\|\|0\|\|0\|\|a_n^{(n-1)}\|$ $\|a_{n+1}^{(n-1)}]$ у вигляді $a_n^{(n-1)}=t_n^{(n-1)}=$ $=\left[a_n^{(n-2)}-a_{n-1}^{(n-2)}\right]\bmod m_n$.
$k-1$	Виконання операції віднімання $A^{(n-1)}=A^{(n-2)}-КН^{(n-2)}=[0\|\|0\|\|0\|\|\dots$ $\dots\|\|0\|\|0\|\|0\|\|\dots\|\|0\|\|0\|\|a_{n-1}^{(n-2)}\|\|a_n^{(n-2)}\|$ $\|a_{n+1}^{(n-2)}]-[0\|\|0\|\|0\|\|\dots\|\|0\|\|0\|\|0\|\|\dots$ $\dots\|\|0\|\|0\|\|t_{n-1}^{(n-2)}\|\|t_n^{(n-2)}\|\|t_{n+1}^{(n-2)}]$.	Звернення по значенню залишку $a_n^{(n-1)}$ числа $A^{(n-1)}=$ $=[0\|\|0\|\|0\|\|\dots\|\|0\|\|0\|\|0\|\|\dots$ $\dots\|\|0\|\|0\|\|0\|\|a_n^{(n-1)}\|\|a_{n+1}^{(n-1)}]$ у $БКН_{n-1}$ за константою нульовизації $КН^{(n-1)}$.
k	Виконання операції віднімання $A^{(n)}=A^{(n-1)}-КН^{(n-1)}=[0\|\|0\|\|0\|\|\dots$ $\dots\|\|0\|\|0\|\|0\|\|\dots\|\|0\|\|0\|\|0\|\|a_n^{(n-1)}\|\|a_{n+1}^{(n-1)}]-[0\|\|0\|\|0\|\|\dots\|\|0\|\|0\|\|0\|\|\dots$ $\dots\|\|0\|\|0\|\|0\|\|0\|\|t_{n+1}^{(n-1)}]$. Отримання нульовизованого $A^{(H)}$ числа $A^{(H)}=A^{(n)}=[0\|\|0\|\|\dots\|\|0\|\|\dots\|\|0\|\|0\|\|\gamma_{n+1}=a_{n+1}^{(n)}]$.	
$T_{H2}=\left(\left[\frac{n-1}{2}\right]+n\right)\cdot\tau_{сл}$.		

Рис. 4.9, аркуш 6

Час T_{H2} виконання процедури нульовизації ПН ВПЗ визначається значенням (4.18)

$$T_{H2}=\left(\left[\frac{n-1}{2}\right]+n\right)\cdot\tau_{сл} \qquad (4.18)$$

Для реалізації процедури нульовизації розглянутим методом у БКН

необхідно мати $K_{H2}=\sum_{i=1}^{n-1}(m_i-1)$ констант нульвизації. При цьому кількість N_{H2} двійкових розрядів БКН КСКОЦД визначається виразом

$$N_{H2}=\sum_{i=1}^{n-1}(m_i-1)\cdot(n-i).$$

4.4.4 Метод контролю даних у СЗК з попереднім аналізом подальших симетричних залишків контрольованого числа, що заснований на принципі паралельної нульвизації

Істотним недоліком, розглянутих у попередніх розділах методів (*Н*1-*Н*3) контролю даних у СЗК, є необхідність значних часових витрат на контроль, що обумовлює низьку оперативність контролю і значні непродуктивні обчислювальні витрати [130-132].

З метою підвищення оперативності контролю даних, за рахунок зменшення часу реалізації процедури нульвизації, проведемо розробку методу контролю даних у СЗК – метод паралельної нульвизації з визначенням подальших залишків (*Н*4) (ПНН ВПЗ). Цей метод контролю ґрунтується на процедурі використання парної нульвизації чисел з додатковою операцією попередньої вибірки залишків (див. метод (*Н*2)). Суть методу контролю полягає у тому, що попередня вибірка проводиться одночасно по двох залишках $a_{i+1}^{(i)}$ та $a_{n-i}^{(i)}$ числа $A^{(i)}=[\overbrace{0\|0\|\ldots\|0}^{i-\text{нулів}}\|a_{i+1}^{(i)}\|a_{i+2}^{(i)}\|\ldots\|a_{n-i-1}^{(i)}\|a_{n-i}^{(i)}\|\overbrace{0\|\ldots\|0\|0}^{i-\text{нулів}}\|a_{n+1}^{(i)}]$. Таким чином, при реалізації процедури нульвизації поєднуються у часі операція вибору, по залишках $a_{i+1}^{(i)}$ і $a_{n-i}^{(i)}$ числа

$$A^{(i)}=[0\|0\|\ldots\|0\|a_{i+1}^{(i)}\|a_{i+2}^{(i)}\|a_{i+3}^{(i)}\|\ldots\|a_{n-i-2}^{(i)}\|a_{n-i-1}^{(i)}\|a_{n-i}^{(i)}\|0\|\ldots\|0\|a_{n+1}^{(i)}]$$

константи нульовизації

$$KH^{(i)} = [0 \| 0 \| \ldots \| 0 \| t_{i+1}^{(i)} \| t_{i+2}^{(i)} \| t_{i+3}^{(i)} \| \ldots \| t_{n-i-2}^{(i)} \| t_{n-i-1}^{(i)} \| t_{n-1}^{(i)} \| 0 \| \ldots \| 0 \| t_{n+1}^{(i)}]$$

і операція визначення, по значеннях залишків $a_{i+1}^{(i)}$ та $a_{n-i}^{(i)}$, подальших значень залишків $a_{i+2}^{(i+1)}$ та $a_{n-i-1}^{(i+1)}$ числа

$$A^{(i+1)} = [0 \| 0 \| \ldots \| 0 \| 0 \| a_{i+2}^{(i+1)} \| a_{i+3}^{(i+1)} \| \ldots \| a_{n-i-2}^{(i+1)} \| a_{n-i-1}^{(i+1)} \| 0 \| 0 \| \ldots \| 0 \| 0 \| a_{n+1}^{(i+1)}].$$

Також поєднуються у часі операція віднімання $A^{(i+1)} = A^{(i)} - KH^{(i)}$ та операція вибору чергової константи нульовизації $KH^{(i+1)} = [0 \| 0 \| 0 \| \ldots \| 0 \| 0 \| \| t_{i+2}^{(i+1)} \| \ldots \| t_{n-i-2}^{(i+1)} \| t_{n-i-1}^{(i+1)} \| 0 \| 0 \| t_{n+1}^{(i+1)}]$. Алгоритм нульовизації представлений у табл. 4.10. Значення величин Δa_{i+2} та Δa_{n-i-1}, які будуть відніматись з відповідних значень $a_{i+2}^{(i)}$ та $a_{n-i-1}^{(i)}$, щоб отримати значення залишків, $a_{i+2}^{(i+1)}$ та $a_{n-i-1}^{(i+1)}$, визначаються тільки значеннями відповідних залишків числа $a_{i+1}^{(i)}$ та $a_{n-i}^{(i)}$. Аналітично це можна представити у вигляді наступних двох виразів

$$a_{i+2}^{(i+1)} = [a_{i+2}^{(i)} - \Delta a_{i+2}] \bmod m_{i+2} \quad \text{та} \quad a_{n-i-1}^{(i+1)} = [a_{n-i-1}^{(i)} - \Delta a_{n-i-1}] \bmod m_{n-i-1}.$$

У процесі вибірки $KH^{(i)}$ по значеннях залишків $a_{i+1}^{(i)}$ та $a_{n-i}^{(i)}$ числа $A^{(i)}$, ці залишки будуть передані в обчислювач по відповідним основам m_{i+2} та m_{n-i-1}. З двовхідних таблиць $F_1\left\{a_{i+2}^{(i+1)}\right\} = \left[a_{i+1}^{(i)};\ a_{i+2}^{(i)}\right]$ та $F_2\left\{a_{n-i-1}^{(i+1)}\right\} = \left[a_{n-1}^{(i)};\ a_{n-i-1}^{(i)}\right]$ вибираються (визначаються) значення $a_{i+2}^{(i+1)}$ та $a_{n-i-1}^{(i+1)}$. У цьому випадку загальна кількість тактів, що вільні від додавання, під час яких робитися звернення у БКН та утворення чергової адреси дорівнює значенню $[(n+1)/2]$, (де [X] – ціле, найбільш найближче до X число, але таке, що

його не перевершує). При цьому нульовизація проводиться одночасно по двох інформаційних основах СЗК a_1, a_n; a_2, a_{n-1} і так далі. Після кожних двох операцій віднімання потрібно ще один додатковий часовий такт для утворення чергової адреси і звернення до накопичувача констант нульовизації. У зв'язку з цим на кожні два такти додавання ($\tau_{сл} = \tau_0$) доводиться один такт вільний від операції додавання.

На основі вищевикладеного час виконання операції нульовизації для розглянутого методу оперативного контролю ($H4$) визначиться таким чином

$$T_{H4} = \left[\frac{n+1}{2}\right] \cdot \tau_{дод.} + \left[\frac{\frac{n+1}{2}+1}{2}\right] \cdot \tau_{виб}. \qquad (4.19)$$

Враховуючи, що $\tau_{сл} = \tau_{виб}$ отримаємо:

$$T_{H4} = \left(\left[\frac{n+1}{2}\right] + \left[\frac{\frac{n+1}{2}+1}{2}\right]\right) \cdot \tau_{дод.} \qquad (4.20)$$

При n – парному, вираз (4.20) набуває вигляду:

$$T'_{H4} = \left(\frac{n}{2} + \left[\frac{\frac{n}{2}+1}{2}\right]\right) \cdot \tau_{дод.} \qquad (4.21)$$

Таблиця 4.10

Алгоритм ПНН ВПЗ

№ оп.	Зміст операції	
1	Звернення по значеннях залишків $a_1^{(0)}$ та $a_n^{(0)}$ числа $A^{(0)}$ у $БКН_0$ за $КН^{(0)}$.	Утворення значень залишків $a_2^{(1)}$ та $a_{n-1}^{(1)}$ числа $A^{(1)}$ у вигляді $a_2^{(1)} = t_2^{(1)} = \left[a_2^{(0)} - a_1^{(0)} \right] \bmod m_2$ та $a_{n-1}^{(1)} = t_{n-1}^{(1)} = \left[a_{n-1}^{(0)} - a_n^{(0)} \right] \bmod m_{n-1}$.
2	Виконання операції віднімання $A^{(1)} = A^{(0)} - KH^{(0)}$.	Звернення по значеннях залишків $a_2^{(1)}$ та $a_{n-1}^{(1)}$ числа $A^{(1)}$ у $БКН_1$ за $КН^{(1)}$.
3	Виконання операції віднімання $A^{(2)} = A^{(1)} - KH^{(1)}$.	Утворення значень залишків $a_3^{(2)}$ та $a_{n-2}^{(2)}$ числа $A^{(2)}$ у вигляді $a_3^{(2)} = t_3^{(2)} = \left[a_3^{(1)} - a_2^{(1)} \right] \bmod m_3$ та $a_{n-2}^{(2)} = t_{n-2}^{(2)} = \left[a_{n-2}^{(1)} - a_{n-1}^{(1)} \right] \bmod m_{n-2}$.
⋮	…	…
i	Виконання операції віднімання $A^{(i)} = A^{(i-1)} - KH^{(i-1)}$.	Звернення по значеннях залишків $a_{i+1}^{(i)}$ та $a_{n-i}^{(i)}$ числа $A^{(i)}$ у $БКН_i$ за $КН^{(i)}$.
$i+1$	Виконання операції віднімання $A^{(i+1)} = A^{(i)} - KH^{(i)}$.	Утворення значень залишків $a_{i+2}^{(i+1)}$ та $a_{n-i-1}^{(i+1)}$ числа $A^{(i+1)}$ у вигляді $a_{i+2}^{(i+1)} = t_{i+2}^{(i+1)} = \left[a_{i+2}^{(i)} - a_{i+1}^{(i)} \right] \bmod m_{i+2}$ та $a_{n-i-1}^{(i+1)} = t_{n-i-1}^{(i+1)} = \left[a_{n-i-1}^{(i)} - a_{n-i-2}^{(i)} \right] \bmod m_{n-i-1}$.
$i+2$	Звернення по значеннях залишків $a_{i+2}^{(i+1)}$ та $a_{n-i-1}^{(i+1)}$ числа $A^{(i+1)}$ у $БКН_{i+1}$ за $КН^{(i+1)}$.	Утворення значень залишків $a_{i+3}^{(i+2)}$ та $a_{n-i-2}^{(i+2)}$ числа $A^{(i+2)}$ у вигляді $a_{i+3}^{(i+2)} = t_{i+2}^{(i+2)} = \left[a_{i+3}^{(i+1)} - a_{i+2}^{(i+1)} \right] \bmod m_{i+3}$ та $a_{n-i-2}^{(i+2)} = t_{n-i-2}^{(i+2)} = \left[a_{n-i-2}^{(i+1)} - a_{n-i-3}^{(i+1)} \right] \bmod m_{n-i-2}$.
⋮	…	…
$k-2$	Звернення по значеннях залишків $a_{n/2-1}^{(n/2-2)}$ та $a_{n/2+2}^{(n/2-2)}$ числа $A^{(n/2-2)}$ у $БКН_{n/2-2}$ за $КН^{(n/2-2)}$.	Утворення значень залишків $a_{n/2}^{(n/2-1)}$ та $a_{n/2+1}^{(n/2-1)}$ числа $A^{(n/2-1)}$ у вигляді $a_{n/2}^{(n/2-1)} = t_{n/2}^{(n/2-1)} = \left[a_{n/2}^{(n/2-2)} - a_{n/2-1}^{(n/2-2)} \right] \bmod m_{n/2}$ та $a_{n/2+1}^{(n/2-1)} = t_{n/2+1}^{(n/2-1)} = \left[a_{n/2+1}^{(n/2-2)} - a_{n/2}^{(n/2-2)} \right] \bmod m_{n/2+1}$.
$k-1$	Виконання операції віднімання $A^{(n/2-1)} = A^{(n/2-2)} - KH^{(n/2-2)}$.	Звернення по значеннях залишків $a_{n/2}^{(n/2-1)}$ та $a_{n/2+1}^{(n/2-1)}$ числа $A^{(n/2-1)}$ у $БКН_{n/2-1}$ за $КН^{(n/2-1)}$.
k	Виконання операції віднімання $A^{(n/2)} = A^{(n/2-1)} - KH^{(n/2-1)}$. Отримання нульовизованого числа $A^{(H)} = A^{(n/2)} = [0 \,\|\, 0 \,\|\, \ldots \,\|\, 0 \,\|\, \ldots \,\|\, 0 \,\|\, 0 \,\|\, \gamma_{n+1} = a_{n+1}^{(n/2)}]$.	

Якщо $\frac{n}{2}$ – парне, то

$$T'_{H4} = \frac{3}{4} n \cdot \tau_{дод.}. \tag{4.22}$$

Якщо $\frac{n}{2}$ - непарне, то

$$T'_{H4} = \left(\frac{3n+2}{4} \right) \cdot \tau_{дод.}. \tag{4.23}$$

При n непарному:

$$T''_{H4} = \left(\frac{n+1}{2} + \left[\frac{\frac{n+1}{2}+1}{2} \right] \right) \cdot \tau_{дод.}. \tag{4.24}$$

Якщо $\frac{n+1}{2}$ парне, то

$$T''_{H4} = \frac{3}{4} (n+1) \cdot \tau_{дод.}. \tag{4.25}$$

Якщо $\frac{n+1}{2}$ непарне, то

$$T''_{H4} = \left(\frac{3n+5}{4} \right) \cdot \tau_{дод.}. \qquad (4.26)$$

Доказ виведеного співвідношення (4.20) зручно провести методом математичної індукції по n.

Перший етап доказу. Для мінімального значення n = 3 час нульовизації дорівнює $T_{H4} = 3 \cdot \tau_{дод.}$. Це очевидно з рис. 4.10, діаграма (H4) (ПНН ВПЗ).

Другий етап. Припустимо, що вираз (4.20) правдивий і при $n = K$ тобто

$$T_{H4} = \left(\left[\frac{K+1}{2} \right] + \left[\frac{\left[\frac{K-1}{2} \right] + 1}{2} \right] \right) \cdot \tau_{дод.}.$$

Третій етап. Доведемо, що вираз (4.19) правдивий і при $n = K+1$, тобто

$$T_{H4} = \left(\left[\frac{K+2}{2} \right] + \left[\frac{\left[\frac{K+2}{2} + 1 \right]}{2} \right] \right) \cdot \tau_{дод.}.$$

При K – парному (K+1 – непарне) маємо:

$$T'_{H4} = \left(\frac{K}{2} + 1 + \left[\frac{\frac{K}{2} + 2}{2} \right] \right) \cdot \tau_{дод.}.$$

Якщо $\frac{K}{2}$ парне, то $T'_{H4}=\left(\frac{3K+8}{4}\right)\cdot\tau_{\partial o\partial.}$. Якщо $\frac{K}{2}$ - непарне, то $T'_{H4}=\left(\frac{3K+6}{4}\right)\cdot\tau_{\partial o\partial.}$.

При K непарному (K+1 – парне), маємо:

$$T''_{H4}=\left(\frac{K+1}{2}+\left[\frac{\left[\frac{K+1}{2}\right]+1}{2}\right]\right)\cdot\tau_{\partial o\partial.}.$$

Якщо $\frac{K+1}{2}$ – парне, то $T''_{H4}=\left(\frac{3K+3}{4}\right)\cdot\tau_{\partial o\partial.}$; якщо $\frac{K+1}{2}$ – непарне, то $T''_{H4}=\left(\frac{3K+5}{4}\right)\cdot\tau_{\partial o\partial.}$. Тоді відповідно до виразів (4.22), (4.23), (4.24) і (4.26) запишемо, що:

$$\frac{3K+3}{4}\cdot\tau_{\partial o\partial.}=\frac{3}{4}(K+1)\cdot\tau_{\partial o\partial.},$$

$$\frac{3K+5}{4}\cdot\tau_{\partial o\partial.}=\left\{\frac{3(K+1)+2}{4}\right\}\cdot\tau_{\partial o\partial.},$$

$$\frac{3K+6}{4}\cdot\tau_{\partial o\partial.}=\frac{3}{4}\{(K+1)+1\}\cdot\tau_{\partial o\partial.},$$

$$\frac{3K+8}{4}\cdot\tau_{\partial o\partial.}=\left\{\frac{3(K+1)+5}{4}\right\}\cdot\tau_{\partial o\partial.}.$$

Таким чином, вираз (4.20) правдивий і при $n = K + 1$, що і вимагалося довести. У практичних розрахунках, для визначення часу контролю даних у СЗК рекомендується користуватись виразами (4.22), (4.23), (4.25) і (4.26).

На рис. 4.10 приведені часові діаграми роботи БН для МПН (діаграма (*H*1)), для методу ПН ВПЗ (діаграма (Н2)), а також для першого ПНН (діаграма (Н3)) і другого ПНН ВПЗ (діаграма (Н4)) методів контролю, розглянутих вище.

Де: Зв. $a_i^{(i-1)}$, $a_{n-i+1}^{(i-1)}$ – звернення по значенням цифр $a_i^{(i-1)}$ та $a_{n-i+1}^{(i-1)}$ числа $A^{(i-1)} = (0 \| ... \| 0 \| a_i^{(i-1)} \| a_{i+1}^{(i-1)} \| ... \| a_{n-i}^{(i-1)} \| a_{n-i+1}^{(i-1)} \| 0 \| ... \| 0 \| a_{n+1}^{(i-1)})$ у БКН за константою нульовизації виду $KH^{(i)} = (0 \| ... \| 0 \| t_{i,i} \| t_{i+1,i} \| ... \| t_{n-i,i} \| t_{n-i+1,i} \| \| 0 \| ... \| 0 \| t_{n+1,i})$;

$a_{i+1}^{(i+1)}$, $a_{n-i}^{(i+1)}$ – створення по значеннях $a_i^{(i)}$ та $a_{n-i+1}^{(i)}$ числа $A^{(i-1)}$ наступних цифр $a_{i+1}^{(i)}$ та $a_{n-1}^{(i)}$ для числа $A^{(i)} = (0 \| ... \| 0 \| a_{i+1}^{(i)} \| ... \| a_{n-1}^{(i)} \| 0 \| ... \| 0 \| a_{n+1}^{(i)})$;

$\sum i$ – операція віднімання значення константи $KH^{(i-1)}$ з числа $A^{(i-1)}$, тобто проведення операції $A^{(i-1)} - KH^{(i-1)}$.

При реалізації процедури нульовизації для методу Н4 у БКН необхідно мати констант нульовизації згідно з виразом:

$$K_{H4} = \sum_{i=1}^{\left\lceil \frac{n}{2} \right\rceil} (m_i \cdot m_{n-i+1} - 2).$$

При цьому кількість N_{H3} двійкових розрядів констант нульовизації визначається виразом

$$K_{H4} = \sum_{i=1}^{\left\lceil \frac{n}{2} \right\rceil} (m_i \cdot m_{n-i+1} - 2) \cdot (n - 2i + 1).$$

Н1	Зв. a_1	Σ1	Зв. $a_2^{(1)}$	Σ2	Зв. $a_3^{(2)}$	Σ3	Зв. $a_4^{(3)}$	Σ4	…
Н3	Зв. a_1, a_n	Σ1	Зв. $a_2^{(1)}$, $a_{n-1}^{(1)}$	Σ2	Зв. $a_3^{(2)}$, $a_{n-2}^{(2)}$	Σ3	Зв. $a_4^{(3)}$, $a_{n-3}^{(3)}$	Σ4	…
Н2	Зв. a_1	Σ1	Σ2	Зв. $a_3^{(2)}$	Σ3	Σ4	Зв. $a_5^{(4)}$	Σ5	…
	$a_2^{(1)}$	Зв. $a_2^{(1)}$	$a_3^{(2)}$	$a_4^{(3)}$	Зв. $a_4^{(3)}$	$a_5^{(4)}$	$a_6^{(5)}$	Зв. $a_6^{(5)}$	
Н4	Зв. a_1, a_n	Σ1	Σ2	Зв. $a_3^{(2)}$, $a_{n-2}^{(2)}$	Σ3	Σ4	Зв. $a_5^{(4)}$, $a_{n-4}^{(4)}$	Σ5	…
	$a_2^{(1)}$, $a_{n-1}^{(1)}$	Зв. $a_2^{(1)}$, $a_{n-1}^{(1)}$	$a_3^{(2)}$, $a_{n-2}^{(2)}$	$a_4^{(3)}$, $a_{n-3}^{(3)}$	Зв. $a_4^{(3)}$, $a_{n-3}^{(3)}$	$a_5^{(4)}$, $a_{n-4}^{(4)}$	$a_6^{(5)}$, $a_{n-5}^{(5)}$	Зв. $a_6^{(5)}$, $a_{n-5}^{(5)}$	…
0	1	2	3	4	5	6	7	8	9 $T_{Hi}/\tau_{сл}$

Рис. 4.10 – Часові діаграми роботи блок нульвизації при різних методах нульовизації

Метод контролю даних ПНН ВПЗ представлений на рис. 4.11.

Проведемо розрахунок і порівняльний аналіз основних характеристик методів контролю даних у СЗК.

При виборі методу контролю даних у СЗК необхідно враховувати кількісні значення показника (характеристик), що характеризують цей метод. Виведені вирази є робочими формулами для оцінки швидкодії реалізації процедури нульовизації залежно від величин значень n і $\tau_{сл}$.

Узагальнені основні характеристики усіх чотирьох методів контролю даних представлені у табл. 4.11. На основі даних табл. 4.12, у табл. 4.13 представлені результати розрахунку характеристик розглянутих методів контролю для l–байтових ($l = \overline{1 \div 8}$) розрядних сіток обчислювача у СЗК.

№ Опе-рації (такту)	Зміст операції	
1	Звернення по значеннях залишків $a_1^{(0)}$ та $a_n^{(0)}$ числа $A = A^{(0)} = [a_1^{(0)} \| a_2^{(0)} \| \| a_3^{(0)} \| \ldots \| a_{i-1}^{(0)} \| a_i^{(0)} \| a_{i+1}^{(0)} \| \ldots \| a_{n-3}^{(0)} \| \| a_{n-2}^{(0)} \| a_{n-1}^{(0)} \| a_n^{(0)} \| a_{n+1}^{(0)}]$ у $БКН_0$ за константою нульвизації $KH^{(0)} = [t_1^{(0)} \| \| t_2^{(0)} \| t_3^{(0)} \| \ldots \| t_{i-1}^{(0)} \| t_i^{(0)} \| t_{i+1}^{(0)} \| \ldots \| t_{n-3}^{(0)} \| \| t_{n-2}^{(0)} \| t_{n-1}^{(0)} \| t_n^{(0)} \| t_{n+1}^{(0)}]$; $t_1^{(0)} = a_1^{(0)}$, $t_n^{(0)} = a_n^{(0)}$; $t_1^{(0)} = \overline{0, m_1 - 1}$, $t_n^{(0)} = \overline{0, m_n - 1}$.	Утворення значень залишків $a_2^{(1)}$ і $a_{n-1}^{(1)}$ числа $A^{(1)} = [0 \| a_2^{(1)} \| a_3^{(1)} \| \ldots \| a_{i-1}^{(1)} \| \| a_i^{(1)} \| a_{i+1}^{(1)} \| \ldots \| a_{n-3}^{(1)} \| a_{n-2}^{(1)} \| \| a_{n-1}^{(1)} \| 0 \| a_{n+1}^{(1)}]$ у вигляді $a_2^{(1)} = t_2^{(1)} = \left[a_2^{(0)} - a_1^{(0)} \right] \bmod m_2$ і $a_{n-1}^{(1)} = t_{n-1}^{(1)} = \left[a_{n-1}^{(0)} - a_n^{(0)} \right] \bmod m_{n-1}$.
2	Виконання операції віднімання $A^{(1)} = A^{(0)} - KH^{(0)} = [a_1^{(0)} \| a_2^{(0)} \| a_3^{(0)} \| \ldots \ldots \| a_{i-1}^{(0)} \| a_i^{(0)} \| a_{i+1}^{(0)} \| \ldots \| a_{n-3}^{(0)} \| a_{n-2}^{(0)} \| a_{n-1}^{(0)} \| \| a_n^{(0)} \| a_{n+1}^{(0)}] - [t_1^{(0)} \| t_2^{(0)} \| t_3^{(0)} \| \ldots \| t_{i-1}^{(0)} \| \| t_i^{(0)} \| t_{i+1}^{(0)} \| \ldots \| t_{n-3}^{(0)} \| t_{n-2}^{(0)} \| t_{n-1}^{(0)} \| t_n^{(0)} \| t_{n+1}^{(0)}] = \{ [a_1^{(0)} - t_1^{(0)}] \bmod m_1 \| \| [a_2^{(0)} - t_2^{(0)}] \bmod m_2 \| \| [a_3^{(0)} - t_3^{(0)}] \bmod m_3 \| \ldots \ldots \| [a_{i-1}^{(0)} - t_{i-1}^{(0)}] \bmod m_{i-1} \| \| [a_i^{(0)} - t_i^{(0)}] \bmod m_i \| \| [a_{i+1}^{(0)} - t_{i+1}^{(0)}] \bmod m_{i+1} \| \ldots \ldots \| [a_{n-3}^{(0)} - t_{n-3}^{(0)}] \bmod m_{n-3} \| \| [a_{n-2}^{(0)} - t_{n-2}^{(0)}] \bmod m_{n-2} \| \| [a_{n-1}^{(0)} - t_{n-1}^{(0)}] \bmod m_{n-1} \| \| [a_n^{(0)} - t_n^{(0)}] \bmod m_n \| \| [a_{n+1}^{(0)} - t_{n+1}^{(0)}] \bmod m_{n+1} \} = [0 \| a_2^{(1)} \| a_3^{(1)} \| \ldots \ldots \| a_{i-1}^{(1)} \| a_i^{(1)} \| a_{i+1}^{(1)} \| \ldots \ldots \| a_{n-3}^{(1)} \| a_{n-2}^{(1)} \| a_{n-1}^{(1)} \| 0 \| a_{n+1}^{(1)}]$.	Звернення по значеннях залишків $a_2^{(1)}$ та $a_{n-1}^{(1)}$ числа $A^{(1)} = [0 \| a_2^{(1)} \| a_3^{(1)} \| \ldots \| a_{i-1}^{(1)} \| \| a_i^{(1)} \| a_{i+1}^{(1)} \| \ldots \| a_{n-3}^{(1)} \| a_{n-2}^{(1)} \| \| a_{n-1}^{(1)} \| 0 \| a_{n+1}^{(1)}]$ у $БКН_1$ за константою нульвизації $KH^{(1)} = [0 \| t_2^{(1)} \| t_3^{(1)} \| \ldots \| t_{i-1}^{(1)} \| \| t_i^{(1)} \| t_{i+1}^{(1)} \| \ldots \| t_{n-3}^{(1)} \| t_{n-2}^{(1)} \| t_{n-1}^{(1)} \| 0 \| t_{n+1}^{(1)}]$; $t_2^{(1)} = a_2^{(1)}$, $t_{n-1}^{(1)} = a_{n-1}^{(1)}$; $t_2^{(1)} = \overline{0, m_2 - 1}$, $t_{n-1}^{(1)} = \overline{0, m_{n-1} - 1}$.

Рис. 4.11 Метод контролю даних ПНН ВПЗ

3	Виконання операції віднімання $A^{(2)} = A^{(1)} - KH^{(1)} =$ $= \{0 \Vert [a_2^{(1)} - t_2^{(1)}] \bmod m_2 \Vert$ $\Vert [a_3^{(1)} - t_3^{(1)}] \bmod m_3 \Vert$ $\Vert [a_4^{(1)} - t_4^{(1)}] \bmod m_4 \Vert ...$ $... \Vert [a_{i-1}^{(1)} - t_{i-1}^{(1)}] \bmod m_{i-1} \Vert$ $\Vert [a_i^{(1)} - t_i^{(1)}] \bmod m_i \Vert$ $\Vert [a_{i+1}^{(1)} - t_{i+1}^{(1)}] \bmod m_{i+1} \Vert ...$ $... \Vert [a_{n-3}^{(1)} - t_{n-3}^{(1)}] \bmod m_{n-3} \Vert$ $\Vert [a_{n-2}^{(1)} - t_{n-2}^{(1)}] \bmod m_{n-2} \Vert$ $\Vert [a_{n-1}^{(1)} - t_{n-1}^{(1)}] \bmod m_{n-1} \Vert 0 \Vert$ $\Vert [a_{n+1}^{(1)} - t_{n+1}^{(1)}] \bmod m_{n+1} \} = [0 \Vert 0 \Vert a_3^{(2)} \Vert$ $\Vert a_4^{(2)} \Vert ... \Vert a_{i-1}^{(2)} \Vert a_i^{(2)} \Vert a_{i+1}^{(2)} \Vert ... \Vert a_{n-3}^{(2)} \Vert$ $\Vert a_{n-2}^{(2)} \Vert 0 \Vert 0 \Vert a_{n+1}^{(2)}]$.	Утворення значень залишків $a_3^{(2)}$ і $a_{n-2}^{(2)}$ числа $A^{(2)} = [0 \Vert 0 \Vert a_3^{(2)} \Vert ... \Vert a_{i-1}^{(2)} \Vert$ $\Vert a_i^{(2)} \Vert a_{i+1}^{(2)} \Vert ... \Vert a_{n-3}^{(2)} \Vert a_{n-2}^{(2)} \Vert$ $\Vert 0 \Vert 0 \Vert a_{n+1}^{(2)}]$ у вигляді $a_3^{(2)} = t_3^{(2)} = \left[a_3^{(1)} - a_2^{(1)} \right] \bmod m_3$ і $a_{n-2}^{(2)} = t_{n-2}^{(2)} =$ $= \left[a_{n-2}^{(1)} - a_{n-1}^{(1)} \right] \bmod m_{n-2}$.
⋮	…	…
Для значення $A^{(i)}$	Виконання операції віднімання $A^{(i)} = A^{(i-1)} - KH^{(i-1)} = [0 \Vert 0 \Vert 0 \Vert ...$ $\Vert 0 \Vert a_i^{(i-1)} \Vert a_{i+1}^{(i-1)} \Vert ... \Vert 0 \Vert 0 \Vert a_{n+1}^{(i-1)}] - [0 \Vert 0 \Vert$ $\Vert 0 \Vert ... \Vert 0 \Vert t_i^{(i-1)} \Vert t_{i+1}^{(i-1)} \Vert ... \Vert 0 \Vert 0 \Vert t_{n+1}^{(i-1)}] =$ $\{0 \Vert 0 \Vert ... \Vert 0 \Vert [a_i^{(i-1)} - t_i^{(i-1)}] \bmod m_i \Vert$ $\Vert [a_{i+1}^{(i-1)} - t_{i+1}^{(i-1)}] \bmod m_{i+1} \Vert$ $\Vert [a_{i+2}^{(i-1)} - t_{i+2}^{(i-1)}] \bmod m_{i+2} \Vert ...$ $... \Vert [a_{n-i-1}^{(i-1)} - t_{n-i-1}^{(i-1)}] \bmod m_{n-i-1} \Vert$ $\Vert [a_{n-i}^{(i-1)} - t_{n-i}^{(i-1)}] \bmod m_{n-i} \Vert$ $\Vert [a_{n-i+1}^{(i-1)} - t_{n-i+1}^{(i-1)}] \bmod m_{n-i+1} \Vert 0 \Vert 0 \Vert ...$ $... \Vert 0 \Vert [a_{n+1}^{(i-1)} - t_{n+1}^{(i-1)}] \bmod m_{n+1} \} = [0 \Vert 0 \Vert ...$ $... \Vert 0 \Vert 0 \Vert a_{i+1}^{(i)} \Vert a_{i+2}^{(i)} \Vert a_{i+3}^{(i)} \Vert ... \Vert a_{n-i-1}^{(i)} \Vert$ $\Vert a_{n-i}^{(i)} \Vert 0 \Vert 0 \Vert ... \Vert 0 \Vert a_{n+1}^{(i)}]$.	Звернення по значеннях залишків $a_{i+1}^{(i)}$ і $a_{n-i}^{(i)}$ числа $A^{(i)} = [0 \Vert 0 \Vert ... \Vert 0 \Vert a_{i+1}^{(i)} \Vert$ $\Vert a_{i+2}^{(i)} \Vert ... \Vert a_{n-i-1}^{(i)} \Vert a_{n-i}^{(i)} \Vert 0 \Vert ...$ $... \Vert 0 \Vert 0 \Vert a_{n+1}^{(i)}]$ у БКН$_i$ за константою нульовизації $KH^{(i)} = [0 \Vert 0 \Vert ... \Vert 0 \Vert t_{i+1}^{(i)} \Vert$ $\Vert t_{i+2}^{(i)} \Vert ... \Vert t_{n-i-1}^{(i)} \Vert t_{n-i}^{(i)} \Vert 0 \Vert ...$ $... \Vert 0 \Vert 0 \Vert t_{n+1}^{(i)}]$; $t_{i+1}^{(i)} = a_{i+1}^{(i)}$, $t_{n-i}^{(i)} = a_{n-i}^{(i)}$; $t_{i+1}^{(i)} = \overline{0, m_{i+1} - 1}$; $t_{n-i}^{(i)} = \overline{0, m_{n-i} - 1}$.

Рис. 4.11, аркуш 2

Для значення $A^{(i+1)}$	Виконання операції віднімання $A^{(i+1)} = A^{(i)} - KH^{(i)} = [0 \| 0 \| \ldots \| 0 \| a_{i+1}^{(i)} \|$ $\| a_{i+2}^{(i)} \| a_{i+3}^{(i)} \| \ldots \| a_{n-i-2}^{(i)} \| a_{n-i-1}^{(i)} \| a_{n-i}^{(i)} \| 0 \| \ldots$ $\ldots \| 0 \| a_{n+1}^{(i)}] - [0 \| 0 \| \ldots \| 0 \| t_{i+1}^{(i)} \| t_{i+2}^{(i)} \|$ $\| t_{i+3}^{(i)} \| \ldots \| t_{n-i-2}^{(i)} \| t_{n-i-1}^{(i)} \| t_{n-1}^{(i)} \| 0 \| \ldots \| 0 \|$ $\| t_{n+1}^{(i)}] = \{0 \| 0 \| \ldots \| 0 \|$ $\| [a_{i+1}^{(i)} - t_{i+1}^{(i)}] \bmod m_{i+1} \|$ $\| [a_{i+2}^{(i)} - t_{i+2}^{(i)}] \bmod m_{i+2} \|$ $\| [a_{i+3}^{(i)} - t_{i+3}^{(i)}] \bmod m_{i+3} \| \ldots$ $\ldots \| [a_{n-i-2}^{(i)} - t_{n-i-2}^{(i)}] \bmod m_{n-i-2} \|$ $\| [a_{n-i-1}^{(i)} - t_{n-i-1}^{(i)}] \bmod m_{n-i-1} \|$ $\| [a_{n-i}^{(i)} - t_{n-i}^{(i)}] \bmod m_{n-i} \| 0 \| \ldots \| 0 \|$ $\| [a_{n+1}^{(i)} - t_{n+1}^{(i)}] \bmod m_{n+1}\} =$ $= [0 \| 0 \| \ldots \| 0 \| 0 \| a_{i+2}^{(i+1)} \| a_{i+3}^{(i+1)} \| \ldots$ $\ldots \| a_{n-i-2}^{(i+1)} \| a_{n-i-1}^{(i+1)} \| 0 \| 0 \| \ldots \| 0 \| 0 \| a_{n+1}^{(i+1)}].$	Утворення значень залишків $a_{i+2}^{(i+1)}$ та $a_{n-i-1}^{(i+1)}$ числа $A^{(i+1)} = [0 \| 0 \| \ldots \| 0 \| 0 \|$ $\| a_{i+2}^{(i+1)} \| a_{i+3}^{(i)} \| \ldots \| a_{n-i-2}^{(i+1)} \| a_{n-i-1}^{(i+1)} \|$ $\| 0 \| 0 \| \ldots \| 0 \| 0 \| a_{n+1}^{(i+1)}]$ у вигляді $a_{i+2}^{(i+1)} = t_{i+2}^{(i+1)} =$ $= \left[a_{i+2}^{(i)} - a_{i+1}^{(i)} \right] \bmod m_{i+2}$ та $a_{n-i-1}^{(i+1)} = t_{n-i-1}^{(i+1)} =$ $= \left[a_{n-i-1}^{(i)} - a_{n-i-2}^{(i)} \right] \bmod m_{n-i-1}.$
$i+2$	Звернення по значеннях залишків $a_{i+2}^{(i+1)}$ і $a_{n-i-1}^{(i+1)}$ числа $A^{(i+1)} = [0 \| 0 \| \ldots$ $\ldots \| 0 \| 0 \| a_{i+2}^{(i+1)} \| a_{i+3}^{(i)} \| \ldots \| a_{n-i-2}^{(i+1)} \| a_{n-i-1}^{(i+1)} \|$ $\| 0 \| 0 \| \ldots \| 0 \| 0 \| a_{n+1}^{(i+1)}]$ у БКН$_{i+1}$ за константою нульовизації $KH^{(i+1)} = [0 \|$ $\| 0 \| \ldots \| 0 \| 0 \| t_{i+2}^{(i+1)} \| t_{i+3}^{(i+1)} \| \ldots \| t_{n-i-2}^{(i+1)} \|$ $\| t_{n-i-1}^{(i+1)} \| 0 \| 0 \| \ldots \| 0 \| 0 \| t_{n+1}^{(i+1)}];$ $t_{i+2}^{(i+1)} = a_{i+2}^{(i+1)},\ t_{n-i-1}^{(i+1)} = a_{n-i-1}^{(i+1)};$ $t_{i+2}^{(i+1)} = \overline{0, m_{i+2} - 1},\ t_{n-i-1}^{(i+1)} = \overline{0, m_{n-i-1} - 1}.$	Утворення значень залишків $a_{i+3}^{(i+2)}$ і $a_{n-i-2}^{(i+2)}$ числа $A^{(i+2)} = [0 \| 0 \| \ldots \| 0 \| 0 \|$ $\| a_{i+3}^{(i+2)} \| a_{i+4}^{(i+2)} \| \ldots \| a_{n-i-3}^{(i+2)} \|$ $\| a_{n-i-2}^{(i+2)} \| 0 \| 0 \| \ldots \| 0 \| 0 \| a_{n+1}^{(i+2)}]$ у вигляді $a_{i+3}^{(i+2)} = t_{i+2}^{(i+2)} =$ $= \left[a_{i+3}^{(i+1)} - a_{i+2}^{(i+1)} \right] \bmod m_{i+3}$ та $a_{n-i-2}^{(i+2)} = t_{n-i-2}^{(i+2)} =$ $= \left[a_{n-i-2}^{(i+1)} - a_{n-i-3}^{(i+1)} \right] \bmod m_{n-i-2}.$
$\vdots$	…	…

Рис. 4.11, аркуш 3

$k-2$	Звернення по значеннях залишків $a_{n/2-1}^{(n/2-2)}$ і $a_{n/2+2}^{(n/2-2)}$ числа $A^{(n/2-2)}=[0\|\|0\|\|...$ $...\|\|0\|\|0\|\|a_{n/2-1}^{(n/2-2)}\|\|a_{n/2}^{(n/2-2)}\|\|a_{n/2+1}^{(n/2-2)}\|\|a_{n/2+2}^{(n/2-2)}\|\|$ $\|\|0\|\|0\|\|...\|\|0\|\|0\|\|a_{n+1}^{(n/2-2)}]$ у $БКН_{n/2-2}$ за константою нульовизації $КН^{(n/2-2)}=[0\|\|$ $\|\|0\|\|...\|\|0\|\|0\|\|t_{n/2-1}^{(n/2-2)}\|\|t_{n/2-2}^{(n/2-2)}\|\|...\|\|t_{n/2+1}^{(n/2-2)}\|\|$ $\|\|t_{n/2+2}^{(n/2-2)}\|\|0\|\|0\|\|...\|\|0\|\|0\|\|t_{n+1}^{(n/2-2)}]$; $t_{n/2-1}^{(n/2-1)}=a_{n/2-1}^{(n/2-2)}$, $t_{n/2+2}^{(n/2-2)}=a_{n/2+2}^{(n/2-2)}$; $t_{n/2-1}^{(n/2-2)}=\overline{0,m_{n/2-1}-1}$, $t_{n/2+2}^{(n/2-2)}=\overline{0,m_{n/2+2}-1}$.	Утворення значень залишків $a_{n/2}^{(n/2-1)}$ і $a_{n/2+1}^{(n/2-1)}$ числа $A^{(n/2-1)}=[0\|\|0\|\|...\|\|0\|\|0\|\|$ $\|\|a_{n/2}^{(n/2-1)}\|\|a_{n/2+1}^{(n/2-1)}\|\|0\|\|0\|\|...$ $...\|\|0\|\|0\|\|a_{n+1}^{(n/2-1)}]$ у вигляді $a_{n/2}^{(n/2-1)}=t_{n/2}^{(n/2-1)}=$ $=\left[a_{n/2}^{(n/2-2)}-a_{n/2-1}^{(n/2-2)}\right]\bmod m_{n/2}$ та $a_{n/2+1}^{(n/2-1)}=t_{n/2+1}^{(n/2-1)}=$ $=\left[a_{n/2+1}^{(n/2-2)}-a_{n/2}^{(n/2-2)}\right]\bmod m_{n/2+1}$.
$k-1$	Виконання операції віднімання $A^{(n/2-1)}=A^{(n/2-2)}-KH^{(n/2-2)}=[0\|\|0\|\|...$ $...\|\|0\|\|0\|\|a_{n/2-1}^{(n/2-2)}\|\|a_{n/2}^{(n/2-2)}\|\|a_{n/2+1}^{(n/2-2)}\|\|$ $\|\|a_{n/2+2}^{(n/2-2)}\|\|0\|\|0\|\|...\|\|0\|\|0\|\|a_{n+1}^{(n/2-2)}]-[0\|\|$ $\|\|0\|\|...\|\|0\|\|0\|\|t_{n/2-1}^{(n/2-2)}\|\|t_{n/2}^{(n/2-2)}\|\|t_{n/2+1}^{(n/2-2)}\|\|$ $\|\|t_{n/2+2}^{(n/2-2)}\|\|0\|\|0\|\|...\|\|t_{n+1}^{(n/2-2)}]=\{0\|\|0\|\|...$ $...\|\|0\|\|0\|\|[a_{n/2-1}^{(n/2-2)}-t_{n/2-1}^{(n/2-2)}]\bmod m_{n/2-1}\|\|$ $\|\|[a_{n/2}^{(n/2-2)}-t_{n/2}^{(n/2-2)}]\bmod m_{n/2}\|\|...$ $...\|\|[a_{n/2+1}^{(n/2-2)}-t_{n/2+1}^{(n/2-2)}]\bmod m_{n/2+1}\|\|$ $\|\|[a_{n/2+2}^{(n/2-2)}-t_{n/2+2}^{(n/2-2)}]\bmod m_{n/2+2}\|\|0\|\|0\|\|...$ $...\|\|0\|\|0\|\|[a_{n+1}^{(n/2-2)}-t_{n+1}^{(n/2-2)}]\bmod m_{n+1}\}=$ $=[0\|\|0\|\|...\|\|0\|\|0\|\|0\|\|a_{n/2}^{(n/2-1)}\|\|a_{n/2+1}^{(n/2-1)}\|\|$ $\|\|0\|\|0\|\|...\|\|0\|\|0\|\|a_{n+1}^{(n/2-1)}]$.	Звернення по значеннях залишків $a_{n/2}^{(n/2-1)}$ і $a_{n/2+1}^{(n/2-1)}$ числа $A^{(n/2-1)}=[0\|\|0\|\|...\|\|0\|\|0\|\|$ $\|\|a_{n/2}^{(n/2-1)}\|\|a_{n/2+1}^{(n/2-1)}\|\|0\|\|0\|\|...\|\|0\|\|$ $\|\|0\|\|a_{n+1}^{(n/2-1)}]$; у $БКН_{n/2-1}$ за константою нульовизації $КН^{(n/2-1)}=[0\|\|0\|\|...\|\|0\|\|0\|\|$ $\|\|t_{n/2}^{(n/2-1)}\|\|t_{n/2+1}^{(n/2-1)}\|\|0\|\|0\|\|...\|\|0\|\|$ $\|\|0\|\|t_{n+1}^{(n/2-1)}]$; $t_{n/2}^{(n/2-1)}=a_{n/2}^{(n/2-1)}$, $t_{n/2+1}^{(n/2-1)}=a_{n/2+1}^{(n/2-1)}$; $t_{n/2}^{(n/2-1)}=\overline{0,m_{n/2}-1}$, $t_{n/2+1}^{(n/2-1)}=\overline{0,m_{n/2+1}-1}$.
k	Отримання нульовизованого $A^{(H)}$ числа. Виконання операції $A^{(n/2-1)}=A^{(n/2-2)}-KH^{(n/2-2)}=[0\|\|0\|\|...\|\|0\|\|a_{n/2}^{(n/2-1)}\|\|a_{n/2+1}^{(n/2-1)}\|\|0\|\|...$ $...\|\|0\|\|a_{n+1}^{(n/2-1)}]-[0\|\|0\|\|...\|\|0\|\|t_{n/2}^{(n/2-1)}\|\|t_{n/2+1}^{(n/2-1)}\|\|0\|\|...\|\|0\|\|t_{n+1}^{(n/2-1)}]=$ $=[0\|\|0\|\|...\|\|0\|\|[a_{n/2}^{(n/2-1)}-t_{n/2}^{(n/2-1)}]\bmod m_{n/2}\|\|[a_{n/2+1}^{(n/2-1)}-t_{n/2+1}^{(n/2-1)}]\bmod m_{n/2+1}\|\|$ $\|\|0\|\|...\|\|0\|\|[a_{n+1}^{(n/2-1)}-t_{n+1}^{(n/2-1)}]\bmod m_{n+1}=[0\|\|0\|\|...\|\|0\|\|...\|\|0\|\|0\|\|(\gamma_{n+1}=a_{n+1}^{(n/2)})]$.	

$$T_{H4}=\left(\left[\frac{n+1}{2}\right]+\left[\frac{\frac{n+1}{2}+1}{2}\right]\right)\cdot\tau_{сл}$$

Рис. 4.11, аркуш 4

Таблиця 4.11

Основні характеристики методів контролю даних у СЗК

Методи контролю даних *Hi*		Час нульовизації T_{Hi}	Кількість констант нульовизації K_{Hi}	Кількість двійкових розрядів констант нульовизації N_{Hi}
*H*1	Метод послідовної нульовизації	$T_{H1} = 2 \cdot n \cdot \tau_{сл}$	$K_{H1} = \sum_{i=1}^{n} (m_i - 1)$	$N_{H1} = \sum_{i=1}^{n} (m_i - 1) \cdot (n - i + 1)$
*H*2	Метод послідовної нульовизації з визначенням подальшого залишку	$T_{H2} = \left(\left[\frac{n-1}{2} \right] + n \right) \cdot \tau_{сл}$	$K_{H2} = \sum_{i=1}^{n-1} (m_i - 1)$	$N_{H2} = \sum_{i=1}^{n-1} (m_i - 1) \cdot (n - i)$
*H*3	Метод паралельної нульовизації	$T_{H3} = n \cdot \tau_{сл}$	$K_{H3} = \sum_{i=1}^{\left[\frac{n}{2}\right]} (m_i \cdot m_{n-i+1} - 1)$	$N_{H3} = \sum_{i=1}^{\left[\frac{n}{2}\right]} (m_i \cdot m_{n-i+1} - 1) \cdot (n - 2 \cdot i + 1)$
*H*4	Метод паралельної нульовизації з визначенням подальших залишків	$T_{H4} = \left(\left[\frac{n+1}{2} \right] + \left[\frac{\left[\frac{n+1}{2} \right]}{2} \right] \right) \tau_{сл}$	$K_{H4} = \sum_{i=1}^{\left[\frac{n}{2}\right]} (m_i \cdot m_{n-i+1} - 2)$	$N_{H4} = \sum_{i=1}^{\left[\frac{n}{2}\right]} (m_i \cdot m_{n-i+1} - 2) \cdot (n - 2 \cdot i + 1)$

Таблиця 4.12

Сукупність основ СЗК для *l*–байтових ($l=\overline{1\div 8}$) розрядних сіток обчислювача

Величина розрядної сітки $l(n)$	Інформаційні основи СЗК $\{m_i\},\ i=\overline{1,n}$	Контрольна основа СЗК m_{n+1}
1(4)	$m_1=3,\ m_2=4,\ m_3=5,\ m_4=7$	$m_5=11$
2(6)	$m_1=2,\ m_2=5,\ m_3=7,\ m_4=9,\ m_5=11,\ m_6=13$	$m_7=17$
3(8)	$m_1=3,\ m_2=4,\ m_3=5,\ m_4=7,\ m_5=11,\ m_6=13,$ $m_7=17,\ m_8=19$	$m_9=23$
4(10)	$m_1=2,\ m_2=3,\ m_3=5,\ m_4=7,\ m_5=11,\ m_6=13,$ $m_7=17,\ m_8=19,\ m_9=23,\ m_{10}=29$	$m_{11}=31$
8(16)	$m_1=3,\ m_2=4,\ m_3=5,\ m_4=7,\ m_5=11,\ m_6=13,$ $m_7=17,\ m_8=19,\ m_9=23,\ m_{10}=29,\ m_{11}=31,$ $m_{12}=37,\ m_{13}=41,\ m_{14}=43,\ m_{15}=47,\ m_{16}=53$	$m_{17}=59$

Таблиця 4.13

Розрахункові дані характеристик методів контролю даних у СЗК для *l*–байтових ($l=\overline{1\div 8}$) розрядних сіток

$l\ (n)$	$H1$			$H2$			$H3$			$H4$		
	$\frac{T_{H1}}{\tau_{сл}}$	K_{H1}	N_{H1}	$\frac{T_{H2}}{\tau_{сл}}$	K_{H2}	N_{H2}	$\frac{T_{H3}}{\tau_{сл}}$	K_{H3}	N_{H3}	$\frac{T_{H4}}{\tau_{сл}}$	K_{H4}	N_{H4}
1 (4)	8	15	31	5	9	16	4	39	79	3	37	75
2 (6)	12	41	106	8	29	65	6	141	349	4	138	340
3 (8)	16	71	217	11	53	146	8	263	995	6	259	979
4 (10)	20	119	412	14	91	293	10	479	1955	7	474	1930
8 (16)	32	367	1947	23	315	1580	16	2581	16493	12	2573	16429

Для зручності проведення порівняльного аналізу ефективності використання представлених методів контролю, узагальнені дані табл. 4.13

доцільно розмістити у трьох (по числу характеристик) окремих таблицях (табл. 4.14–4.16).

Таблиця 4.14

Часові характеристики методів контролю

l (n)	$T_{H_i} / \tau_{сл}$			
	$H1$	$H2$	$H3$	***H*4**
1 (4)	8	5	4	**3**
2 (6)	12	8	6	**4**
3 (8)	16	11	8	**6**
4 (10)	20	14	10	**7**
8 (16)	32	23	16	**12**

Таблиця 4.15

Характеристики методів контролю

l (n)	K_{H_i}			
	$H1$	***H*2**	$H3$	$H4$
1 (4)	15	**9**	39	37
2 (6)	41	**29**	141	138
3 (8)	71	**53**	263	259
4 (10)	119	**91**	479	474
8 (16)	367	**315**	2581	2573

Таблиця 4.16

Характеристики методів контролю

l (n)	N_{H_i}			
	$H1$	***H*2**	$H3$	$H4$
1 (4)	31	**16**	79	75
2 (6)	106	**65**	349	340
3 (8)	217	**146**	995	979
4 (10)	412	**293**	1955	1930
8 (16)	1947	**1580**	16493	16429

На основі табл. 4.16 складена табл. 4.17 даних порівняльного аналізу ефективності застосування методу оперативного контролю ПНН ВПЗ,

порівняно з існуючими методами контролю у СЗК за швидкодією реалізації процедури нульовизації.

Коефіцієнт K_{Hi} ефективності використання методу контролю ПНН ВПЗ, порівняно з існуючими методами нульовизації, визначається співвідношенням

$$K_{Hi} = \frac{T_{H1} - T_{Hi}}{T_{H1}} \cdot 100\%, \ (i = \overline{1,3}).$$

Таблиця 4.17

Дані порівняльного аналізу часу контролю даних у СЗК

n	$T_{Hi} = T/\tau$				Виграш в [%]		
	T_{H1}	T_{H2}	T_{H3}	T_{H4}	K_{H1}	K_{H2}	K_{H3}
4	8	5	4	**3**	62	40	25
6	12	8	6	**4**	66	55	33
8	16	11	8	**6**	62	45	25
10	20	14	10	**7**	65	53	30
16	32	23	16	**12**	62	47	25

З табл. 4.17 видна висока ефективність методу оперативного контролю (*H*4), заснованого на реалізації процедури паралельної нульовизації з визначенням подальших залишків.

4.5 Методи контролю даних у СЗК, що засновані на використанні позиційної ознаки непозиційної кодової структури

4.5.1 Метод оперативного контролю даних у СЗК, що заснований на використанні позиційної ознаки НКС

Ґрунтуючись на результатах, що описані у розділі 3.4, слід зазначити, що для визначення тільки факту спотворення числа *A,* немає необхідності мати і аналізувати усю послідовність *N* сукупності значень $Z_{K_A}^{(A)}$ ОК

$K_N^{(n_A)} = \left\{ Z_{N-1}^{(A)}\ Z_{N-1}^{(A)} \ldots Z_1^{(A)}\ Z_0^{(A)} \right\}$. Для цього досить мати ОК $K_{N_i}^{(n_A)}$ завдовжки усього $N_i =]M / m_i[$ двійкових розрядів (де значення $]M / m_i[$ означає цілу частину числа M / m_i, його не меншу; тобто робиться округлення числа M / m_i до найближчого цілого у більшу сторону) [133-135].

Цей факт можна пояснити таким чином. При проведенні процедури контролю, для встановлення факту правильності або неправильності числа $A = (a_1 \,||\, a_2 \,||\, \ldots \,||\, a_{i-1} \,||\, a_i \,||\, a_{i+1} \,||\, \ldots \,||\, a_n \,||\, a_{n+1})$, немає необхідності аналізувати усі числові інтервали $[j_i \cdot m_i,\ (j_i + 1) \cdot m_i)$, де знаходиться спотворене число, що розташовані поза інформаційним інтервалом $[0, M)$. В цьому випадку, для встановлення тільки факту правильності або неправильності числа *A,* визначення номерів та аналіз місця розташування цих інтервалів $[j_i \cdot m_i,\ (j_i + 1) \cdot m_i)$ не має ніякого значення. Для контролю НКС *A* у СЗК досить знати місце розташування нуля у записі $K_N^{(n_A)} = \left\{ Z_{N-1}^{(A)}\ Z_{N-2}^{(A)} \ldots Z_1^{(A)}\ Z_0^{(A)} \right\}$ ОК (знати чисельне значення n_A) тільки у числових інтервалах $[j_i \cdot m_i,\ (j_i + 1) \cdot m_i)$, що лежать в інформаційному числовому інтервалі $0 \div M$, та у першому, що розташований після значення *M* інтервалі, який розташований на відрізку $0 \div M_0$ (рис. 4.12). Як видно, для контролю даних $A = (a_1 \,||\, a_2 \,||\, \ldots \,||\, a_{i-1} \,||\, a_i \,||\, a_{i+1} \,||\, \ldots \,||\, a_n \,||\, a_{n+1})$ досить мати ОК $K_{N_i}^{(n_A)}$ завдовжки усього $N_i =]M / m_i[$ двійкових розрядів.

Суть методу контролю даних у СЗК полягає у наступному. Для НКС у СЗК $A = (a_1 \,||\, a_2 \,||\, \ldots \,||\, a_{i-1} \,||\, a_i \,||\, a_{i+1} \,||\, \ldots \,||\, a_n \,||\, a_{n+1})$, що контролюється, визначається ПОНКС n_A шляхом формування ОК $K_{N_i}^{(n_A)} = \left\{ Z_{N_i-1}^{(A)}\ Z_{N_i-2}^{(A)} \ldots Z_1^{(A)}\ Z_0^{(A)} \right\}$ у вигляді послідовності з N_i двійкових розрядів [136-138].

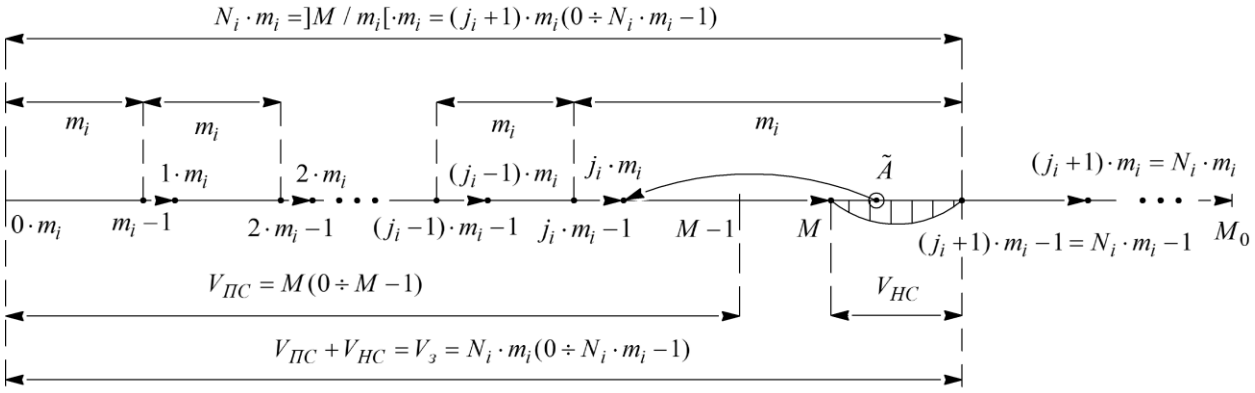

Рис. 4.12 Схема контролю даних для довільного значення модуля m_i

Виходячи зі значення залишку a_i числа $A = (a_1 \,||\, a_2 \,||\, ... \,||\, a_{i-1} \,||\, a_i \,||\, a_{i+1} \,||\, ... \,||\, a_n \,||\, a_{n+1})$, вибирається константа нульовизації виду $KH_{m_i}^{(A)} = \left(a_1' \,||\, a_2' \,||\, ... \,||\, a_{i-1}' \,||\, a_i \,||\, a_{i+1}' \,||\, ... \,||\, a_n' \,||\, a_{n+1}'\right)$. Далі проводитися реалізація операції $A_{m_i} = A - KH_{m_i}^{(A)}$.

Використовуючи N_i констант $K_A \cdot m_i$ $\left(K_A = \overline{0, N_i - 1}\right)$, одночасно проводяться операції віднімання $A_{m_i} - K_A \cdot m_i$, у результаті яких, утворюється значення двійкових розрядів $Z_{K_A}^{(A)}$, тобто формується ОК $K_{N_i}^{(n_A)}$. Значення ПОНКС n_A визначається з рівності $A_{m_i} - n_A \cdot m_i = 0$.

Процедура контролю числа *A* полягає у наступному. Якщо $n_A > N_i$, то вважається, що число *A* – неправильне. У протилежному випадку ($n_A \le N_i$) число *A* – правильне.

Таким чином, за рахунок одночасного і паралельного проведення операції віднімання констант, в $\approx N_i$ раз зменшується час визначення значення ПОНКС n_A. Ця обставина дозволяє підвищити оперативність контролю даних, в порівнянні з існуючими методами, на 30-40 %.

Розроблений метод представлено на рис. 4.13

1	Визначення ОК $K_{N_i}^{(n_A)} = \left\{ Z_{N_i-1}^{(A)}\ Z_{N_i-2}^{(A)} \dots Z_1^{(A)}\ Z_0^{(A)} \right\}$ числа $A = (a_1 \,\|\| \, a_2 \,\|\| \dots \|\| \, a_{i-1} \,\|\| \, a_i \,\|\| \, a_{i+1} \,\|\| \dots \|\| \, a_n \,\|\| \, a_{n+1})$.
2	Визначення ПОНКС n_A: $A_{m_i} - n_A \cdot m_i = 0$, $Z_{n_A}^{(A)} = 0$; $Z_l^{(A)} = 1$, $A_{m_i} - l \cdot m_i = 1$; $l \neq n_A$.
3	Проведення процедури контролю даних $A = (a_1 \,\|\| \, a_2 \,\|\| \dots \|\| \, a_{i-1} \,\|\| \, a_i \,\|\| \, a_{i+1} \,\|\| \dots \|\| \, a_n \,\|\| \, a_{n+1})$ у СЗК. Якщо $n_A > N_i$, то число $\tilde{A}$ неправильне (спотворене). Якщо $n_A \le N_i$, то число A правильне (неспотворене).

Рис. 4.13 Метод контролю даних у СЗК

Розглянемо приклади реалізації методу контролю для конкретної СЗК, яка заданий основами $m_1 = 3$, $m_2 = 4$, $m_3 = 5$, $m_4 = 7$ і $m_k = m_{n+1} = m_5 = 11$. Ця СЗК забезпечує обробку даних в однобайтовій ($l = 1$) розрядній сітці КСКОЦД. При цьому $M = \prod_{i=1}^{4} m_i = 420$, $M_0 = M \cdot m_{n+1} = 4620$. Окрім цього будемо вважати, що $m_i = 11$. У цьому випадку $N_i = N_{n+1} =]M / m_i[=]M / m_{n+1}[=]420 / 11[=]38{,}18[= 39$.

У таблиці 4.18 приведений вміст БКН КСКОЦД відносно основи $m_k = m_{n+1} = 11$.

Приклад 4.3. Провести контроль даних, що представлені у вигляді $A = (01 \,\|\| \, 00 \,\|\| \, 000 \,\|\| \, 010 \,\|\| \, 0001)$ при $m_k = m_{n+1} = m_5 = 11$. За значенням залишку $a_K = a_{n+1} = a_5 = 0001$ числа A у БКН (табл. 4.18) вибирається константа $KH_{m_{n+1}}^{(A)} = (01 \,\|\| \, 01 \,\|\| \, 001 \,\|\| \, 001 \,\|\| \, 0001)$ нульовизації. Далі визначаємо $A_{m_{n+1}} = A - KH_{m_{n+1}}^{(A)} = (00 \,\|\| \, 11 \,\|\| \, 100 \,\|\| \, 001 \,\|\| \, 0000)$.

За допомоги реалізації співвідношення

$$\begin{cases} A_{m_i} - 0 \cdot m_i = Z_0^{(A)}, \\ A_{m_i} - 1 \cdot m_i = Z_1^{(A)}, \\ A_{m_i} - 2 \cdot m_i = Z_2^{(A)}, \\ \quad \dots \\ A_{m_i} - (N-2) \cdot m_i = Z_{N-2}^{(A)}, \\ A_{m_i} - (N-1) \cdot m_i = Z_{N-1}^{(A)} \end{cases},$$

сформуємо ОК виду $K_{N_i}^{(n_A)} = K_{39}^{(9)} = \{11...110111111111\}$. Виходячи з виду ОК та використовуючи вираз $A_{m_{n+1}} - n_A \cdot m_{n+1} = 0$, визначаємо, що $n_A = 9$ ($A_{m_{n+1}} - n_A \cdot m_{n+1} = 99 - 9 \cdot 11 = 0$), тобто $Z_{n_A}^{(A)} = Z_9^{(A)}$. Так, як $N_i = 39 > n_A = 9$, то помилки у даних немає.

Перевірка: $A = 100 < M = 420$ (число A правильне).

Таблиця 4.18

Константи $KH_{m_{n+1}}^{(A)}$ нульовизації

Остача $a_к = a_{n+1}$	Константи нульовизації				
	$m_1 = 3$	$m_2 = 4$	$m_3 = 5$	$m_4 = 7$	$m_k = m_5 = 11$
	a'_1	a'_2	a'_3	a'_4	a_5
0000	00	00	000	000	0000
0001	01	01	001	001	0001
0010	10	10	010	010	0010
0011	00	11	011	011	0011
0100	01	00	100	100	0100
0101	10	01	000	101	0101
0110	00	10	001	110	0110
0111	01	11	010	000	0111
1000	10	00	011	001	1000
1001	00	01	100	010	1001
1010	01	10	000	011	1010

Приклад 4.4. Провести контроль даних $A=(00\,||\,01\,||\,000\,||\,010\,||\,1010)$. За значенням $a_5=1010$ у БКН (таблиця. 4.18) вибирається константа виду $KH^{(A)}_{m_{n+1}}=(01\,||\,10\,||\,000\,||\,011\,||\,1010)$. Отримаємо, що $A_{m_{n+1}}=A-KH^{(A)}_{m_{n+1}}=$ $=(10\,||\,00\,||\,000\,||\,110\,||\,0000)$. Оскільки $A_{m_{n+1}}-n_A\cdot m_{n+1}=440-44\cdot 11=0$, то ОК має вигляд $K^{(n_A)}_{N_i}=K^{(40)}_{39}=\{11...11...11\}$ і $n_A=40$. Оскільки $N_i=39<n_A=40$ то помилка в даних є присутньою.

Перевірка: $A=450>M=420$ (число A неправильне).

Приклад 4.5. Провести контроль даних $A=(01\,||\,11\,||\,010\,||\,000\,||\,1001)$. За значенням $a_5=1001$ у БКН (табл. 4.18) вибирається константа $KH^{(A)}_{m_{n+1}}=(00\,||\,01\,||\,100\,||\,010\,||\,1001)$. Отримуємо, що $A_{m_{n+1}}=A-KH^{(A)}_{m_{n+1}}=$ $(01\,||\,10\,||\,011\,||\,101\,||\,0000)$. Оскільки $A_{m_{n+1}}-n_A\cdot m_{n+1}=418-38\cdot 11=0$, то ОК має вигляд $K^{(n_A)}_{N_i}=K^{(38)}_{39}=\{011...11...11\}$ та $n_A=38$. Виходячи з того, що $n_A=38<N_i=39$ робимо висновок: число A правильне (не спотворено). Проте перевірка показує, що $A=427>M=420$ тобто A – неправильне число (рис. 4.14). В цьому випадку при контролі даних припустилася помилка.

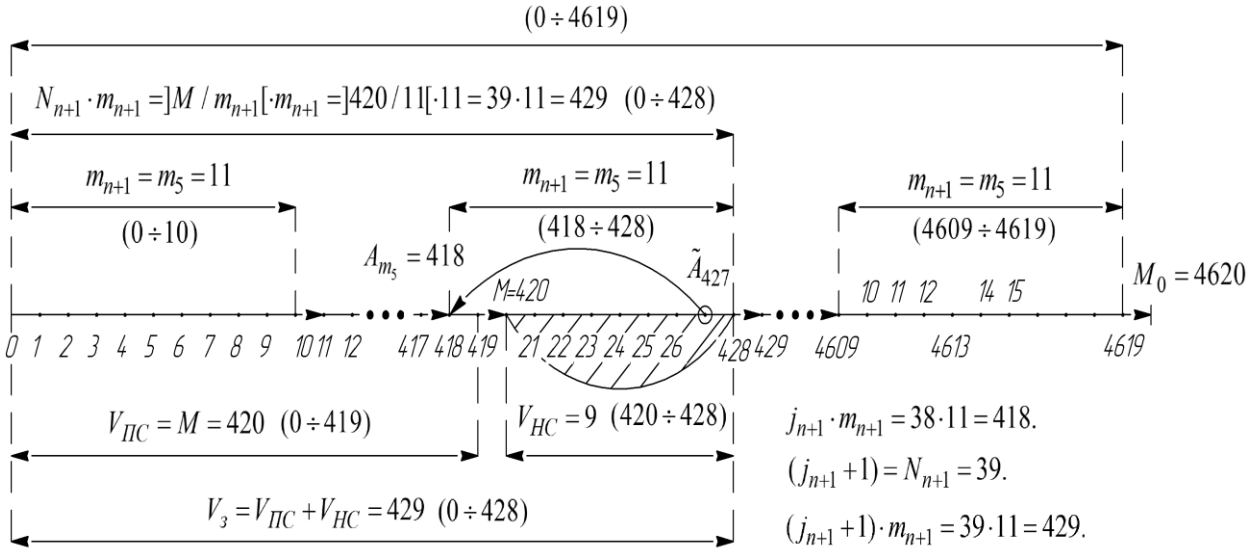

Рис. 4.14 Схема контролю даних у СЗК для $m_i=11$

З прикладу 4.5 видно, що застосування розглянутого методу для оперативного контролю даних у СЗК не в усіх випадках забезпечує достовірний результат контролю. Дійсно, існує сукупність $(j_{n+1}+1)\cdot m_{n+1} - M$ неправильних $\tilde{A}$ чисел, які визначаються системою контролю КСКОЦД як правильні, що обумовлює низьку достовірність контролю [139]. Для прикладу 4.5, таких чисел буде більше 80% (табл. 4.19).

Таблиця 4.19

Сукупність кодових слів

Числовий діапазон [418, 429)	
Правильні числа A	Сукупність неправильних $\tilde{A}$ чисел, які визначаються системою контролю КСКОЦД як правильні
418, 419	420, 421, 422, 423, 424, 425, 426, 427, 428

Проведемо розрахунок часу контролю даних для розробленого методу. Виходячи з вищевикладеного, загальний час контролю визначиться як:

$$T_{к\ ПО} = t_{виб} + t_{\Sigma 1} + t_{\Sigma 2} + t_{n_A} + t_n,$$

де $t_{виб}$ - час вибірки константи нульовизації з БКН за значенням залишку a_i числа $A = (a_1 \| a_2 \| ... \| a_i \| ... \| a_n \| a_{n+1})$ по модулю m_i СЗК – виду $KH_{m_{n+1}}^{(A)} = (t_1' \| t_2' \| ... \| t_i \| ... \| t_n' \| t_{n+1}')$;

$t_{\Sigma 1}$ – час визначення значення $A_{m_i} = A - KH_{m_i}^{(A)}$;

$t_{\Sigma 2}$ – час реалізації операції $A_{m_i} - n_A \cdot m_i$, тобто час, який потрібний для визначення ОК виду $K_{N_i}^{(n_A)} = \left\{ Z_{N_i-1}^{(A)}\ Z_{N_i-2}^{(A)} \dots Z_1^{(A)}\ Z_0^{(A)} \right\}$;

t_{n_A} – час визначення ПОНКС (n_A);

t_n – час перевірки умови $n_A \le N_i$.

З урахуванням того, що арифметичні операції додавання, віднімання і множення у СЗК, реалізовані на основі табличного принципу, виконуються за один часовий *t* такт функціонування, то час підсумовування буде рівний $t_{\Sigma 1} = t_{\Sigma 2} = t$.

Час $t_{виб.}$ вибірки константи $KH_{m_i}^{(A)}$ з БКН проводиться також за один часовий *t* такт, і буде дорівнюватись $t_{виб.} \approx \tau_{дод.} = \tau_{множ.} = t$, де $\tau_{дод.}$ і $\tau_{множ.}$ – час реалізації операцій логічного додавання (елементу АБО) та логічного множення (елементу І), відповідно.

Оскільки процес аналізу ОК на наявність нуля в його записі реалізується за допомогою багатовхідного логічного елементу І, то $t_{n_A} = t = \tau_I$.

Час перевірки умови $n_A \le N_i$ можна визначити за чотири часові машинні такти, то $t_{ср} = 4t$.

Для проведення порівняльного аналізу оперативності контролю зручно скористатися величиною $\tau = 2 \cdot t$, де τ – умовний часовий такт обробки даних.

У цьому випадку час контролю НКС, для описаного методу, визначиться як:

$$T_{к\ ПО} = \tau / 2 + \tau / 2 + \tau / 2 + \tau / 2 + 2\tau = 4\tau.$$

Таким чином, використання розробленого методу контролю даних, дозволяє провести процес контролю НКС за 4τ умовних часових тактів не залежно від величини *l* розрядної сітки КСКЦОД.

У табл. 4.20 представлені дані порівняльного аналізу часу контролю даних у СЗК для методу, заснованого на принципі паралельної нульвизації і для методу, заснованого на використанні позиційної ознаки непозиційної кодової структури.

Таблиця 4.20

Дані порівняльного аналізу часу контролю даних у СЗК

Метод контролю	Відносний час контролю даних T / τ				
	Величина розрядної сітки $l(n)$				
	$l=1$ $(n=4)$	$l=2$ $(n=6)$	$l=3$ $(n=8)$	$l=4$ $(n=10)$	$l=8$ $(n=16)$
Заснований на принципі паралельної нульовизації	3	4	6	7	12
Заснований на використанні ПОНКС	4	4	4	4	4
Виграш в %	–	0	33	42	66

Аналіз отриманих результатів проведених розрахунків та порівняльного аналізу оперативності розроблених методів контролю даних у СЗК, що поміщені у табл. 4.20, показав, що зі збільшенням розрядності l чисел, які оброблюються, що характерно для сучасної тенденції розвитку КСКОЦД, ефективність використання методу заснованого на використанні позиційної ознаки НКС – зростає.

4.5.2 Метод підвищення достовірності оперативного контролю даних у СЗК

Варто відмітити, що розроблений метод оперативного контролю даних у СЗК має дуже низьку достовірність контролю [140-142].

Низька достовірність контролю даних спричинена наявністю ненульового значення залишку a у виразі

$$a = M_{n+1} / m_{n+1} - [M_{n+1} / m_{n+1}] = M / m_{n+1} - [M / m_{n+1}]. \qquad (4.27)$$

У свою чергу наявність ненульового $a \neq 0$ залишку визначається фактом не кратності значення M по контрольному модулю m_{n+1} СЗК, який визначає величину числового інтервалу $[j_{n+1} \cdot m_{n+1},\ (j_{n+1}+1) \cdot m_{n+1})$ можливого знаходження числа A. У цьому випадку контроль даних $A = (a_1 \| a_2 \| \ldots \| a_{i-1} \| a_i \| a_{i+1} \| \ldots \| a_n \| a_{n+1})$ здійснюється на основі використання контрольної m_{n+1} основи СЗК, шляхом формування ОК $K_{N_{n+1}}^{(n_A)} = \left\{ Z_{N_{n+1}-1}^{(A)}\ Z_{N_{n+1}-2}^{(A)} \ldots Z_0^{(A)} \right\}$.

Геометрично низьку достовірність контролю даних можна пояснити таким чином. Числовий інформаційний інтервал $[0,\ M = \prod_{i=1}^{n} m_i)$ не вміщує ціле число відрізків довжиною рівних значенню $m_i = m_{n+1}$. У цьому випадку на числовій осі $0 \div M_0$ існує числовий інтервал $[j_{n+1} \cdot m_{n+1},\ (j_{n+1}+1) \cdot m_{n+1})$ (або $[(N_{n+1}-1) \cdot m_{n+1}, N_{n+1} \cdot m_{n+1})$) усередині якого знаходиться число M. Тому у цьому інтервалі одночасно знаходиться сукупність $(j_{n+1}+1) \cdot m_{n+1}) - M$ неправильних чисел (або $N_{n+1} \cdot m_{n+1} - M$) і сукупність $M - j_{n+1} \cdot m_{n+1}$ правильних чисел (або $M - (N_{n+1}-1) \cdot m_{n+1}$). У процесі контролю даних A, при проведенні процедури нульовизації, усі, як неправильні $(j_{n+1}+1) \cdot m_{n+1}) - M$, так і правильні $M - j_{n+1} \cdot m_{n+1}$ числа, зміщуються на лівий край (до одного правильного числа $j_{n+1} \cdot m_{n+1}$) інтервалу $[j_{n+1} \cdot m_{n+1},\ (j_{n+1}+1) \cdot m_{n+1})$. У цьому випадку, СК КСКОЦД, неправильні $[N_{n+1} \cdot m_{n+1}) - M]$ числа будуть ідентифікуватися (визначатися) як правильні.

Під достовірністю контролю даних у СЗК будемо розуміти імовірність отримання істинного результату операції контролю даних, що представлені у СЗК. У якості показника для кількісної оцінки достовірності контролю даних у СЗК можемо скористатися співвідношенням

$$P_{ок} = V_{ПС} / V_{ОС}, \qquad (4.28)$$

де у загальному випадку: $V_{ПС} = M$ – кількість (від 0 до $M-1$) правильних ($A < M$), що лежать у робітнику числовому $[0, M_0)$ діапазоні, кодових слів для даної СЗК;

$V_{ОС} = (V_{ПС} + V_{НС})$ – загальна кількість кодових слів, які у результаті проведення контролю даних вважаються правильними;

$V_{НС} = (N_i \cdot m_i - M)$ – кількість неправильних ($A \geq M$) кодових слів, які в результаті проведення контролю даних вважаються правильними (відмітимо, що $N_i =]M / m_i[= j_i + 1$).

З урахуванням цього, показник достовірності (4.28) визначається співвідношенням

$$P_{дк} = \frac{M}{M + N_i \cdot m_i - M} = \frac{M}{N_i \cdot m_i}. \qquad (4.29)$$

При $m_i = m_{n+1}$ маємо, що $V_{НС} = (N_{n+1} \cdot m_{n+1} - M)$. Якщо $m_i = m_{n+1}$, то вираз (4.29) набуде вигляду

$$P_{дк} = \frac{M}{M + N_{n+1} \cdot m_{n+1} - M} = \frac{M}{N_{n+1} \cdot m_{n+1}}. \qquad (4.30)$$

Так, як наперед відомо, що $N_{n+1} \cdot m_{n+1} > M$, то у цьому випадку завжди $P_{дк} < 1$.

Якщо в якості основи m_i, що визначає величини числових $j_i \cdot m_i \div (j_i + 1) \cdot m_i$ інтервалів, візьмемо інформаційну основу СЗК, наприклад, $m_i = m_1$, тоді $N_i =]M / m_i[= N_1 =]M / m_1[$ та $N_1 = \prod_{i=2}^{n} m_i$. У цьому випадку, вираз (4.29) набуде вигляду

$$P_{дк} = \frac{M}{M + N_1 \cdot m_1 - M} = \frac{M}{N_1 \cdot m_1} = 1. \qquad (4.31)$$

У цьому випадку маємо, що завжди $Д = 1$, тобто, у разі вибору $m_i = m_1$, СК КСКОЦД завжди забезпечує достовірний результат контролю даних у СЗК.

Запропонований метод підвищення достовірності контролю, що заснований на описаному у попередньому розділі 4.5.1 методі оперативного контролю інформації у СЗК, який, у свою чергу, складається з процедур отримання і використання ПОНКС. Ця ознака являється однією з характеристик ОК, що отримується з вихідної НКС $A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1})$ даних, яка представлена у СЗК основами $\{m_i\}$, $i = \overline{1, n+1}$, та однією контрольною основою m_{n+1}.

Суть запропонованого методу підвищення достовірності контролю даних у СЗК полягає у забезпеченні максимальної $P_{дк} = 1$ достовірності контролю даних, шляхом забезпечення виконання умови $a = 0$ (див. вираз (4.27)). У цьому випадку для обчислення значення $N_i =]M / m_i[$ вибирається модуль m_i, який визначає номер j_i числового інтервалу $[j_i \cdot m_i, (j_i + 1) \cdot m_i)$ знаходження числа $A = (a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1})$, тільки з сукупності *n* інформаційних модулів СЗК, які, звичайно, кратні значенню *M*. У цьому випадку $a = M - [M / m_i] \cdot m_i = 0$, що і забезпечує максимальне значення показника достовірності контролю $P_{дк} = 1$ (див. вираз (4.29)).

Розроблений метод підвищення достовірності контролю даних у СЗК, представлено на рис. 4.15.

Наведемо приклад застосування розробленого методу для підвищення достовірності контролю даних у СЗК.

1	Вибір модуля m_i, що визначає номер j_i числового інтервалу $[j_i \cdot m_i,\ (j_i+1)\cdot m_i)$ знаходження числа $A=(a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n, a_{n+1})$ з сукупності *n* інформаційних модулів СЗК
2	Перевірка забезпечення виконання умови $a = M - [M / m_i]\cdot m_i = 0$, для забезпечення максимального значення показника достовірності контролю $P_{дк} = \dfrac{M}{M + N_i \cdot m_i - M} = \dfrac{M}{N_i \cdot m_i} = 1$
3	Для забезпечення мінімальної кількості обладнання системи контролю у СЗК, виходячи з виразу $N_i = \prod_{\substack{K=1;\\ K\neq i.}}^{n+1} m_K \ \ (i=\overline{1,n})$, для впорядкованої $(m_i < m_{i+1})$ СЗК, вибирається максимальна за величиною інформаційна основа m_n.

Рис. 4.15 Метод підвищення достовірності контролю даних у СЗК

Приклад 4.6. З наведеної вище СЗК вибираємо, наприклад, інформаційну основу $m_i = m_1 = 3$ (рис. 4.16). При цьому $N_i = N_1 = M / m_1 = 4\cdot 5\cdot 7 = 140$. У цьому випадку робочий числовий $[0, M_0)$ діапазон СЗК розбивається на інтервали $[j_1 \cdot m_1, (j_1+1)\cdot m_1)$. Для значення $m_1 = 3$ інформаційний числовий інтервал $[0, M)$ розбивається точно на $N_1 = M / m_1 = 140$ відрізків завдовжки три одиниці кожен (див. рис. 4.16). У табл. 4.20 приведено вміст БКН відносно основи $m_1 = 3$.

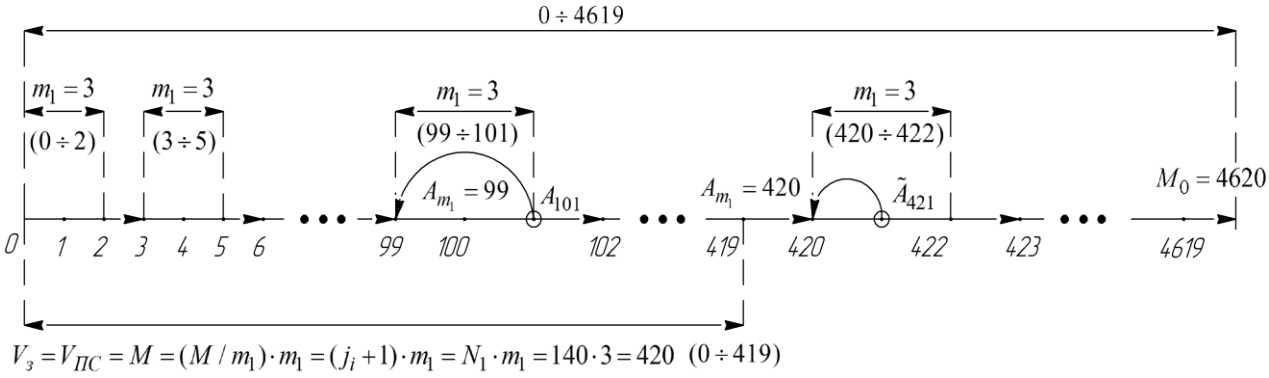

Рис. 4.16 Схема контролю даних у СЗК для $m_i = 3$

Таблиця 4.20

Вміст блоку констант нульовизації для $m_1 = 3$

a_i	Константи				
	$m_1 = 3$	$m_2 = 4$	$m_3 = 5$	$m_4 = 7$	$m_5 = 11$
00	00	00	000	000	0000
01	01	01	001	001	0001
10	10	10	010	010	0010

Нехай необхідно провести контроль числа $A = (01 \| 11 \| 010 \| 000 \| 1001)$. За значенням $a_1 = 01$ у БКН (табл. 4.20) вибираємо константу нульовизації виду $KH_{m_1}^{(A)} = (01 \| 01 \| 001 \| 001 \| 0001)$.

Далі визначаємо $A_{m_1} = A - KH_{m_1}^{(A)} = (00 \| 10 \| 001 \| 110 \| 1000)$. Якщо $A_{m_1} - n_A \cdot m_1 = 426 - 142 \cdot 3 = 0$, то ОК має вигляд $K_{N_i}^{(n_A)} = K_{140}^{(142)} =$ $= \{Z_{139}^{(A)}\ Z_{138}^{(A)} \ldots Z_1^{(A)}\ Z_0^{(A)}\} = \{11...11...11\}$. Оскільки $N_i = 140 < n_A = 142$, тобто помилка у числі A.

Перевірка: $A = 427 > M = 420$. Число $A > M$, тобто воно неправильне (спотворено).

У табл. 4.21 приведені результати розрахунку і порівняльного аналізу достовірності контролю даних у СЗК.

Окрім оперативності контролю даних важливою характеристикою КСКОЦД являється кількість обладнання СК. Відмітимо, що у СЗК кількість обладнання СК в основному залежить від кількості суматорів. Таким чином, кількість обладнання СК залежить від величини значення $N_i = \prod_{\substack{K=1;\\ K\neq i.}}^{n+1} m_K$ ($i = \overline{1,n}$). У цьому випадку, з урахуванням вимоги $a = 0$, та вимоги не зниження оперативності контролю, для мінімізації кількості обладнання СК у СЗК необхідно вибрати максимальний за величиною інформаційний модуль. Для впорядкованої ($m_i < m_{i+1}$) СЗК це буде основа m_n [143].

Таблиця 4.21

Результат розрахунку значень $Д_i$ і $Д_{n+1}$ достовірності контролю у СЗК

№ п.п	m_{n+1}	M	M / m_{n+1}	$]M / m_{n+1}[$	$N_{n+1} =]M / m_{n+1}[\cdot m_{n+1}$	$Д_{n+1}$	$Д_i$, $i = \overline{1,n}$	Виграш у [%]
	1	2	3	4	5	6	7	8
1	11	420	38,2	39	429	0,979	1	2,1
2	13	420	32,3	33	429	0,979	1	2,1
3	17	420	24,7	25	425	0,988	1	1,2
4	19	420	22,1	23	437	0,961	1	3,9
5	23	420	18,2	19	437	0,961	1	3,9
6	29	420	14,4	15	435	0,965	1	3,5

Попередня оцінка кількості обладнання для *l*-байтової розрядної сітки представлення машинного слова КСКОЦД може бути проведена за допомогою значення коефіцієнта ефективності, який представляється у

вигляді:

$$K_{еф}^{(l)} = \frac{N_1}{N_n} = \frac{M / m_1}{M / m_n} = \frac{m_n}{m_1}.$$

Наведемо приклад контролю даних у СЗК для $m_i = m_n$.

Приклад 4.7. Максимальною з інформаційних основ для наведеної вище СЗК являється $m_n = m_4 = 7$. При цьому $N_i = N_4 = M / m_4 = 3 \cdot 4 \cdot 5 = 60$. Робочий числовий $[0, M_0)$ діапазон розбивається на інтервали $[j_4 \cdot m_4, (j_4 + 1) \cdot m_4)$, тобто на $M_0 / m_4 = 4620 / 7 = 660$ відрізків. Для значення $m_4 = 7$ інформаційний $[0, M)$ інтервал розбивається на $N_4 = M / m_4 = 60$ числових відрізків довжиною сім одиниць (див. рис. 4.17). У табл. 4.22 приведений вміст БКН відносно основи $m_4 = 7$.

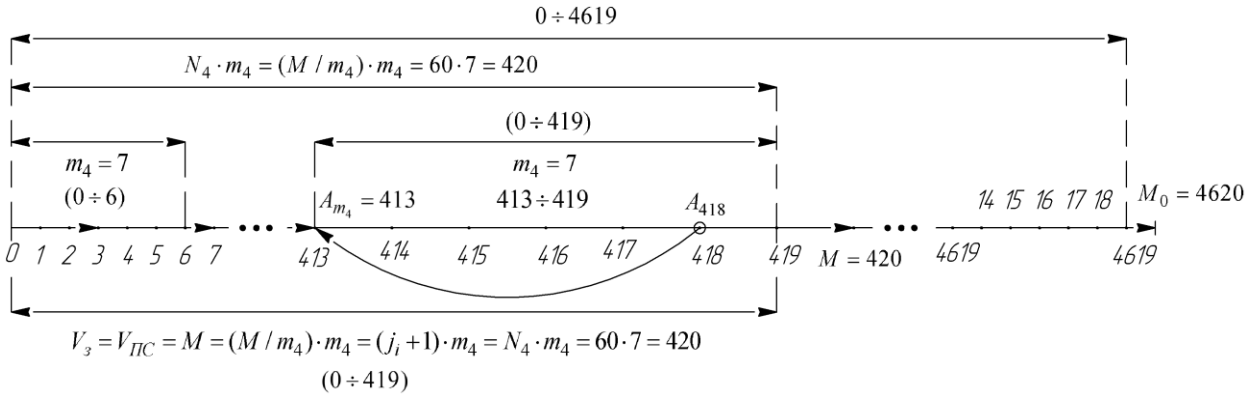

Рис. 4.17 Схема контролю даних у СЗК для $m_i = 7$

Нехай необхідно провести контроль числа $A = (01 \| 11 \| 010 \| 000 \| 1001)$. За значенням $a_4 = 000$ у БКН (табл. 4.21) вибираємо константу $KH_{m_n}^{(A)} = KH_7^{(A)} = (00 \| 00 \| 000 \| 000 \| 0000)$. Далі визначаємо значення $A_{m_n} = A_7 = A - KH_7^{(A)} = (01 \| 11 \| 010 \| 000 \| 1001)$.

Таблиця 4.22

Вміст блоку констант нульовизації для $m_4 = 7$

a_4	Константи				
	$m_1 = 3$	$m_2 = 4$	$m_3 = 5$	$m_4 = 7$	$m_5 = 11$
000	00	00	000	0000	0000
001	01	01	001	001	0001
010	10	10	010	010	0010
011	00	11	011	011	0011
100	01	00	100	100	0100
101	10	01	000	101	0101
110	11	10	001	110	0110

Формулюємо ОК $K_{N_4}^{(n_A)} = K_{60}^{(61)} = \left\{ Z_{59}^{(A)}\, Z_{58}^{(A)} \ldots Z_1^{(A)}\, Z_0^{(A)} \right\} = \{11...11...11\}$.

Виходячи з виду ОК і використовуючи вираз $A_{m_n} - n_A \cdot m_n = 0$, визначаємо, що $n_A = 61$ ($A_{m_n} - n_A \cdot m_n = 427 - 61 \cdot 7 = 0$).

Оскільки $N_4 = 60 < n_A = 61$, то присутня помилка в даних A.

Перевірка: $A = 427 > M = 420$.

У табл. 4.23 приведені розрахункові дані умовної кількості обладнання системи контролю КСКОЦД, що функціонує у СЗК, і дані порівняльного аналізу скорочення кількості обладнання СК для $m_i = m_n$.

Таким чином, розроблений метод підвищення достовірності контролю даних у СЗК, що заснований на використанні ПОНКС n_A, який є однією з характеристик ОК. При цьому вибирається модуль m_i, що визначає номер числового інтервалу знаходження НКС, з сукупності n можливих інформаційних основ СЗК. Застосування цього методу забезпечує отримання достовірного результату, до одиниці довжини числового інтервалу попадання неправильного числа, результату контролю даних у СЗК.

Таблиця 4.23

Порівняльні дані кількості обладнання СК КСКОЦД

Розрядна сітка l-байтової КСКОЦД у СЗК $(\rho,\ n,\ k)$	Інформаційні основи СЗК $m_i\ (i=\overline{1,n})$	Контрольні m_{n+1} основи СЗК	min інформаційна m_1 основа СЗК	max інформаційна m_n основа СЗК	$K_{еф.}^{(l)}$
$l=1$ $(\rho=8,$ $n=4,$ $k=3)$	$m_1=3,\ m_2=4,\ m_3=5,$ $m_4=7$	$m_5=11$	$m_1=3$	$m_4=7$	2,3
$l=2$ $(\rho=16,$ $n=6,$ $k=4)$	$m_1=2,\ m_2=5,\ m_3=7,$ $m_4=9,\ m_5=11,\ m_6=13$	$m_7=17$	$m_1=2$	$m_6=13$	6,5
$l=3$ $(\rho=24,$ $n=8,$ $k=5)$	$m_1=3,\ m_2=4,\ m_3=5,$ $m_4=7,\ m_5=11,\ m_6=13,$ $m_7=17,\ m_8=19$	$m_9=23$	$m_1=3$	$m_8=19$	6,3
$l=4$ $(\rho=32,$ $n=10,$ $k=5)$	$m_1=2,\ m_2=3,\ m_3=5,$ $m_4=7,\ m_4=11,\ m_5=13,$ $m_6=17,\ m_7=19,$ $m_9=23,\ m_{10}=29$	$m_{11}=31$	$m_1=2$	$m_{10}=29$	14,5
$l=8$ $(\rho=64,$ $n=16,$ $k=6)$	$m_1=3,\ m_2=4,\ m_3=5,$ $m_4=7,\ m_5=11,\ m_6=13,$ $m_7=17,\ m_8=19,$ $m_9=23,\ m_{10}=29,$ $m_{11}=31,\ m_{12}=37,$ $m_{13}=41,\ m_{14}=43,$ $m_{15}=47,\ m_{16}=53$	$m_{17}=59$	$m_1=3$	$m_{16}=53$	17,6

Розрахункові дані і порівняльний аналіз достовірності контролю даних та кількості обладнання СК у СЗК показав, що з ростом розрядної сітки оброблюваних даних у КСКОЦД, ефективність непозиційного кодування у СЗК істотно зростає [144-147].

Висновки до розділу 4

У четвертому розділі вирішені **четверта**, **п'ята і шоста** задачі досліджень і отримані **перший, другий та третій** наукові результати.

1. У розділі досліджені методи контролю даних у СЗК, що засновані на принципі нульовизації. На основі результатів аналізу існуючих методів контролю даних у СЗК, у розділі розроблений метод контролю даних, заснований на принципі паралельної нульовизації з попереднім аналізом подальших симетричних залишків числа, що контролюється. Цей метод, у порівнянні з існуючими методами, що засновані на принципі нульовизації, дозволяє, залежно від довжини машинного слова КСКОЦД, на 25-30 % підвищити оперативність контролю даних. На основі розробленого методу контролю даних, заснованого на принципі паралельної нульовизації з попереднім аналізом подальших симетричних залишків числа, що контролюється, синтезований алгоритм контролю помилок на основі, якого отримані пристрої для його реалізації. На цей пристрій отримані патенти України (Пат. 79673 Україна, МПК G 06 F 11/08 (2006.01); Пат. 105455 Україна, МПК G06F 11/08 (2006.01); Пат. 105742 Україна, МПК G06F 11/08 (2006.01).

2. У розділі 4 розроблений метод контролю даних у СЗК, який заснований на використанні сформованої позиційної ознаки НКС. Цей метод, у порівнянні з існуючими методами дозволяє до 60 % підвищити оперативність контролю даних представлених у СЗК.

3. У цьому розділі розроблений метод підвищення достовірності контролю даних, які представлені у СЗК. Цей метод заснований на використанні позиційної ознаки НКС. Використання цього методу забезпечує отримання достовірного результату контролю з точністю до одиниці довжини числового інтервалу.

Основні положення цього розділу викладені у публікаціях автора [126-132, 136-140, 143].

РОЗДІЛ 5. МЕТОДИ ОПЕРАТИВНОГО ДІАГНОСТУВАННЯ ПОМИЛОК У СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ

5.1 Теоретичні основи діагностики даних, що представлені у СЗК

У загальному випадку під діагностикою даних у СЗК будемо розуміти процес визначення спотворених залишків у надмірній НКС, що має вид $A_{СЗК} = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n \| ... \| a_{n+k})$, де n і k – кількість, відповідно, інформаційних і контрольних основ m_i $(\mathrm{i} = \overline{1, n+k})$ у впорядкованій $(m_i < m_{i+1})$ СЗК. Діагноста НКС проводиться після контролю даних, для подальшої можливої корекції помилок.

Розглянемо ряд наукових тверджень, результати доказів яких можна покласти в основу методів діагностики помилок даних, що представлені у СЗК [148-150]. Нагадаємо, що надалі передбачається тільки одноразова (в одному залишку a_i, $(i = \overline{1, n+1})$ числа $A = (a_1 \| a_2 \| ... \| a_n \| a_{n+1})$, що представлене у СЗК) помилка.

Твердження 5.1. Нехай задана впорядкована $(m_i < m_{i+1},\ i = \overline{1, n})$ система основ (модулів) СЗК з n інформаційними і одним $m_к = m_{n+1}$ контрольним основами, і нехай число $A = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n \| a_{n+1})$ неспотворене (правильне), тобто $A < M_0 / m_{n+1}$ де $M_0 = M \cdot m_{n+1}$ та $M = \prod_{i=1}^{n} m_i$. Тоді величина A не зміниться, якщо це число будемо представляти у СЗК з якої вилучена одна основа m_i, тобто, якщо у зображенні числа A прибрати залишок a_i. Отримане таким чином число $A_i = (a_1 \| a_2 \| ... \| a_{i-1} \| a_{i+1} \| ... \| a_n \| a_{n+1})$ будемо називати проекцією числа A по модулю m_i.

Твердження 5.2. Якщо у впорядкованій системі основ СЗК задано правильне число A, то проекції A_i $(i = \overline{1, 1+n})$ цього числа рівні між собою,

тобто $A = A_1 = A_2 = ... = A_i = ... = A_n = A_{n+1} < M_0 / m_{n+1}$. Дійсно, для правильного числа A має місце співвідношення $A < M_0 / m_{n+1} < M_0 / m_k < ... < M_0 / m_i < ... < M_0 / m_1$. Відповідно до результатів твердження 5.1 маємо що $A = A_i$.

Твердження 5.3. Нехай для впорядкованої системи основ СЗК усі можливі проекції $A_i = (a_1 \| a_2 \| ... \| a_{i-1} \| a_{i+1} \| ... \| a_n \| a_{n+1})$ A_i $(i = \overline{1, n+1})$ числа $A = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n \| a_{n+1})$ співпадають. У цьому випадку число $A = (a_1 \| a_2 \| ... \| a_n \| a_{n+1})$ є правильним.

Покажемо це. Припустимо, що число $A = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n \| a_{n+1})$ неправильне за рахунок спотворення залишку a_i по модулю m_i. Замінимо в числі A спотворений залишок a_i на правильний $\tilde{a}_i$. У цьому випадку отримали правильне число $\tilde{A} = (a_1 \| a_2 \| ... \| \tilde{a}_i \| ... \| a_n \| a_{n+1})$. Тоді відповідно до результату твердження 5.2 маємо $\tilde{A}_1 = \tilde{A}_2 = ... = \tilde{A}_i = ... = \tilde{A}_n = \tilde{A}_{n+1}$. З іншого боку $A_i = (a_1 \| a_2 \| ... \| a_{i-1} \| a_{i+1} \| ... \| a_n \| a_{n+1})$ і одночасно $\tilde{A}_i = (a_1 \| a_2 \| ... \| a_{i-1} \| \| a_{i+1} \| ... \| a_n \| a_{n+1})$, тобто $A_i = \tilde{A}_i$. У цьому випадку повинне виконуватись наступне співвідношення $A = A_1 = \tilde{A}_1 = A_2 = \tilde{A}_2 = ... = A_n = \tilde{A}_n = A_{n+1} = \tilde{A}_{n+1}$. Проте по умові твердження 5.3 проекція A_j $(i \neq j)$ числа A відрізняється від проекції A_i значенням залишку a_i по основі m_i. Внаслідок цього $A_i \neq A_j$, що суперечить умові неправильності числа A.

Твердження 5.4. Якщо у впорядкованій системі основ СЗК проекція $A_i = (a_1 \| a_2 \| ... \| a_{i-1} \| a_{i+1} \| ... \| a_n \| a_{n+1})$ числа $A = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| \| a_{i+1} \| ... \| a_n \| a_{n+1})$ задовольняє умові $A_i \geq M_0 / m_{n+1}$, то у цьому випадку вважається, що залишок a_i числа A по модулю m_i не спотворений. Відмітимо ще раз, що передбачається тільки одноразова помилка. Дійсно, якщо залишок a_i числа A по модулю m_i спотворений, то проекція A_i, що складена з неспотворених a_j $(j = \overline{1, n+1}$ та $i \neq j)$ залишків, має бути правильним

числом. Проте, за умовою $A_i \geq M_0 / m_{n+1}$ – неправильне число, що суперечить умові твердження 5.4. Окрім цього, відмітимо, що, якщо усі значення $A_i \geq M_0 / m_{n+1}$ $(i = \overline{1,n})$, то спотворений залишок a_{n+1}.

На основі результатів вищевикладених наукових тверджень розглянемо метод контролю і метод діагностики даних, представлених у СЗК. Нехай дано число, що необхідно перевірити $A = (a_1 \| a_2 \| ... \| a_i \| ... \| a_n \| a_{n+1})$ у СЗК з інформаційними m_i $(i = \overline{1,n})$ і однією контрольною $m_k = m_{n+1}$ основами. Необхідно, по-перше, провести контроль (визначити правильність) числа *A*, і, по-друге, провести діагностику залишків a_i $(i = \overline{1,n+1})$ числа *A,* тобто визначити спотворені (чи неспотворені) залишки.

На підставі результатів доказів тверджень 5.3 та 5.4 на рис. 5.1 представлений метод діагностики даних у СЗК.

Контроль і діагностика даних проводяться послідовно у два етапи.

I. Перший етап. Метод контролю даних $A = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n \| a_{n+1})$.

1.1. Визначити значення $B_i (i = \overline{1,n+1})$ ортогональних базисів для повної системи основ $\{m_i\}$ СЗК.

1.2. Використовуючи систему ортогональних базисів B_i, вихідне *A* число у СЗК перевести у ПСЧ по формулі : $A_{ПСЧ} = (\sum_{i=1}^{n+1} a_i \cdot B_i) \bmod M_0$.

1.3. Провести операції позиційного порівняння значень $A_{ПСЧ}$ і *M*. Якщо результат порівняння показав, що $A_{ПСЧ} < M$, то число *A* правильне. Якщо $A_{ПСЧ} \geq M$, то вважається, що число $\tilde{A}$ неправильне, у випадку якщо спотворений тільки один із залишків a_i числа *A*.

II. Другий етап. Метод діагностики залишків a_i $(i = \overline{1,n+1})$ кодової структури $\tilde{A}$ даних, що заснований на використанні отриманих результатів наступного твердження.

1	Задати СЗК, за допомогою основ $\{m_i\}$, $i=\overline{1,n+1}$.
2	Визначення констант $M=\prod_{i=1}^{n} m_i$, $M_0=\prod_{i=1}^{n+1} m_i$, $M_i=\prod_{\substack{k=1 \\ k\neq i}}^{n+1} m_k$.
3	Визначення ортогональних базисів $B_i=\bar{m}_i\cdot M_0 / m_i=\bar{m}_i\cdot M_i$.
4	Визначення частинних $B_{ij}=M_i\cdot\bar{m}_{ij}/m_i$ ортогональних базисів.
5	Визначення значень $\tilde{A}_{\substack{j\,ПСЧ \\ j=const}}=\left(\sum_{i=1}^{n} a_i\cdot B_{ij}\right)\bmod M_j$ проекцій числа $\tilde{A}_j$ числа A у СЗК, $j=(\overline{1,n+1})$, $i=\overline{(1,n)}$.
6	Порівняння отриманих $\tilde{A}_{j\ ПСЧ}$ проекцій з модулем M.
7	Визначення неспотворених a_i залишків числа A у СЗК.

Рис. 5.1 Метод діагностики даних у СЗК

Твердження 5.5 Нехай у впорядкованій ($m_i<m_{i+1}$, $i=\overline{1,n}$) СЗК з n інформаційними та однією контрольною $m_k=m_{n+1}$ основами число

$A=(a_1 \| a_2 \| ... \| a_i \| ... \| a_n \| a_{n+1})$ задовольняє наступній умові $M = M_0 / m_{n+1} = M_{n+1} < A < M_i$, де: $M = \prod_{i=1}^{n} m_i$; $M_0 = M \cdot m_{n+1}$; $M_i = \prod_{\substack{\kappa=1,\\ \kappa \neq i.}}^{n+1} m_\kappa$. Тоді залишки a_z $(z = \overline{1,i})$ числа A не спотворені (правильні), якщо можлива тільки одноразова (у одному залишку a_i) помилка.

Покажемо це. Спочатку методом від протилежного встановимо, що залишок a_i правильний. Припустимо, що залишок a_i спотворений, а залишок $\tilde{a}_i$ правильний. У цьому випадку правильне число $\tilde{A}$ представится у вигляді $\tilde{A}=(a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n \| a_{n+1})$. З урахуванням того, що спотворений залишок a_i спотвореного числа A представимо у вигляді $a_i = \tilde{a}_i + \Delta a_i$ (вважається, що помилка Δa_i носить адитивний характер, тобто $A = \tilde{A} + \Delta A$), то число $\tilde{A}$ буде мати вигляд $\tilde{A} = A - \Delta A$, або

$$\tilde{A} = A - (a_i - \tilde{a}_i) \cdot B_i \qquad (5.1)$$

оскільки $\Delta a_i = a_i - \tilde{a}_i$.

Використовуючи ортогональні базиси для даної СЗК (де $\bar{m}_i$ – вага i-го ортогонального базису B_i) по формулі (4.1) визначимо чисельне значення числа $\tilde{A}$ наступним чином:

$$\begin{aligned}
&\tilde{A} = A - \Delta A,\\
&\tilde{A} = A + (\tilde{a}_i - a_i) \cdot B_i,\\
&\tilde{A} = A + (\tilde{a}_i - a_i) \cdot m_i \cdot M_i,\\
&\tilde{A} = A + (\tilde{a}_i - a_i) \cdot m_i \cdot M_0 / m_i. \qquad (5.2)
\end{aligned}$$

Оскільки значення $(\tilde{a}_i - a_i) \bmod m_i$ може змінюватись від 0 і до величини $m_i - 1$, то максимально можливе значення величини

$[(\tilde{a}_i - a_i) \cdot m_i \cdot M_0 / m_i] \bmod M_0$ буде дорівнювати $(m_i - 1) \cdot M_0 / m_i$. У цьому випадку максимальне значення виразу (5.2) має вигляд:

$$\{[(\tilde{a}_i - a_i) \cdot \bar{m}_i \cdot M_0 / m_i] \bmod M_0\} = (m_i - 1) \cdot M_0 / m_i . \quad (5.3)$$

На підставі вираження (5.3) і враховуючи також умову твердження про те, що дане число лежить у межах $M < \tilde{A} < M_i$ можна записати, що

$$\tilde{A} < M_0 / m_i + (m_i - 1) \cdot M_0 / m_i = M_0 . \quad (5.4)$$

Число $\tilde{A}$ буде правильним (що лежить в інформаційному числовому [0, M) інтервалі) тільки у тому випадку, якщо б від додавання величини $(\tilde{a}_i - a_i) \cdot B_i$ (див. вираз (5.2)) воно стало б більше ніж величина M_0. Проте, виходячи з виразу (5.4) цього досягти не можливо шляхом виправлення спотвореного залишку a_i числа A. У цьому випадку залишок a_i правильний, тобто вихідне припущення про те, що цей залишок спотворений невірно. Оскільки за умовою твердження виконується нерівність $A < M_i$, то і тим більш виконуються наступні нерівності:

$$A < M_i < M_{i-1} < ... < M_2 < M_1 . \quad (5.5)$$

Нерівності (5.5) підтверджують умови твердження, що залишки a_z $(z = \overline{1,i})$ числа $A = (a_1 \,||\, a_2 \,||\, ... \,||\, a_{i-1} \,||\, a_i \,||\, a_{i+1} \,||\, ... \,||\, a_n \,||\, a_{n+1})$ правильні [151-154].

Розглянемо приклад 5.1 застосування методу контролю і діагностики у СЗК, як вже вказувалося у главі 4, для однобайтового (l = 1) машинного слова (8 двійкових розрядів) КСКОЦД.

При цьому повна СЗК з однією контрольною основою задана

інформаційними $m_1 = 3,\ m_2 = 4,\ m_3 = 5,\ m_4 = 7$ і контрольною $m_k = m_{n+1} = 11$ основами.

Таблиця 5.1

Набір частинних основ СЗК

i / j	1	2	• • •	$j-1$	j	• • •	$n-2$	$n-1$	n	$M_j = \prod_{\substack{\kappa=1,\\ \kappa\neq j.}}^{n+1} m_\kappa$
j	$m_1^{(j)}$	$m_2^{(j)}$	• • •	$m_{j-1}^{(j)}$	$m_{j+1}^{(j)}$	• • •	$m_{n-2}^{(j)}$	$m_{n-1}^{(j)}$	$m_n^{(j)}$	
1	$m_1^{(1)} = m_2$	$m_2^{(1)} = m_3$	• • •	$m_{j-1}^{(1)} = m_{j-1}$	$m_j^{(1)} = m_{j+1}$	• • •	$m_{n-2}^{(1)} = m_{n-1}$	$m_{n-1}^{(1)} = m_n$	$m_n^{(1)} = m_{n+1}$	$M_1 = \prod_{k=2.}^{n+1} m_k$
2	$m_1^{(2)} = m_1$	$m_2^{(2)} = m_3$	• • •	$m_{j-1}^{(2)} = m_j$	$m_j^{(2)} = m_{j+1}$	• • •	$m_{n-2}^{(2)} = m_{n-1}$	$m_{n-1}^{(2)} = m_n$	$m_n^{(2)} = m_{n+1}$	$M_2 = \prod_{\substack{k=1,\\ k\neq 2.}}^{n+1} m_k$
• • •										
j	$m_1^{(j)} = m_1$	$m_2^{(j)} = m_2$	• • •	$m_{j-1}^{(j)} = m_{j-1}$	$m_j^{(j)} = m_{j+1}$	• • •	$m_{n-2}^{(j)} = m_{n-1}$	$m_{n-1}^{(j)} = m_n$	$m_n^{(j)} = m_{n+1}$	M_j
• • •										
n	$m_1^{(n)} = m_1$	$m_2^{(n)} = m_2$	• • •	$m_{j-1}^{(n)} = m_{j-1}$	$m_j^{(n)} = m_j$	• • •	$m_{n-2}^{(n)} = m_{n-2}$	$m_{n-1}^{(n)} = m_{n-1}$	$m_n^{(n)} = m_{n+1}$	$M_n = \prod_{\substack{k=1,\\ k\neq n.}}^{n+1} m_k$
$n+1$	$m_1^{(n+1)} = m_1$	$m_2^{(n+1)} = m_2$	• • •	$m_{j-1}^{(n+1)} = m_{j-1}$	$m_j^{(n+1)} = m_j$	• • •	$m_{n-2}^{(n+1)} = m_{n-2}$	$m_{n-1}^{(n+1)} = m_{n-1}$	$m_n^{(n+1)} = m_n$	$M_{n+1} = \prod_{\kappa=1}^{n} m_\kappa$

Таблиця 5.2

Набір частинних робочих основ СЗК (*l* = 1)

i / j	m_1	m_2	m_3	m_4	M_j
1	4	5	7	11	1540
2	3	5	7	11	1155
3	3	4	7	11	924
4	3	4	5	11	660
5	3	4	5	7	420

В цьому випадку повний (робочий) $[0, M_0)$ та інформаційний $[0, M)$ числові діапазони чисел визначаються, відповідно, як [0, 4620) та [0, 420). Усі можливі частинні набори основ СЗК представлені у табл. 5.1 та 5.2 де $M_j = M_0 / m_j$. У табл. 5.3 представлені усі можливі числові діапазони $[jM_1, (j+1)\cdot M]$ попадання неправильного $\tilde{A}$ числа для $l = 1$, а у табл. 5.4 значення можливих рангів $r \cdot M_0$ числа A [143, 155-157].

Таблиця 5.3

Числові діапазони

j	$[jM, (j+1)\cdot M)$	$\gamma_{n+1}^{(j)} = \gamma_5^{(j)}$
0	[0, 420)	$\gamma_5^{(0)} = 0$
1	[420, 840)	$\gamma_5^{(1)} = 2$
2	[840, 1260)	$\gamma_5^{(2)} = 4$
3	[1260, 1680)	$\gamma_5^{(3)} = 6$
4	[1680, 2100)	$\gamma_5^{(4)} = 8$
5	[2100, 2520)	$\gamma_5^{(5)} = 10$
6	[2520, 2940)	$\gamma_5^{(6)} = 1$
7	[2940, 3360)	$\gamma_5^{(7)} = 3$
8	[3360, 3780)	$\gamma_5^{(8)} = 5$
9	[3780, 4200)	$\gamma_5^{(9)} = 7$
10	[4200, 4620)	$\gamma_5^{(10)} = 9$

Таблиця 5.4

Значення рангів *r* числа *A* для діапазону [0, 4620)

r	$r \cdot M_0 = r \cdot 4620$
1	4620
2	9240
3	13860
4	18480
5	23100
6	27720
7	32340
8	36960
9	41580
10	46200

Приклад 5.1. Нехай у процесі передачі або обробки даних замість правильного $A = (1\,||\,0\,||\,0\,||\,2\,||\,1)$ результату операції ($100 < M = 420$) отримано число виду $\tilde{A} = (0||0||0||2||1)$, де $\tilde{A}_{ПСЧ} = 3180 > M = 420$. Необхідно провести контроль правильності числа $\tilde{A}$ і діагностику його залишків a_i $(i = \overline{1, 5})$.

I. Перший етап.

1.1 Визначаємо усі значення $B_i\,(i=\overline{1,5})$ ортогональних базисів для повної системи основ $m_1=3$, $m_2=4$, $m_3=5$, $m_4=7$ та $m_5=11$ СЗК.

1.2. Використовуючи представлені дані, по відомій формулі, визначаємо значення $\tilde{A}_{ПСС}=(0\cdot 1540+0\cdot 3465+0\cdot 3696+2\cdot 2640+$ $+1\cdot 2520)\bmod 4620=3180(\bmod 4620)$.

1.3. Проводимо порівняння отриманого числа $A_{ПСЧ}$ і значення $M=420$. Так, як $\tilde{A}_{ПСЧ}>M=420$, то робиться висновок, що отриманий $\tilde{A}$ результат спотворений по якомусь одному із залишків a_i правильного числа $A=(1\|0\|0\|2\|1)$.

II. Другий етап.

2.1. Визначимо значення частинних B_{ij} ортогональних базисів для кожного з 5 наборів (табл. 5.5) основ СЗК. Так, для $i=4$ і $j=5$ маємо:

$$\begin{cases} B_{1j}=(1,0,0,0), \\ B_{2j}=(0,1,0,0), \\ B_{3j}=(0,0,1,0), \\ B_{4j}=(0,0,0,1). \end{cases}$$

Таблиця 5.5

Частинні ортогональні базиси B_{ij} для $l=1$

Bij / i \ j	1	2	3	4
1	385	616	1100	980
2	385	231	330	210
3	616	693	792	672
4	220	165	396	540
5	280	105	336	120

У загальному випадку значення B_{ij} частинних ортогональних базисів визначається виходячи з наступного порівняння

$$B_{ij} = \frac{M_i \cdot \bar{m}_{ij}}{m_i} \equiv 1(\mathrm{mod}\, m_i), \qquad (5.6)$$

де $\bar{m}_{ij} \equiv \overline{1, m_i - 1}$ – вага ортогонального базису B_{ij}.

2.1.1. Визначимо значення B_{i1} для першого (i = 1) набору основ $m_1 = 4$, $m_2 = 5$, $m_3 = 7$ та $m_4 = 11$ (табл. 5.2). У цьому випадку $M_1 = \prod_{i=1}^{4} m_i = 1540$ (M = 420). Визначаємо значення базисів B_{i1} виходячи із співвідношення (5.6).

Визначаємо значення B_{11}. У даному випадку використовуємо m_1 = 4. При цьому M_1/m_1 = 1540 / 4 = 385; $\bar{m}_{11} \equiv \overline{1, m_1 - 1} = \overline{1, 3}$. Складемо можливі значення для i = 1, тобто $\bar{m}_{11} \cdot M_1 / m_1$:

$$\begin{cases} 1 \cdot 385 \equiv 1(\mathrm{mod}\, 4), \\ 2 \cdot 385 \equiv 2(\mathrm{mod}\, 4), \\ 3 \cdot 385 \equiv 3(\mathrm{mod}\, 4). \end{cases}$$

У цьому випадку $B_{11} = 1 \cdot 385 = 385$.

Визначимо значення B_{21}. У даному випадку $m_2 = 5$, $M_1 / m_2 = 1540 / 5 = 308$, $\bar{m}_{21} = \overline{1, m_2 - 1} = \overline{1, 4}$.

Складаємо сукупність порівнянь :

$$\begin{cases} 1 \cdot 308 \equiv 3(\mathrm{mod}\, 5), \\ 2 \cdot 308 \equiv 1(\mathrm{mod}\, 5), \end{cases} \qquad \begin{cases} 3 \cdot 308 \equiv 4(\mathrm{mod}\, 5), \\ 4 \cdot 308 \equiv 2(\mathrm{mod}\, 5). \end{cases}$$

Маємо, що $B_{21} = 2 \cdot 308 = 616$.

Визначимо значення B_{31}. Маємо $m_3 = 7$, $M_1 / m_3 = 1540 / 7 = 220$, $\bar{m}_{31} \equiv \overline{1, m_3 - 1} = \overline{1, 6}$. Тоді

$$\begin{cases} 1 \cdot 220 \equiv 3 (\mathrm{mod}\, 7), \\ 2 \cdot 220 \equiv 6 (\mathrm{mod}\, 7), \\ 3 \cdot 220 \equiv 2 (\mathrm{mod}\, 7), \end{cases} \qquad \begin{cases} 4 \cdot 220 \equiv 5 (\mathrm{mod}\, 7), \\ 5 \cdot 220 \equiv 1 (\mathrm{mod}\, 7), \\ 6 \cdot 220 \equiv 4 (\mathrm{mod}\, 7). \end{cases}$$

В цьому випадку $B_{31} = 5 \cdot 220 = 1100$.

Визначаємо значення B_{41}. В цьому випадку $m_4 = 11$, $M_1 / m_4 = 1540 / 11 = 140$, $\bar{m}_{41} \equiv \overline{1, m_4 - 1} = \overline{1, 10}$. Маємо

$$\begin{cases} 1 \cdot 140 \equiv 8 (\mathrm{mod} 11), \\ 2 \cdot 140 \equiv 5 (\mathrm{mod} 11), \\ 3 \cdot 140 \equiv 2 (\mathrm{mod} 11), \\ 4 \cdot 140 \equiv 10 (\mathrm{mod} 11), \\ 5 \cdot 140 \equiv 7 (\mathrm{mod} 11), \end{cases} \qquad \begin{cases} 6 \cdot 140 \equiv 4 (\mathrm{mod} 11), \\ 7 \cdot 140 \equiv 1 (\mathrm{mod} 11), \\ 8 \cdot 140 \equiv 9 (\mathrm{mod} 11), \\ 9 \cdot 140 \equiv 6 (\mathrm{mod} 11), \\ 10 \cdot 140 \equiv 3 (\mathrm{mod} 11). \end{cases}$$

В цьому випадку $B_{41} = 7 \cdot 140 = 980$.

2.1.2. Визначаємо значення B_{i2} для другого (j = 2) набору основ $m_1 = 3$, $m_2 = 5$, $m_3 = 7$ та $m_4 = 11$ СЗК (табл. 5.2). У цьому випадку $M_2 = \prod_{i=1}^{4} m_i = 1155$ ($M = 420$).

Визначаємо значення B_{12}. У цьому випадку $m_1 = 3$, $M_2 / m_1 = 1155 / 3 = 385$, $\bar{m}_{12} \equiv \overline{1, m_1 - 1} = \overline{1, 2}$.

$$\begin{cases} 1 \cdot 385 \equiv 1 (\mathrm{mod}\, 3), \\ 2 \cdot 385 \equiv 2 (\mathrm{mod}\, 3). \end{cases}$$

В цьому випадку $B_{12} = 1 \cdot 385 = 385$.

Визначимо B_{22}. Маємо $m_2 = 5$, $M_2 / m_2 = 1155/5 = 231$, $\bar{m}_{22} \equiv \overline{1, m_2 - 1} = \overline{1, 4}$.

$$\begin{cases} 1 \cdot 231 \equiv 1 (\mathrm{mod}\, 5), \\ 2 \cdot 231 \equiv 2 (\mathrm{mod}\, 5), \end{cases} \qquad \begin{cases} 3 \cdot 231 \equiv 3 (\mathrm{mod}\, 5), \\ 4 \cdot 231 \equiv 4 (\mathrm{mod}\, 5). \end{cases}$$

Тоді $B_{22} = 1 \cdot 231 = 231$.

Визначимо B_{32}. Маємо $m_3 = 7$, $M_2 / m_3 = 1155/7 = 165$, $\bar{m}_{32} \equiv \overline{1, m_3 - 1} = \overline{1, 6}$.

$$\begin{cases} 1 \cdot 165 \equiv 4 (\mathrm{mod}\, 7), \\ 2 \cdot 165 \equiv 1 (\mathrm{mod}\, 7), \\ 3 \cdot 165 \equiv 5 (\mathrm{mod}\, 7), \end{cases} \qquad \begin{cases} 4 \cdot 165 \equiv 2 (\mathrm{mod}\, 7), \\ 5 \cdot 165 \equiv 6 (\mathrm{mod}\, 7), \\ 6 \cdot 165 \equiv 3 (\mathrm{mod}\, 7). \end{cases}$$

Тоді $B_{32} = 2 \cdot 165 = 330$.

Визначимо B_{42}. Маємо $m_4 = 11$, $M_2 / m_4 = 1155/11 = 105$, $\bar{m}_{42} \equiv \overline{1, m_4 - 1} = \overline{1, 10}$.

$$\begin{cases} 1 \cdot 105 \equiv 6 (\mathrm{mod} 11), \\ 2 \cdot 105 \equiv 1 (\mathrm{mod} 11), \\ 3 \cdot 105 \equiv 7 (\mathrm{mod} 11), \\ 4 \cdot 105 \equiv 2 (\mathrm{mod} 11), \\ 5 \cdot 105 \equiv 8 (\mathrm{mod} 11), \end{cases} \qquad \begin{cases} 6 \cdot 105 \equiv 3 (\mathrm{mod} 11), \\ 7 \cdot 105 \equiv 9 (\mathrm{mod} 11), \\ 8 \cdot 105 \equiv 4 (\mathrm{mod} 11), \\ 9 \cdot 105 \equiv 10 (\mathrm{mod} 11), \\ 10 \cdot 105 \equiv 2 (\mathrm{mod} 11). \end{cases}$$

Тоді $B_{42} = 2 \cdot 105 = 210$.

2.1.3. Визначимо значення B_{i3} для третього (j = 3) набору основ $m_1 = 3$,

$m_2 = 4$, $m_3 = 7$ та $m_4 = 11$ СЗК (табл. 5.2). У цьому випадку $M_3 = \prod_{i=1}^{4} m_i = 924$ ($M = 420$).

Визначимо B_{13}. Маємо $m_1 = 3$, $M_3 / m_1 = 924 / 3 = 308$, $\overline{m}_{13} \equiv \overline{1, m_1 - 1} = \overline{1, 2}$.

$$\begin{cases} 1 \cdot 308 \equiv 2 (\mathrm{mod}\, 3), \\ 2 \cdot 308 \equiv 1 (\mathrm{mod}\, 3). \end{cases}$$

Тоді $B_{13} = 2 \cdot 308 = 616$.

Визначимо B_{23}. Маємо $m_2 = 4$, $M_3 / m_2 = 924 / 4 = 231$, $\overline{m}_{23} \equiv \overline{1, m_2 - 1} = \overline{1, 3}$.

$$\begin{cases} 1 \cdot 231 \equiv 3 (\mathrm{mod}\, 4), \\ 2 \cdot 231 \equiv 2 (\mathrm{mod}\, 4), \\ 3 \cdot 231 \equiv 1 (\mathrm{mod}\, 4). \end{cases}$$

В цьому випадку $B_{23} = 3 \cdot 231 = 693$.

Визначимо B_{33}. Маємо $m_3 = 7$, $M_3 / m_3 = 924 / 7 = 132$, $\overline{m}_{33} \equiv \overline{1, m_3 - 1} = \overline{1, 6}$.

$$\begin{cases} 1 \cdot 132 \equiv 6 (\mathrm{mod}\, 7), \\ 2 \cdot 132 \equiv 5 (\mathrm{mod}\, 7), \\ 3 \cdot 132 \equiv 4 (\mathrm{mod}\, 7), \end{cases} \qquad \begin{cases} 4 \cdot 132 \equiv 3 (\mathrm{mod}\, 7), \\ 5 \cdot 132 \equiv 2 (\mathrm{mod}\, 7), \\ 6 \cdot 132 \equiv 1 (\mathrm{mod}\, 7). \end{cases}$$

У цьому випадку $B_{33} = 6 \cdot 132 = 792$.

Визначимо B_{43}. Маємо $m_4 = 11$, $M_3 / m_3 = 924 / 11 = 84$, $\overline{m}_{43} \equiv \overline{1,\ m_4 - 1} = \overline{1, 10}$.

$$\begin{cases} 1\cdot 84 \equiv 7(\mathrm{mod}11), \\ 2\cdot 84 \equiv 3(\mathrm{mod}11), \\ 3\cdot 84 \equiv 10\,\mathrm{mod}11), \\ 4\cdot 84 \equiv 6(\mathrm{mod}11), \\ 5\cdot 84 \equiv 3(\mathrm{mod}11), \end{cases} \qquad \begin{cases} 6\cdot 84 \equiv 9(\mathrm{mod}11), \\ 7\cdot 84 \equiv 5(\mathrm{mod}11), \\ 8\cdot 84 \equiv 1(\mathrm{mod}11), \\ 9\cdot 84 \equiv 8(\mathrm{mod}11), \\ 10\cdot 84 \equiv 4(\mathrm{mod}11). \end{cases}$$

В цьому випадку $B_{43} = 8\cdot 84 = 672$.

2.1.4. Визначимо значення B_{i4} для четвертого ($j = 4$) набору основ $m_1 = 3$, $m_2 = 4$, $m_3 = 5$, $m_4 = 11$ СЗК (табл. 5.2). У цьому випадку $M_4 = \prod_{i=1}^{4} m_i = 660$ $(M = 420)$.

Визначимо B_{14}. Маємо $m_1 = 11$, $M_4 / m_1 = 660/3 = 220$, $\overline{m}_{14} \equiv \overline{1, m_1 - 1} = \overline{1, 2}$.

$$\begin{cases} 1\cdot 220 \equiv 1(\mathrm{mod}\,3), \\ 2\cdot 220 \equiv 2(\mathrm{mod}\,3). \end{cases}$$

У цьому випадку $B_{14} = 1\cdot 220 = 220$.

Визначимо B_{24}. Маємо $m_2 = 4$, $M_4 / m_2 = 660/4 = 165$, $\overline{m}_{24} \equiv \overline{1, m_2 - 1} = \overline{1, 3}$.

$$\begin{cases} 1\cdot 165 \equiv 1(\mathrm{mod}\,4), \\ 2\cdot 165 \equiv 2(\mathrm{mod}\,4), \\ 3\cdot 165 \equiv 3(\mathrm{mod}\,4). \end{cases}$$

У цьому випадку $B_{24} = 1\cdot 165 = 165$.

Визначимо B_{34}. Маємо $m_3 = 5$, $M_4 / m_3 = 660/5 = 132$, $\overline{m}_{34} \equiv \overline{1, m_3 - 1} = \overline{1, 4}$.

$$\begin{cases} 1\cdot 132 \equiv 2(\mathrm{mod}\,5), \\ 2\cdot 132 \equiv 4(\mathrm{mod}\,5), \end{cases} \qquad \begin{cases} 3\cdot 132 \equiv 1(\mathrm{mod}\,5), \\ 4\cdot 132 \equiv 3(\mathrm{mod}\,5). \end{cases}$$

В цьому випадку $B_{34} = 3\cdot 132 = 396$.

Визначимо B_{44}. Маємо $m_4 = 11$, $M_4 / m_4 = 660/11 = 60$, $\bar{m}_{44} \equiv \overline{1, m_4 - 1} = \overline{1, 10}$.

$$\begin{cases} 1\cdot 60 \equiv 5(\mathrm{mod}11), \\ 2\cdot 60 \equiv 10(\mathrm{mod}11), \\ 3\cdot 60 \equiv 4(\mathrm{mod}11), \\ 4\cdot 60 \equiv 9(\mathrm{mod}11), \\ 5\cdot 60 \equiv 3(\mathrm{mod}11), \end{cases} \qquad \begin{cases} 6\cdot 60 \equiv 8(\mathrm{mod}11), \\ 7\cdot 60 \equiv 2(\mathrm{mod}11), \\ 8\cdot 60 \equiv 7(\mathrm{mod}11), \\ 9\cdot 60 \equiv 1(\mathrm{mod}11), \\ 10\cdot 60 \equiv 6(\mathrm{mod}11). \end{cases}$$

В цьому випадку $B_{44} = 9\cdot 60 = 540$.

2.1.5. Визначимо значення B_{i5} для п'ятого ($j = 5$) набору основ $m_1 = 3$, $m_2 = 4$, $m_3 = 5$, $m_4 = 7$ СЗК (табл. 5.2). У цьому випадку $M_5 = \prod_{i=1}^{4} m_i = 420$ ($M = 420$).

Визначимо B_{15}. Маємо $m_1 = 3$, $M_5 / m_1 = 420/3 = 140$, $\bar{m}_{15} \equiv \overline{1, m_1 - 1} = \overline{1, 2}$.

$$\begin{cases} 1\cdot 140 \equiv 2(\mathrm{mod}\,3), \\ 2\cdot 140 \equiv 1(\mathrm{mod}\,3). \end{cases}$$

У цьому випадку $B_{15} = 9\cdot 140 = 280$.

Визначимо B_{25}. Маємо $m_2 = 4$, $M_5 / m_2 = 420/4 = 105$, $\bar{m}_{25} \equiv \overline{1, m_2 - 1} = \overline{1, 3}$.

$$\begin{cases} 1\cdot 105 \equiv 1 (\mathrm{mod}\, 4), \\ 2\cdot 105 \equiv 2 (\mathrm{mod}\, 4), \\ 3\cdot 105 \equiv 3 (\mathrm{mod}\, 4). \end{cases}$$

У цьому випадку $B_{25} = 1\cdot 105 = 105$.

Визначимо B_{35}. Маємо $m_3 = 5$, $M_5 / m_3 = 420/5 = 84$, $\bar{m}_{35} \equiv \overline{1, m_3 - 1} = \overline{1, 4}$.

$$\begin{cases} 1\cdot 84 \equiv 4 (\mathrm{mod}\, 5), \\ 2\cdot 84 \equiv 3 (\mathrm{mod}\, 5), \end{cases} \qquad \begin{cases} 3\cdot 84 \equiv 2 (\mathrm{mod}\, 5), \\ 4\cdot 84 \equiv 1 (\mathrm{mod}\, 5). \end{cases}$$

У цьому випадку $B_{35} = 4\cdot 84 = 336$.

Визначимо B_{35}. Маємо $m_4 = 7$, $M_5 / m_4 = 420/7 = 60$, $\bar{m}_{45} \equiv \overline{1, m_4 - 1} = \overline{1, 6}$.

$$\begin{cases} 1\cdot 60 \equiv 4 (\mathrm{mod}\, 7), \\ 2\cdot 60 \equiv 1 (\mathrm{mod}\, 7), \\ 3\cdot 60 \equiv 5 (\mathrm{mod}\, 7), \end{cases} \qquad \begin{cases} 4\cdot 60 \equiv 2 (\mathrm{mod}\, 7), \\ 5\cdot 60 \equiv 6 (\mathrm{mod}\, 7), \\ 6\cdot 60 \equiv 3 (\mathrm{mod}\, 7). \end{cases}$$

У цьому випадку $B_{45} = 2\cdot 60 = 120$.

Сукупність розрахованих частинних ортогональних базисів B_{ij} приведена у табл. 5.5.

2.2. Визначимо правильність залишків числа $\tilde{A}$. Спочатку складемо усі можливі проекції $\tilde{A}_j$ числа $\tilde{A} = (0\,||\,0\,||\,2\,||\,1)$

$$\begin{cases} \tilde{A}_1 = (0\,||\,0\,||\,2\,||\,1), \\ \tilde{A}_2 = (0\,||\,0\,||\,2\,||\,1), \\ \tilde{A}_3 = (0\,||\,0\,||\,2\,||\,1), \end{cases} \qquad \begin{cases} \tilde{A}_4 = (0\,||\,0\,||\,0\,||\,1), \\ \tilde{A}_5 = (0\,||\,0\,||\,0\,||\,2). \end{cases}$$

По відомій формулі, використовуючи дані табл. 5.5, представимо

значення проекцій $\tilde{A}_j \;\; j=\overline{1,5}$ у ПСЧ:

$$\tilde{A}_{1ПСЧ}=(a_1\cdot B_{11}+a_2\cdot B_{21}+a_3\cdot B_{31}+a_4\cdot B_{41})\bmod M_1=$$

$$=(0\cdot 385+0\cdot 616+2\cdot 1100+1\cdot 980)\bmod 1540=100<420$$

$$\tilde{A}_{2ПСЧ}=(a_1\cdot B_{12}+a_2\cdot B_{22}+a_3\cdot B_{32}+a_4\cdot B_{42})\bmod M_2=$$

$$=(0\cdot 385+0\cdot 231+2\cdot 330+1\cdot 210)\bmod 1155=870>420.$$

$$\tilde{A}_{3ПСЧ}=(a_1\cdot B_{13}+a_2\cdot B_{23}+a_3\cdot B_{33}+a_4\cdot B_{43})\bmod M_3=$$

$$=(0\cdot 616+0\cdot 693+2\cdot 792+1\cdot 672)\bmod 924=418<420.$$

$$\tilde{A}_{4ПСЧ}=(a_1\cdot B_{14}+a_2\cdot B_{24}+a_3\cdot B_{34}+a_4\cdot B_{44})\bmod M_4=$$

$$=(0\cdot 220+0\cdot 165+2\cdot 396+1\cdot 540)\bmod 660=540>420.$$

$$\tilde{A}_{5ПСЧ}=(a_1\cdot B_{15}+a_2\cdot B_{25}+a_3\cdot B_{35}+a_4\cdot B_{45})\bmod M_5=$$

$$=(0\cdot 280+0\cdot 105+2\cdot 336+1\cdot 120)\bmod 420=240<420.$$

Таким чином, серед усіх отриманих проекцій $\tilde{A}_i$ числа $\tilde{A}$ проекції $\tilde{A}_1$, $\tilde{A}_3$ і $\tilde{A}_5$ менше значення $M=420$, а проекції $\tilde{A}_2$ і $\tilde{A}_4$ більше $M=420$. Отже, результати діагностики неправильного $\tilde{A}$ числа стверджують, що серед усіх п'яти залишків числа саме залишки a_1, a_3 і a_5 можуть бути помилковими, а залишки a_2 і a_4 точно не спотворені. У цьому випадку $r=3$ та $Д = 1/3 \approx 0{,}3$ [158-161].

5.2 Метод визначення альтернативної сукупності НКС у СЗК

Для здійснення контролю, діагностики та корекції помилок у НКС необхідно ввести певну інформаційну надмірність. Ступінь R інформаційної надмірності, яка обумовлює коригувальні здібності коду, оцінюється величиною $d_{\min}^{(СЗК)}$ мінімальної кодової відстані. У СЗК значення МКВ

визначається співвідношенням $d_{\min}^{(СЗК)} = k+1$ [1]. При одній контрольній основі МКВ дорівнює величині рівній $d_{\min}^{(СЗК)} = 2$. Відповідно до теорії кодування при мінімальній кодовій відстані $d_{\min}^{(СЗК)} = 2$ у кодовій структурі достовірно визначається факт спотворення тільки одного із залишків (одноразова помилка) кодового слова у СЗК. Для виправлення (корекції), наприклад, одноразової помилки необхідно забезпечити умову, коли $d_{\min}^{(СЗК)} = 3.$

У зв'язку з впливом властивостей СЗК на процес обробки даних, у деяких випадках, є можливість проводити корекцію одноразових (у одному залишку НКС) помилок даних при введенні мінімальної $(k = 1)$ інформаційної кодової надмірності. Одним з випадків корекції, обумовленою такою властивістю СЗК, як незалежність залишків НКС, є випадок корекції помилок тільки кінцевого результату обчислення [47]. Типовим прикладом для даного випадку є можливість реалізації процедури корекції помилок даних за наявності однієї контрольної основи без зупинки процесу проміжних обчислень (у динаміці обчислювального процесу (ДОП)).

Для реалізації такої процедури виникає необхідність проведення діагностики проміжних результатів обчислень, на основі використання поняття альтернативної сукупності (АС) $W(\tilde{A}) = \left\{ m_{l_1}, m_{l_2}, ..., m_{l_\rho} \right\}$ числа у СЗК неправильних $\tilde{A} = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n)$ чисел. Під поняттям АС $W(\tilde{A}) = \left\{ m_{l_1}, m_{l_2}, ..., m_{l_\rho} \right\}$ неправильного (спотвореного) числа $\tilde{A} = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n)$ розуміється сукупність $\left\{ m_{l_k} \right\}$ $(k = \overline{1, \rho})$ з ρ основ СЗК, по яких правильне (неспотворене) число (кодове слово) $A = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n)$ може відрізнятися від цієї сукупності $\left\{ \tilde{A} \right\}$ можливих похідних неправильних чисел. При цьому передбачається, що може виникнути тільки одноразова (по одному із залишків m_i $(i = \overline{1, n+1})$

числа $A=(a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n)$ помилка (спотворення одного з (n+1)-го залишку) у правильному числі A.

Відмітимо, що АС розглядається при введенні в кодову структуру СЗК мінімальної інформаційної надмірності, шляхом додання до n інформаційних однієї ($k = 1$) додаткової (контрольної) основи m_{n+1} СЗК, за умови, що $m_i < m_{n+1}$ $(i = \overline{1, n})$. У цьому випадку загальна кількість $N_{ЗК}$ кодових слів у СЗК рівно $N_{ЗК} = \prod_{i=1}^{n+1} m_i$. Кількість $N_{ПК}$ правильних кодових слів дорівнює $N_{ПК} = \prod_{i=1}^{n} m_i$, а кількість $N_{НК}$ неправильних (спотворених) кодових слів дорівнює $N_{НК} = N_{ЗК} - N_{ПК} = N_{ПК} \cdot (m_{n+1} - 1)$.

Необхідність визначення АС може виникати у наступних основних випадках. По-перше, при необхідності проведення процесу контролю, діагности та корекції помилок даних у СЗК. По-друге, при організації процедур контролю, діагности та виправлення помилок даних у СЗК у процесі рішення задачі у ДОП (у реальному часі, тобто без зупинки обчислень) при введенні мінімальної інформаційної надмірності. Одна з основних вимог до процедури визначення АС у СЗК являється вимога зменшення часу визначення цього набору основ. Особливо ця вимога критична для другого випадку – при рішенні обчислювальних задач у ДОП [162-164].

Усі існуючі методи визначення АС чисел ґрунтуються на процедурі послідовного визначення шуканих основ АС чисел у СЗК. Так, наприклад, АС $W(\tilde{A}) = \left\{ m_{l_1}, m_{l_2}, ..., m_{l_\rho} \right\}$ неправильного числа $\tilde{A} = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n)$ може бути встановлена послідовною перевіркою кожної з основ m_i $(i = \overline{1, n})$ СЗК таким чином. Визначається сукупність чисел, що мають однакове значення залишків по всіх основах СЗК, що і число $\tilde{A}$ окрім однієї визначеної основи, і відрізнятися лише

значеннями можливих залишків по цій основі. Серед цієї сукупності чисел може не бути жодного правильного числа, або може бути тільки одне правильне число. У останньому випадку отримане число входить в АС неправильного числа, що перевіряється $\tilde{A}$. Даний метод припускає послідовне проведення аналогічних перевірок для кожної з інформаційних основ СЗК (контрольна основа завжди входить до складу основ АС). Результат таких послідовних перевірок повністю визначає АС $W(\tilde{A}) = \left\{ m_{l_1}, m_{l_2}, ..., m_{l_\rho} \right\}$. Недоліки цього методу визначення АС: висока обчислювальна трудомісткість і значний час визначення АС.

Другий метод визначення АС заснований на обчисленні усіх можливих проекцій $\tilde{A}_i = (a_1 \| a_2 \| ... \| a_{i-1} \| a_{i+1} \| ... \| a_n)$ неправильного числа $\tilde{A}$, і подальшому їх порівнянні зі значенням величини інформаційного діапазону заданої СЗК. У доведено, що необхідною і достатньою умовою входження основи СЗК в АС $W(\tilde{A}) = \left\{ m_{l_1}, m_{l_2}, ..., m_{l_\rho} \right\}$ числа $\tilde{A} = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n)$ являється правильність його проекції $\tilde{A}_i$. Розглянемо приклад визначення АС чисел у СЗК на основі використання другого методу. Нехай необхідно визначити АС числа $A_{СЗК} = (0 \| 0 \| 0 \| 0 \| 5)$ заданого у СЗК інформаційними $m_1 = 3$, $m_2 = 4$, $m_3 = 5$, $m_5 = 7$ та контрольною $m_k = m_5 = 11$ основами. При цьому $M = \prod_{i=1}^{n} m_i = \prod_{i=1}^{4} m_i = 420$ та $M_0 = M \cdot m_{n+1} = 420 \cdot 11 = 4620$. Ортогональні базиси B_i $(i = \overline{1, n+1})$ для даної СЗК визначені у розділі 4 табл. 4.6.

Заздалегідь проведемо контроль даних $A_{СЗК} = (0 \| 0 \| 0 \| 0 \| 5)$. Відповідно до процедури контролю [165] визначимо значення початкового числа у позиційній десятковій системі числення

$$A_{ПСЧ} = \left(\sum_{i=1}^{n+1} a_i \cdot B_i \right) \bmod M_0 = \left(\sum_{i=1}^{5} a_i \cdot B_i \right) \bmod M_0 =$$

$$= (a_1 \cdot B_1 + a_2 \cdot B_2 + a_3 \cdot B_3 + a_4 \cdot B_4 + a_5 \cdot B_5) \bmod M_0 =$$

$$= (0 \cdot 1540 + 0 \cdot 3465 + 0 \cdot 3696 + 0 \cdot 2640 + 5 \cdot 2520) \bmod 4620 =$$

$$= (5 \cdot 2520) \bmod 4620 = 12600 (\bmod 4620) = 3360 > 420 .$$

Таким чином, у процесі контролю визначено, що $A_{ПСЧ} = 3360 > M = 420$. У цьому випадку, при можливості виникнення тільки одноразових помилок, робиться висновок про те, що дане число $\tilde{A}_{3360} = (0 \| 0 \| 0 \| 0 \| 5)$ неправильне. Далі здійснимо процедуру визначення АС числа $\tilde{A}_{3360} = (0 \| 0 \| 0 \| 0 \| 5)$. Відповідно до другого методу визначення АС складемо можливі проекції $\tilde{A}_j$ числа $\tilde{A}_{3360} = (0 \| 0 \| 0 \| 0 \| 5)$: $\tilde{A}_1 = (0 \| 0 \| 0 \| 5)$, $\tilde{A}_2 = (0 \| 0 \| 0 \| 5)$, $\tilde{A}_3 = (0 \| 0 \| 0 \| 5)$, $\tilde{A}_4 = (0 \| 0 \| 0 \| 5)$ і $\tilde{A}_5 = (0 \| 0 \| 0 \| 0)$.

Обчислимо усі значення $A_{j\,ПСЧ}$. Далі проведемо $(n+1)$-о порівняння чисел $\tilde{A}_{j\,ПСЧ}$ і числа $M = M_0 / m_{n+1}$. Якщо серед проекцій $\tilde{A}_{j\,ПСЧ}$ є числа що не знаходяться усередині інформаційного $[0, M)$ числового інтервалу (тобто $\tilde{A}_{k\,ПСЧ} \geq M$), що містить k правильних чисел, то робиться висновок про те, що ці k залишків числа $\tilde{A}_{СЗК}$ не спотворені. Помилковими можуть бути тільки залишки, що знаходяться серед інших $[(n+1)-k]$ залишків числа $\tilde{A}_{СЗК}$. В цьому випадку маємо, що

$$\tilde{A}_{1ПСЧ} = \left(\sum_{i=1}^{4} a_i \cdot B_{i1} \right) \bmod M_1 =$$

$$= (a_1 \cdot B_{11} + a_2 \cdot B_{21} + a_3 \cdot B_{31} + a_4 \cdot B_{41}) \bmod M_1 =$$

$$= (0 \cdot 385 + 0 \cdot 616 + 0 \cdot 1100 + 5 \cdot 980) \bmod 1540 = 280 < 420 .$$

Робимо висновок, що $\bar{a}_1$ – можливо спотворений залишок;

$$\tilde{A}_{2ПСЧ} = \left(\sum_{i=1}^{4} a_i \cdot B_{i2} \right) \bmod M_2 =$$

$$= (a_1 \cdot B_{12} + a_2 \cdot B_{22} + a_3 \cdot B_{32} + a_4 \cdot B_{42}) \bmod M_2 =$$

$$= (0 \cdot 385 + 0 \cdot 231 + 0 \cdot 330 + 5 \cdot 210) \bmod 1155 = 1050 > 420.$$

Таким чином, отримаємо, що a_2 достовірно не спотворений залишок;

$$\tilde{A}_{3ПСЧ} = \left(\sum_{i=1}^{4} a_i \cdot B_{i3} \right) \bmod M_3 =$$

$$= (a_1 \cdot B_{13} + a_2 \cdot B_{23} + a_3 \cdot B_{33} + a_4 \cdot B_{43}) \bmod M_3 =$$

$$(0 \cdot 616 + 0 \cdot 693 + 0 \cdot 792 + 5 \cdot 672) \bmod 924 = 588 > 420.$$

Отримаємо, що a_3 достовірно не спотворений залишок;

$$\tilde{A}_{4ПСЧ} = \left(\sum_{i=1}^{4} a_i \cdot B_{i4} \right) \bmod M_4 =$$

$$= (a_1 \cdot B_{14} + a_2 \cdot B_{24} + a_3 \cdot B_{34} + a_4 \cdot B_{44}) \bmod M_4 =$$

$$(0 \cdot 220 + 0 \cdot 165 + 0 \cdot 369 + 5 \cdot 540) \bmod 660 = 60 < 420.$$

Висновок: $\overline{a}_4$ – можливо спотворений залишок; $\tilde{A}_{5ПСЧ} = \left(\sum_{i=1}^{4} a_i \cdot B_{i5} \right) \bmod M_5$. Оскільки $M_5 = M = 420$, то залишок $\overline{a}_5$ по модулю $m_k = m_5$ завжди буде у сукупності можливих спотворених залишків числа у СЗК.

Таким чином, для числа $\tilde{A}_{СЗК} = (0 \| 0 \| 0 \| 0 \| 5)$ визначилися точно не спотворені залишки. Це $a_2 = 0$ і $a_3 = 0$. Помилковими можуть бути залишки по основах m_1, m_4 та m_5, тобто залишки $a_1 = 0$, $a_4 = 0$ та $a_5 = 5$. У цьому випадку для числа $\tilde{A}_{СЗК} = (0 \| 0 \| 0 \| 0 \| 5)$ АС дорівнює наступній сукупності основ СЗК $W(\tilde{A}) = \{1, 4, 5\}$. Застосування другого методу дозволяє дещо

прискорити процес визначення АС $W(\tilde{A})=\left\{m_{l_1}, m_{l_2}, ..., m_{l_\rho}\right\}$ числа $A=(a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n)$ за рахунок можливості паралельно у часі визначати значення можливих проекцій $\tilde{A}_j$ неправильного числа. Ця обставина знижує часову складність визначення АС. Проте відмітимо, що процедура визначення АС числа містить такі основні операції: переведення числа $A=(a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n)$ з СЗК у ПСЧ; переведення проекцій $\tilde{A}_i$ неправильного числа $A=(a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n)$ з СЗК у ПСЧ та операцію порівняння чисел. У СЗК перелічені операції відноситься до непозиційних операцій, що вимагають великих часових та апаратних витрат на її реалізацію. Недоліки цього методу визначення АС залишаються такі ж, як і при першому методі: висока обчислювальна трудомісткість і значний час визначення АС.

Таким чином, залишається задача вдосконалення другого розглянутого методу у плані зменшення часу визначення АС.

Вдосконалення відомого другого методу полягає у зниженнях часу визначення АС. Суть розробленого методу визначення АС чисел у СЗК полягає у попередньому формуванні M таблиць відповідності (таблиць першого ступеня) $A=\Phi_1(\tilde{A})$, кожного правильного числа $A=(a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n)$ (з числового діапазону $0 \div M-1$), можливій сукупності $\left\{\tilde{A}\right\}$ неправильних чисел (з числового діапазону $M \div M_0-1$) при виникненні у числі A одноразових (у одному залишку) помилок (табл. 5.6 – 5.8). На основі аналізу вмісту цих таблиць першого ступеня складається табл. 5.9 другому ступеню, в якій приведена відповідність $\tilde{A}=\Phi_2(A)$ кожного неправильного $\tilde{A}$ числа з числового діапазону $M \div M_0-1$ можливим значенням виправлених (правильних) $A=(a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n)$ чисел. Кількість правильних A чисел відповідає кількості основ СЗК, що містяться в АС $W(\tilde{A})=\left\{m_{l_1}, m_{l_2}, ..., m_{l_\rho}\right\}$

числа A [166-168].

На рис. 5.2 показані етапи реалізації вдосконаленого методу визначення альтернативної сукупності непозиційних кодових структур у СЗК.

Доцільно розглянути використання запропонованого методу визначення АС для конкретної СЗК, заданої інформаційними $m_1 = 2$, $m_2 = 3$ і контрольною основами $m_k = m_3 = m_{n+1} = 5$ ($M = 2 \cdot 3 = 6$; $M_0 = 30$). Сукупність кодових слів у позиційній (десятковій) системі числення та у СЗК представлена у табл. 5.10. Виходячи з вмісту табл. 5.10 по числу правильних кодових слів 0-5 складаються таблиці (табл. 5.11 – 5.16) відповідностей $A = \Phi_1(\tilde{A})$ першого ступеню.

Таблиця 5.6

Таблиця першого ступеня для $A = (0 \,||\, 0 \,||\, ... \,||\, 0)$

0				
$0(\mathrm{mod}\, m_1)$	$0(\mathrm{mod}\, m_2)$	…	$0(\mathrm{mod}\, m_n)$	$0(\mathrm{mod}\, m_{n+1})$
$1(\mathrm{mod}\, m_1)$	$0(\mathrm{mod}\, m_2)$	…	$0(\mathrm{mod}\, m_n)$	$0(\mathrm{mod}\, m_{n+1})$
⋮	⋮	⋮	⋮	⋮
$m_1 - 1(\mathrm{mod}\, m_1)$	$0(\mathrm{mod}\, m_2)$	…	$0(\mathrm{mod}\, m_n)$	$0(\mathrm{mod}\, m_{n+1})$
$0(\mathrm{mod}\, m_1)$	$1(\mathrm{mod}\, m_2)$	…	$0(\mathrm{mod}\, m_n)$	$0(\mathrm{mod}\, m_{n+1})$
$0(\mathrm{mod}\, m_1)$	$2(\mathrm{mod}\, m_2)$	…	$0(\mathrm{mod}\, m_n)$	$0(\mathrm{mod}\, m_{n+1})$
⋮	⋮	⋮	⋮	⋮
$0(\mathrm{mod}\, m_1)$	$m_2 - 1(\mathrm{mod}\, m_2)$	…	$0(\mathrm{mod}\, m_n)$	$0(\mathrm{mod}\, m_{n+1})$
$0(\mathrm{mod}\, m_1)$	$0(\mathrm{mod}\, m_2)$	…	$1(\mathrm{mod}\, m_n)$	$0(\mathrm{mod}\, m_{n+1})$
$0(\mathrm{mod}\, m_1)$	$0(\mathrm{mod}\, m_2)$	…	$2(\mathrm{mod}\, m_n)$	$0(\mathrm{mod}\, m_{n+1})$
⋮	⋮	⋮	⋮	⋮
$0(\mathrm{mod}\, m_1)$	$0(\mathrm{mod}\, m_2)$	…	$m_n - 1(\mathrm{mod}\, m_n)$	$0(\mathrm{mod}\, m_{n+1})$
$0(\mathrm{mod}\, m_1)$	$0(\mathrm{mod}\, m_2)$	…	$0(\mathrm{mod}\, m_n)$	$1(\mathrm{mod}\, m_{n+1})$
$0(\mathrm{mod}\, m_1)$	$0(\mathrm{mod}\, m_2)$	…	$0(\mathrm{mod}\, m_n)$	$2(\mathrm{mod}\, m_{n+1})$
⋮	⋮	⋮	⋮	⋮
$0(\mathrm{mod}\, m_1)$	$0(\mathrm{mod}\, m_2)$	…	$0(\mathrm{mod}\, m_n)$	$m_{n+1} - 1(\mathrm{mod}\, m_{n+1})$

Таблиця 5.7

Таблиця першого ступеня для $A=(1\|\|1\|\|...\|\|1)$

1				
$1(\mathrm{mod}\, m_1)$	$1(\mathrm{mod}\, m_2)$	…	$1(\mathrm{mod}\, m_n)$	$1(\mathrm{mod}\, m_{n+1})$
$0(\mathrm{mod}\, m_1)$	$1(\mathrm{mod}\, m_2)$	…	$1(\mathrm{mod}\, m_n)$	$1(\mathrm{mod}\, m_{n+1})$
⋮	⋮	⋮	⋮	⋮
$m_1-1(\mathrm{mod}\, m_1)$	$1(\mathrm{mod}\, m_2)$	…	$1(\mathrm{mod}\, m_n)$	$1(\mathrm{mod}\, m_{n+1})$
$1(\mathrm{mod}\, m_1)$	$0(\mathrm{mod}\, m_2)$	…	$1(\mathrm{mod}\, m_n)$	$1(\mathrm{mod}\, m_{n+1})$
$1(\mathrm{mod}\, m_1)$	$2(\mathrm{mod}\, m_2)$	…	$1(\mathrm{mod}\, m_n)$	$1(\mathrm{mod}\, m_{n+1})$
⋮	⋮	⋮	⋮	⋮
$1(\mathrm{mod}\, m_1)$	$m_2-1(\mathrm{mod}\, m_2)$	…	$1(\mathrm{mod}\, m_n)$	$1(\mathrm{mod}\, m_{n+1})$
$1(\mathrm{mod}\, m_1)$	$1(\mathrm{mod}\, m_2)$	…	$0(\mathrm{mod}\, m_n)$	$1(\mathrm{mod}\, m_{n+1})$
$1(\mathrm{mod}\, m_1)$	$1(\mathrm{mod}\, m_2)$	…	$2(\mathrm{mod}\, m_n)$	$1(\mathrm{mod}\, m_{n+1})$
⋮	⋮	⋮	⋮	⋮
$1(\mathrm{mod}\, m_1)$	$1(\mathrm{mod}\, m_2)$	…	$m_n-1(\mathrm{mod}\, m_n)$	$1(\mathrm{mod}\, m_{n+1})$
$1(\mathrm{mod}\, m_1)$	$1(\mathrm{mod}\, m_2)$	…	$1(\mathrm{mod}\, m_n)$	$0(\mathrm{mod}\, m_{n+1})$
$1(\mathrm{mod}\, m_1)$	$1(\mathrm{mod}\, m_2)$	…	$1(\mathrm{mod}\, m_n)$	$2(\mathrm{mod}\, m_{n+1})$
⋮	⋮	⋮	⋮	⋮
$1(\mathrm{mod}\, m_1)$	$1(\mathrm{mod}\, m_2)$	…	$1(\mathrm{mod}\, m_n)$	$m_{n+1}-1(\mathrm{mod}\, m_{n+1})$

Таблиця 5.8

Таблиця першого ступеня для $A=((M-1)(\mathrm{mod}\, m_1)\|\|...\|\|(M-1)(\mathrm{mod}\, m_{n+1}))$

$M-1$				
$(M-1)(\mathrm{mod}\, m_1)$	$(M-1)(\mathrm{mod}\, m_2)$	…	$(M-1)(\mathrm{mod}\, m_n)$	$(M-1)(\mathrm{mod}\, m_{n+1})$
$0(\mathrm{mod}\, m_1)$	$(M-1)(\mathrm{mod}\, m_2)$	…	$(M-1)(\mathrm{mod}\, m_n)$	$(M-1)(\mathrm{mod}\, m_{n+1})$
$1(\mathrm{mod}\, m_1)$	$(M-1)(\mathrm{mod}\, m_2)$	…	$(M-1)(\mathrm{mod}\, m_n)$	$(M-1)(\mathrm{mod}\, m_{n+1})$
⋮	⋮	⋮	⋮	⋮
$m_1-1(\mathrm{mod}\, m_1)$	$(M-1)(\mathrm{mod}\, m_2)$	…	$(M-1)(\mathrm{mod}\, m_n)$	$(M-1)(\mathrm{mod}\, m_{n+1})$
$(M-1)(\mathrm{mod}\, m_1)$	$0(\mathrm{mod}\, m_2)$	…	$(M-1)(\mathrm{mod}\, m_n)$	$(M-1)(\mathrm{mod}\, m_{n+1})$
$(M-1)(\mathrm{mod}\, m_1)$	$1(\mathrm{mod}\, m_2)$	…	$(M-1)(\mathrm{mod}\, m_n)$	$(M-1)(\mathrm{mod}\, m_{n+1})$
⋮	⋮	⋮	⋮	⋮
$(M-1)(\mathrm{mod}\, m_1)$	$m_2-1(\mathrm{mod}\, m_2)$	…	$(M-1)(\mathrm{mod}\, m_n)$	$(M-1)(\mathrm{mod}\, m_{n+1})$
$(M-1)(\mathrm{mod}\, m_1)$	$(M-1)(\mathrm{mod}\, m_2)$	…	$0(\mathrm{mod}\, m_n)$	$(M-1)(\mathrm{mod}\, m_{n+1})$
$(M-1)(\mathrm{mod}\, m_1)$	$(M-1)(\mathrm{mod}\, m_2)$	…	$1(\mathrm{mod}\, m_n)$	$(M-1)(\mathrm{mod}\, m_{n+1})$
⋮	⋮	⋮	⋮	⋮
$(M-1)(\mathrm{mod}\, m_1)$	$(M-1)(\mathrm{mod}\, m_2)$	…	$m_n-1(\mathrm{mod}\, m_n)$	$(M-1)(\mathrm{mod}\, m_{n+1})$
$(M-1)(\mathrm{mod}\, m_1)$	$(M-1)(\mathrm{mod}\, m_2)$	…	$(M-1)(\mathrm{mod}\, m_n)$	$0(\mathrm{mod}\, m_{n+1})$
$(M-1)(\mathrm{mod}\, m_1)$	$(M-1)(\mathrm{mod}\, m_2)$	…	$(M-1)(\mathrm{mod}\, m_n)$	$2(\mathrm{mod}\, m_{n+1})$
⋮	⋮	⋮	⋮	⋮
$(M-1)(\mathrm{mod}\, m_1)$	$(M-1)(\mathrm{mod}\, m_2)$	…	$(M-1)(\mathrm{mod}\, m_n)$	$m_{n+1}-1(\mathrm{mod}\, m_{n+1})$

Таблиця 5.9

Таблиця другого ступеня

Неправильне $\tilde{A}$ число	Правильне A число з діапазону $0 \div (M-1)$	Значення АС $W(\tilde{A})$
$\tilde{A}_M = (a_1 \,\|\| \, a_2 \,\|\| \ldots \|\| \, a_{n+1})$	$\tilde{A}_{i1} = (a_1 \,\|\| \, a_2 \,\|\| \ldots \|\| \, a_{n+1})$, $(i = \overline{0,(M-1)})$ $\vdots$ $\tilde{A}_{i(M-1)} = (a_1 \,\|\| \, a_2 \,\|\| \ldots \|\| \, a_{n+1})$, $(i = \overline{0,(M-1)})$	$W(\tilde{A}_M) = \{m_i, \ldots, m_{n+1}\}$, $(i = \overline{1,n})$
$\vdots$	$\vdots$	$\vdots$
$\tilde{A}_{(M_0-1)} = (a_1 \,\|\| \, a_2 \,\|\| \ldots \|\| \, a_{n+1})$	$\tilde{A}_{i1} = (a_1 \,\|\| \, a_2 \,\|\| \ldots \|\| \, a_{n+1})$, $(i = \overline{0,(M-1)})$ $\vdots$ $\tilde{A}_{i(M-1)} = (a_1 \,\|\| \, a_2 \,\|\| \ldots \|\| \, a_{n+1})$, $(i = \overline{0,(M-1)})$	$W(\tilde{A}_{(M-1)}) = \{m_i, \ldots, m_{n+1}\}$, $(i = \overline{1,n})$

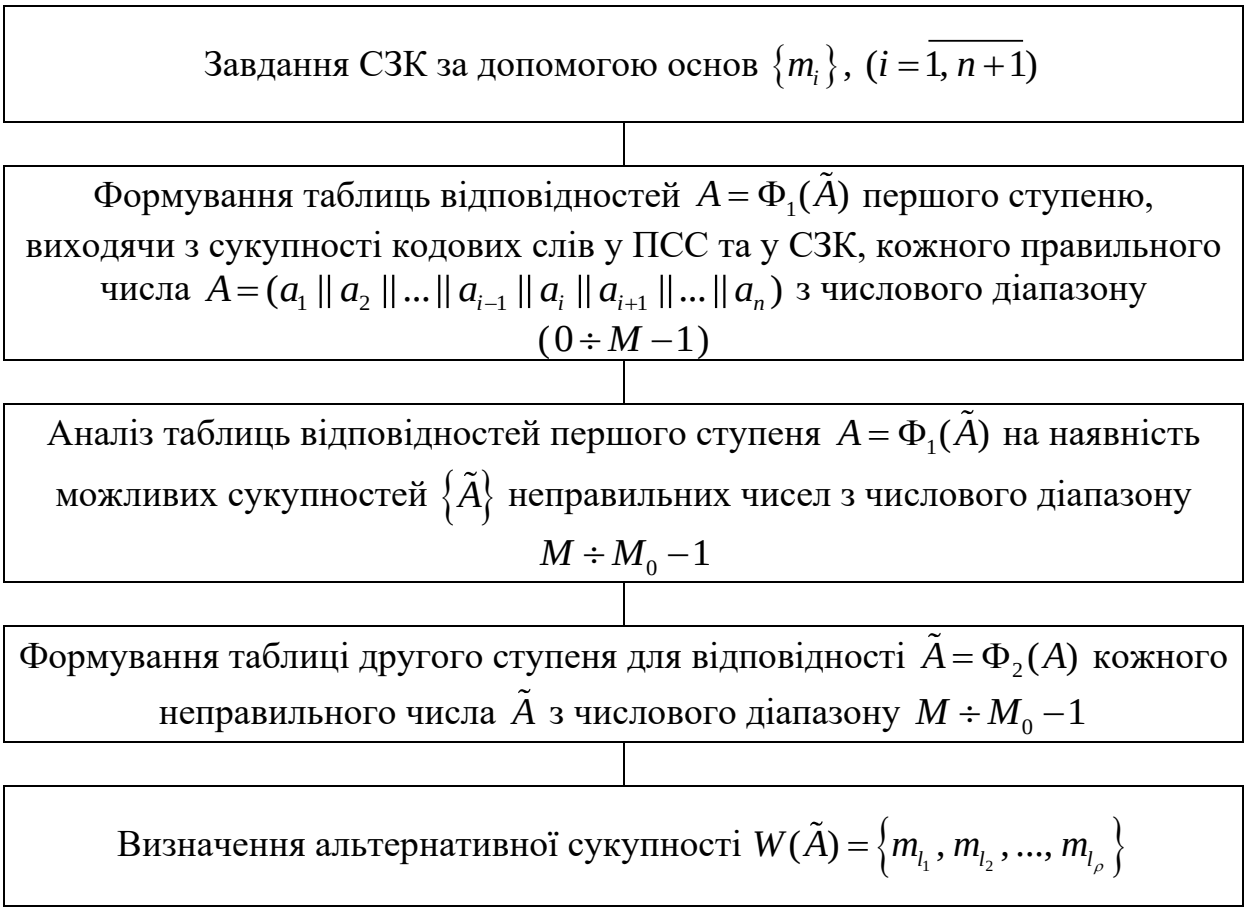

Рис. 5.2 Вдосконалений метод визначення альтернативної сукупності у СЗК

На підставі цих таблиць формується табл. 5.17 другого $\tilde{A} = \Phi_2(A)$ ступеню. У табл. 5.17 приведена відповідність $\tilde{A} = \Phi_2(A)$ кожного неправильного $\tilde{A}$ числа з числового діапазону 6 – 29 можливим значенням виправлених (правильних) A чисел. У табл. 5.17 надано алгоритм визначення АС $W(\tilde{A}) = \left\{ m_{l_1}, m_{l_2}, ..., m_{l_\rho} \right\}$ чисел у СЗК [169-171].

Таблиця 5.10

Сукупність кодових слів у ПСЧ та у СЗК

A у ПСЧ	m_1	m_2	m_3	A у ПСЧ	m_1	m_2	m_3
0	0	0	0	15	1	0	0
1	1	1	1	16	0	1	1
2	0	2	2	17	1	2	2
3	1	0	3	18	0	0	3
4	0	1	4	19	1	1	4
5	1	2	0	20	0	2	0
6	0	0	1	21	1	0	1
7	1	1	2	22	0	1	2
8	0	2	3	23	1	2	3
9	1	0	4	24	0	0	4
10	0	1	0	25	1	1	0
11	1	2	1	26	0	2	1
12	0	0	2	27	1	0	2
13	1	1	3	28	0	1	3
14	0	2	4	29	1	2	4

Таблиця 5.11

0	0	0	0
15	1	0	0
10	0	1	0
20	0	2	0
6	0	0	1
12	0	0	2
18	0	0	3
24	0	0	4

Таблиця 5.12

1	1	1	1
16	0	1	1
21	1	0	1
11	1	2	1
25	1	1	0
7	1	1	2
13	1	1	3
19	1	1	4

Таблиця 5.13

2	0	2	2
17	1	2	2
12	0	0	2
22	0	1	2
20	0	2	0
26	0	2	1
8	0	2	3
14	0	2	4

Таблиця 5.14

3	1	0	3
18	0	0	3
13	1	1	3
23	1	2	3
15	1	0	0
21	1	0	1
27	1	0	2
9	1	0	4

Таблиця 5.15

4	0	1	4
19	1	1	4
24	0	0	4
14	0	2	4
10	0	1	0
16	0	1	1
22	0	1	2
28	0	1	3

Таблиця 5.16

5	1	2	0
20	0	2	0
15	1	0	0
25	1	1	0
11	1	2	1
17	1	2	2
23	1	2	3
29	1	2	4

Розглянемо приклад визначення АС чисел у СЗК запропонованим табличним методом. Нехай дано неправильне число $\tilde{A}_{15} = (1 \mid 0 \mid 0)$ (табл. 5.10). Необхідно визначити АС цього числа.

Спочатку формуються 6 таблиць (табл. 5.11 – 5.16) відповідності першого ступеня кожного правильного $A = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n)$ числа (з числового діапазону 0-5), можливій сукупності неправильних чисел (з числового діапазону 6 – 29) при виникненні у числі A одноразових (в одному залишку) помилок (табл. 5.10).

Таблиця 5.17

Визначення АС $W(\tilde{A}) = \{m_{l_1}, m_{l_2}, ..., m_{l_\rho}\}$ чисел у СЗК

Неправильне $\tilde{A}$ число	Правильне A число	Значення АС $W(\tilde{A})$
1	2	3
$\tilde{A}_6 = (0 \| 0 \| 1)$	$A_0 = (0 \| 0 \| 0)$	$W(\tilde{A}_6) = \{m_3\}$
$\tilde{A}_7 = (1 \| 1 \| 2)$	$A_1 = (1 \| 1 \| 1)$	$W(\tilde{A}_7) = \{m_3\}$
$\tilde{A}_8 = (0 \| 2 \| 3)$	$A_2 = (0 \| 2 \| 3)$	$W(\tilde{A}_8) = \{m_3\}$
$\tilde{A}_9 = (1 \| 0 \| 4)$	$A_3 = (1 \| 0 \| 3)$	$W(\tilde{A}_9) = \{m_3\}$
$\tilde{A}_{10} = (0 \| 1 \| 0)$	$A_0 = (0 \| 0 \| 0)$	$W(\tilde{A}_{10}) = \{m_2, m_3\}$
	$A_4 = (0 \| 1 \| 4)$	
$\tilde{A}_{11} = (1 \| 2 \| 1)$	$A_1 = (1 \| 1 \| 1)$	$W(\tilde{A}_{11}) = \{m_2, m_3\}$
	$A_5 = (1 \| 2 \| 0)$	
$\tilde{A}_{12} = (0 \| 0 \| 2)$	$A_0 = (0 \| 0 \| 0)$	$W(\tilde{A}_{12}) = \{m_2, m_3\}$
	$A_2 = (0 \| 2 \| 2)$	
$\tilde{A}_{13} = (1 \| 1 \| 3)$	$A_1 = (1 \| 1 \| 1)$	$W(\tilde{A}_{13}) = \{m_2, m_3\}$
	$A_3 = (1 \| 0 \| 3)$	
$\tilde{A}_{14} = (0 \| 2 \| 4)$	$A_2 = (0 \| 2 \| 2)$	$W(\tilde{A}_{14}) = \{m_2, m_3\}$
	$A_4 = (0 \| 1 \| 4)$	
$\tilde{A}_{15} = (1 \| 0 \| 0)$	$A_0 = (0 \| 0 \| 0)$	$W(\tilde{A}_{15}) = \{m_1, m_2, m_3\}$
	$A_3 = (1 \| 0 \| 3)$	
	$A_5 = (1 \| 2 \| 0)$	
$\tilde{A}_{16} = (0 \| 1 \| 1)$	$A_1 = (1 \| 1 \| 1)$	$W(\tilde{A}_{16}) = \{m_1, m_3\}$
	$A_4 = (0 \| 1 \| 4)$	

Продовження таблиці 5.17

1	2	3
$\tilde{A}_{17} = (1 \| 2 \| 2)$	$A_2 = (0 \| 2 \| 2)$	$W(\tilde{A}_{17}) = \{m_1, m_3\}$
	$A_5 = (1 \| 2 \| 0)$	
$\tilde{A}_{18} = (0 \| 0 \| 3)$	$A_0 = (0 \| 0 \| 0)$	$W(\tilde{A}_{18}) = \{m_1, m_3\}$
	$A_3 = (1 \| 0 \| 3)$	
$\tilde{A}_{19} = (1 \| 1 \| 4)$	$A_1 = (1 \| 1 \| 1)$	$W(\tilde{A}_{19}) = \{m_1, m_3\}$
	$A_4 = (0 \| 1 \| 4)$	
$\tilde{A}_{20} = (0 \| 2 \| 0)$	$A_0 = (0 \| 0 \| 0)$	$W(\tilde{A}_{20}) = \{m_1, m_2, m_3\}$
	$A_2 = (0 \| 2 \| 2)$	
	$A_5 = (1 \| 2 \| 0)$	
$\tilde{A}_{21} = (1 \| 0 \| 1)$	$A_1 = (1 \| 1 \| 1)$	$W(\tilde{A}_{21}) = \{m_2, m_3\}$
	$A_3 = (1 \| 0 \| 3)$	
$\tilde{A}_{22} = (0 \| 1 \| 2)$	$A_2 = (0 \| 2 \| 2)$	$W(\tilde{A}_{22}) = \{m_2, m_3\}$
	$A_4 = (0 \| 1 \| 4)$	
$\tilde{A}_{23} = (1 \| 2 \| 3)$	$A_3 = (1 \| 0 \| 3)$	$W(\tilde{A}_{23}) = \{m_2, m_3\}$
	$A_5 = (1 \| 2 \| 0)$	
$\tilde{A}_{24} = (0 \| 0 \| 4)$	$A_0 = (0 \| 0 \| 0)$	$W(\tilde{A}_{24}) = \{m_2, m_3\}$
	$A_4 = (0 \| 1 \| 4)$	
$\tilde{A}_{25} = (1 \| 1 \| 0)$	$A_1 = (1 \| 1 \| 1)$	$W(\tilde{A}_{25}) = \{m_2, m_3\}$
	$A_5 = (1 \| 2 \| 0)$	
$\tilde{A}_{26} = (0 \| 2 \| 1)$	$A_2 = (0 \| 2 \| 2)$	$W(\tilde{A}_{26}) = \{m_3\}$
$\tilde{A}_{27} = (1 \| 0 \| 2)$	$A_3 = (1 \| 0 \| 3)$	$W(\tilde{A}_{27}) = \{m_3\}$
$\tilde{A}_{28} = (0 \| 1 \| 3)$	$A_4 = (0 \| 1 \| 4)$	$W(\tilde{A}_{28}) = \{m_3\}$
$\tilde{A}_{29} = (1 \| 2 \| 4)$	$A_5 = (1 \| 2 \| 0)$	$W(\tilde{A}_{29}) = \{m_3\}$

На основі аналізу вмісту цих таблиць першого ступеня складається таблиця другого ступеня, в якій приведена відповідність кожного неправильного числа з числового діапазону $6-29$ можливим значенням виправлених (правильних) $A = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n)$ чисел. Кількість правильних A чисел відповідає кількості основ СЗК, таких, що містяться в АС $W(\tilde{A}) = \left\{m_{l_1}, m_{l_2}, ..., m_{l_\rho}\right\}$ числа A.

При дії одноразових помилок неправильне число $\tilde{A}_{15} = (1 \| 0 \| 0)$ може

бути утворено з наступних правильних *A* чисел. По-перше, правильне число $A_0 = (0 \| 0 \| 0)$ (табл. 5.11) може бути спотворено у першому залишку $a_1 = 0$ $(\tilde{a}_1 = 1)$. По-друге, правильне число $A_3 = (1 \| 0 \| 3)$ (табл. 5.14) може бути спотворено у третьому залишку $a_3 = 3$ $(\tilde{a}_3 = 0)$. І, нарешті, по-третє, правильне число $A_5 = (1 \| 2 \| 0)$ (табл. 5.16) може бути спотворено в другому залишку $a_2 = 2$ $(\tilde{a}_2 = 0)$. Таким чином, АС $W(\tilde{A}) = \{m_{l_1}, m_{l_2}, ..., m_{l_\rho}\}$ неправильного числа $\tilde{A}_{15} = (1 \| 0 \| 0)$ буде дорівнювати значенню $W(\tilde{A}_{15}) = \{m_1, m_2, m_3\}$ (табл. 5.17).

Проведемо розрахунок часу діагностики даних для методу проекцій та для вдосконаленого методу визначення АС.

Час діагностики даних за допомогою методу проекцій ($T_{\text{д }МПр}$) буде визначатись у відповідності з виразом:

$$T_{\text{д }МПр} = t_{пр.} + t_{мн.} + t_{\Sigma} + t_{\text{mod}} + t_{пор.} \tag{5.7}$$

$t_{пр.}$ – час формування можливих проекцій

$$\begin{cases} A_1 = (a_2 \| ... \| a_i \| ... \| a_n \| a_{n+1}), \\ A_2 = (a_1 \| ... \| a_i \| ... \| a_n \| a_{n+1}), \\ \qquad\qquad \vdots \\ A_n = (a_1 \| a_2 \| ... \| a_i \| ... \| a_{n+1}), \\ A_{n+1} = (a_1 \| a_2 \| ... \| a_i \| ... \| a_n) \end{cases}$$

числа $A = (a_1 \| a_2 \| ... \| a_i \| ... \| a_n \| a_{n+1})$;

$t_{мн.}$ – час реалізації операції множення відповідного залишку на частинний ортогональний базис ($a_i \cdot B_{ij}$ де $i = \overline{1, n}$, $j = \overline{1, n+1}$)). Операція

множення виконується паралельно у часі для кожної проекції числа A_j і для кожного залишку a_i;

t_Σ – час реалізації операції додавання попарних добутків ($\sum_{\substack{i=1; \\ j=(\overline{1,n+1})}}^{n} a_i \cdot B_{ij}$);

t_{mod} – час визначення значень проекцій ($A_{jПСС} = (\sum_{\substack{i=1; \\ j=(\overline{1,n+1})}}^{n} a_i \cdot B_{ij}) \bmod M_j$) числа;

$t_{пор.}$ – час порівняння значень проекцій $A_{jПСС}$ числа з максимальним значенням інформаційного числового діапазону (M).

Представимо час реалізації вище вказаних операцій у часових тактах функціонування (t).

При цьому, час формування можливих проекцій числа, буде дорівнювати $t_{пр.} = (n+1) \cdot t$.

З урахуванням того, що арифметичні операції додавання і множення у СЗК, ефективно реалізовувати на основі використання табличного принципу, то вважатимемо, що їх виконання робиться за один часовий t такт функціонування.

У зв'язку з цим час реалізації операції множення відповідного залишку на частинний ортогональний базис буде дорівнювати $t_{мн.} = t$. А час реалізації операції додавання попарних добутків визначиться як: $t_\Sigma = (n-1) \cdot t$;

Час визначення значень проекцій ($A_{jПСС}$) числа, буде дорівнювати $t_{\mathrm{mod}} = 6t$.

Час порівняння значень проекцій $A_{jПСС}$ числа з максимальним значенням інформаційного числового діапазону (M) буде дорівнювати $t_{пор.} = 6t$.

Для проведення порівняльного аналізу оперативності діагностики зручно скористатися величиною $\tau_{ум.} = 2 \cdot t$, де $\tau_{ум.}$ – умовний часовий такт

обробки даних.

У зв'язку з вище сказаним вираз (5.7) можна записати у наступному вигляді:

$$T_{\text{д } МПр} = 2 \cdot t \cdot n + 12 \cdot t = \tau_{ум.} \cdot (n + 6).$$

Час діагностики даних за допомогою вдосконаленого методу визначення альтернативної сукупності у СЗК ($T_{\text{д}W(A)}$), визначимо по формулі (5.8):

$$T_{\text{д}W(A)} = t_{зв.} + t_{W(A)} \tag{5.8}$$

$t_{зв.}$ – час утворення адреси і звернення у таблицю визначення АС, залежить від кількості інформаційних основ, оскільки контрольна основа завжди входить до альтернативної сукупності. У зв'язку з цим $t_{зв.} = n \cdot t$.

$t_{W(A)}$ – час вибірки з таблиці відповідних значень АС, дорівнює одному часовому такту функціонування, тобто $t_{W(A)} = t$.

Виходячи з вище сказаного, вираз (5.8) можна записати у виді:

$$T_{\text{д}W(A)} = n \cdot t + t = 2 \cdot n \cdot t. \tag{5.9}$$

Для зручності приведемо отриманий вираз (5.9) до величини умовного часового такту обробки даних $\tau_{ум.} = 2 \cdot t$ і отримаємо:

$$T_{\text{д}W(A)} = n \cdot \tau.$$

Розрахункові значення часу діагностики даних представлених у СЗК, зведемо у таблицю 5.18.

Таблиця 5.18

Дані порівняльного аналізу часу діагностики даних представлених у СЗК

Метод діагности	Відносний час діагностики даних T/τ				
	Величина розрядної сітки $l(n)$				
	$l=1$ $(n=4)$	$l=2$ $(n=6)$	$l=3$ $(n=8)$	$l=4$ $(n=10)$	$l=8$ $(n=16)$
Метод проекцій	10	12	14	16	22
Вдосконалений метод визначення АС	4	6	8	10	16
Виграш у %	60	50	42,8	37,5	27,3

Таким чином, застосування цього методу, у порівнянні з існуючими методами, дозволяє скоротити час визначення АС чисел. Це досягається, по-перше, за рахунок зменшення кількості основ СЗК, по яких можливо спотворення залишків правильного числа, що послідовно перевіряються $A=(a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n)$. І, по-друге, за рахунок організації процесу швидкої (табличної) вибірки заздалегідь розрахованих даних значень АС $W(\tilde{A})=\left\{m_{l_1}, m_{l_2}, ..., m_{l_\rho}\right\}$. Очевидно, що практично час діагностики даних у СЗК можна зменшити на приблизно 30 %, що підвищує оперативність процедури діагностування.

Зменшення часу визначення АС $W(\tilde{A})=\left\{m_{l_1}, m_{l_2}, ..., m_{l_\rho}\right\}$ чисел дозволить надалі, при необхідності, підвищити швидкодію процесу діагностики та корекції помилок даних у СЗК [172-174].

5.3 Метод оперативної діагностики непозиційних кодових структур у СЗК на основі підвищення інформативності альтернативної сукупності чисел

Розглянемо метод підвищення інформативності АС у СЗК, заснований на отриманні додаткової інформації про можливі спотворені

залишки неправильного операнда $\tilde{A}$. Ця інформація міститься в усіх можливих АС операнда $\tilde{A}$.

Нехай задана СЗК впорядкованими основами $m_i,...,m_{n+1}$ і нехай у ході обчислень визначено неправильне число $\tilde{A}$.

Для підвищення інформативності про місце розташування і величину помилки пропонується додатково визначити АС числа виду

$$W_{k_{\rho i}}\left(\tilde{A}\right)=\left\{m_{k_1},m_{k_2},\ \ldots\ ,m_{k_{\rho_i}}\right\},$$

тобто сукупність АС

$$\begin{aligned}
&W_{1_{\rho 1}}\left(\tilde{A}\right)=\left\{m_{11},m_{12},\ \ldots\ ,m_{1_{\rho_1}}\right\};\\
&W_{2_{\rho 2}}\left(\tilde{A}\right)=\left\{m_{21},m_{22},\ \ldots\ ,m_{2_{\rho_2}}\right\}\ ;\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
&W_{n+1_{\rho_{n+1}}}\left(\tilde{A}\right)=\left\{m_{n11},m_{n12},\ \ldots\ ,m_{n+1_{\rho_{n+1}}}\right\}.
\end{aligned}\qquad (5.6)$$

Щоб визначити сукупність значень (5.6), заздалегідь обчислимо

$$j_k=\bar{m}_k\cdot\gamma_k\left(\operatorname{mod}m_k\right),\qquad (5.7)$$

для $k=\overline{1,n+1}$. Відмітимо, що при $k=n+1$ – $W_{n+1_{\rho_{n+1}}}\left(\tilde{A}\right)=W\left(\tilde{A}\right)$. Відповідно до виразу (5.7) складаємо k таблиць, де значення γ_k зіставляються значенням Δa_i. Після того, як визначені АС $W_{k_{\rho i}}\left(\tilde{A}\right)$, які назвемо первинними, визначимо вторинні АС у вигляді векторів, компонентами яких є можливі значення помилок Δa_i виду:

$$W_1^{(1)}\left(\tilde{A}\right)=\left\{\Delta a_1^{(1)},\Delta a_2^{(1)},...,\Delta a_{n+1}^{(1)}\right\},$$

…

$$W_1^{(\psi_1)}\left(\tilde{A}\right)=\left\{\Delta a_1^{(\psi_1)},\Delta a_2^{(\psi_1)},...,\Delta a_{n+1}^{(\psi_1)}\right\};$$

$$W_2^{(2)}\left(\tilde{A}\right)=\left\{\Delta a_1^{(2)},\Delta a_2^{(2)},...,\Delta a_{n+1}^{(2)}\right\},$$

…

$$W_2^{(\psi_2)}\left(\tilde{A}\right)=\left\{\Delta a_1^{(\psi_2)},\Delta a_2^{(\psi_2)},...,\Delta a_{n+1}^{(\psi_2)}\right\};$$

і так далі до значення векторів виду

$$W_n^{(\psi_n)}\left(\tilde{A}\right)=\left\{\Delta a_1^{(\psi_n)},\Delta a_2^{(\psi_n)},...,\Delta a_{n+1}^{(\psi_n)}\right\}$$

і вектору

$$W_{n+1}(\tilde{A})=\left\{\Delta a_1,\Delta a_2,...,\Delta a_{n+1}\right\}.$$

Компоненти вектора $W_{n+1}(\tilde{A})$ порівнюються з відповідними компонентами всіх векторів $W_i^{(\psi_i)}\left(\tilde{A}\right)$ для $i=\overline{1,n}$. У співпадаючих по величині компонентах векторів визначаються основи СЗК, набір яких і визначить шукану (результуючу) АС виду

$$W'\left(\tilde{A}\right)=\left\{m_{z_1},m_{z_2},\ ...\ ,m_{z_\rho}\right\}.$$

Дійсно, серед АС $W_{k_\rho}\left(\tilde{A}\right)$ завжди міститься основа m_i, по якій сталася помилка Δa_i і ця основа може бути тільки серед основ загальних для сукупності (5.6), тобто

$$W\left(\tilde{A}\right) \geq W'\left(\tilde{A}\right). \qquad (5.8)$$

Коли Δa_i таке, що число $A = A + \Delta A$ лежить в інтервалі $\left[\left(m_{n+1} - 1\right)\ M, M_1\right)$, то

$$W(\tilde{A}) = W'(\tilde{A}). \qquad (5.9)$$

Таким чином, суть запропонованого методу полягає у тому, що визначаються усі можливі АС на кожному з інтервалів попадання операндів *A*. Після цього визначаються загальні для цих інтервалів основи $m_{z_1}, \ldots, m_{z_\rho}$, по яких можлива помилка. Цей набір основ і визначає шукану АС. Скорочення кількості основ в АС підвищує інформативність АС $W(\tilde{A})$ про місце і величину помилки. Це зменшує час стягування АС до помилкової основи (зменшується кількість етапів визначення АС), що підвищує ефективність коригувальних кодів у СЗК. Структурна схема процесу стягання АС представлена на рис. 5.3.

Доцільно розглянути геометричну модель запропонованого методу. Визначення номеру $(j + 1)$ інтервалу попадання (під впливом помилки Δa_i) спотвореного числа $\tilde{A}$ еквівалентно зміщенню цього числа в інтервалі $\left[j\frac{M_i}{m_i}, \left(j+1\right)\frac{M_1}{m_i} \right)$ вліво до значення $j\frac{M_1}{m_i}$. Розіб'ємо числовий відрізок [0, M_1] на відповідні інтервали з тривалістю: $\frac{M_1}{m_1}$, $\frac{M_1}{m_2}$, ., $\frac{M_1}{m_{n+1}}$. Визначимо номери інтервалів $(j+1)$, в яких знаходиться операнд $\tilde{A}$ на кожному з числових відрізків:

$$T_{j_1} = \left[j_1 \frac{M_1}{m_1}, (j_1 + 1)\frac{M_1}{m_1} \right),$$

. . . . . .

$$T_{j_{n+1}} = \left[j_{n+1} \frac{M_1}{m_{n+1}}, (j_{n+1} + 1)\frac{M_1}{m_{n+1}} \right). \qquad (5.10)$$

Визначення первинних АС (5.6) відповідає визначенню номерів інтервалів (5.10). Визначення вторинних АС $W'(\tilde{A})$ геометрично відповідає визначенню інтервалу $[z_1, z_2)$, де

$$z_1 = \max \in j_i \frac{M_1}{m_i};$$

$$z_2 = \min \in (j_i + 1)\frac{M_1}{m_i},$$

тобто інтервал, що шукається, визначиться як перетин сукупностей інтервалів (5.10)

$$T_{W'(\tilde{A})} = T_{j_1} \wedge T_{j_2} \wedge \ ... \ \wedge T_{j_{n+1}}.$$

Очевидно, що

$$z_2 - z_1 = \frac{M_1}{M_{n+1}}. \qquad (5.11)$$

Умова (5.11) еквівалентна умові (5.8). Якщо помилка переводить операнд $\tilde{A}$ в інтервал $[(m_{n+1} - 1)M, M_1)$, то

$$z_2 - z_1 = \frac{M_1}{m_{n+1}} = M \,. \qquad (5.12)$$

Умова (5.12) еквівалентна умові (5.9).

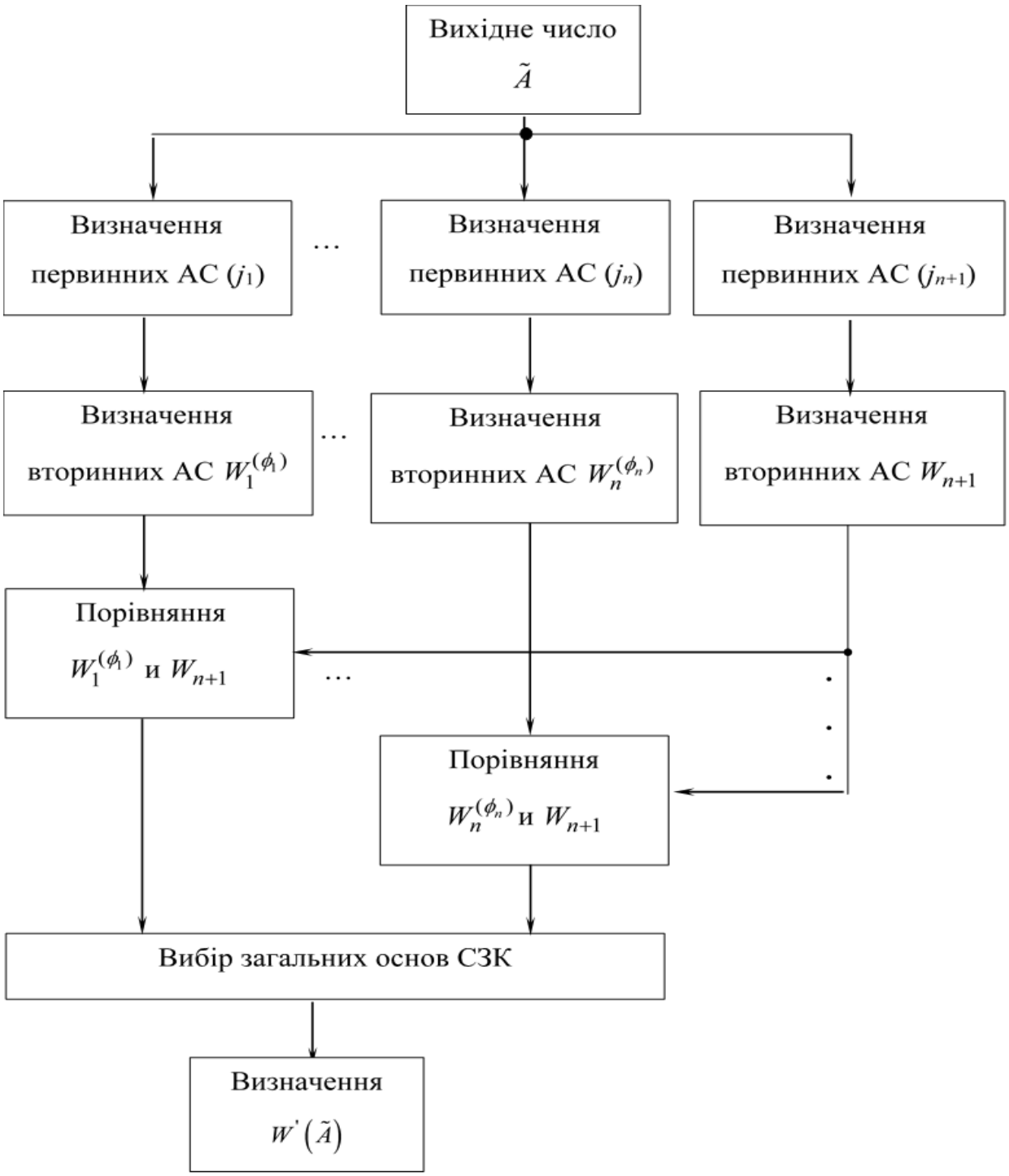

Рис. 5.3 Алгоритм скорочення основ в альтернативній сукупності чисел

Представлена геометрична модель підтверджує правильність математичного опису методу, а також наочніше демонструє суть методу підвищення інформативності АС – звуження інтервалу попадання спотвореного числа $\tilde{A}$.

Розглянемо приклад визначення АС числа $\tilde{A}$ відповідно до розробленого методу. Нехай задана СЗК основами $m_1 = 2$, $m_2 = 3$, $m_3 = 5$. У табл. 5.10 представлені кодові слова даної СЗК. Таким чином $M = 2 \cdot 3 = 6$, $M_0 = M \cdot 5 = 30$, $m_{n+1} = m_3 = 5$; $A = (0,2,2)$, $\Delta A = (0,2,0)$.

Нехай під впливом одноразової помилки $\Delta A = (0, 0, ..., \Delta a_i, ..., 0)$ по i-тій основі ($\Delta a_2 = 2$) отриманий операнд $\tilde{A} = A + \Delta A = (0, 2, 2)$.

Щоб визначити сукупність первинних АС заздалегідь визначимо значення j_k. Для цього проведемо нульовизацію числа $\tilde{A}$ відповідно до таблиць констант нульовизації (див. табл. 5.18 – 5.19).

Отримаємо $\gamma_1 = 1$, $\gamma_2 = 1$, $\gamma_3 = 2$. Сукупність первинних АС визначиться так:

$$W_{1\rho_1}\left(\tilde{A}\right) = \{m_2, m_3\},$$

$$W_{2\rho_2}\left(\tilde{A}\right) = \{m_1, m_3\},$$

$$W_{3\rho_3}\left(\tilde{A}\right) = W\left(\tilde{A}\right)\{m_1, m_2, m_3\}.$$

Таблиця 5.18

m_1	m_2
(1, 1, 1)	(0, 1, 4) (0, 2, 2)

Таблиця 5.19

m_1	m_3
(1, 1, 1)	(0, 0, 1) (0, 2, 2) (0, 0, 3) (0, 1, 4)

Таблиця 5.20

m_2	m_3
(0, 1, 0) (1, 2, 0)	(1, 0, 3) (0, 2, 2) (1, 1, 1)

З табл. 5.21 – 5.23, складених по значеннях j_n, визначимо набір вторинних АС:

$$\text{для } j_3 = 2,\ W_3(\tilde{A}) = \{1, 1, 2\};$$

$$\text{для } j_2 = 1,\ \begin{matrix} W_2^{(1)}\left(\tilde{A}\right) = \{1,0,2\}; \\ W_2^{(2)}\left(\tilde{A}\right) = \{0,0,3\}; \end{matrix}$$

$$\text{для } j_1 = 1,\ \begin{matrix} W_1^{(1)}\left(\tilde{A}\right) = \{0,2,3\}; \\ W_1^{(2)}\left(\tilde{A}\right) = \{0,0,4\}. \end{matrix}$$

Вибір загальних основ СЗК зручно реалізувати у вигляді таблиць (див. табл. 5.24 – 5.27), де знаком «+» відмічений збіг компонент вторинних АС, а знаком «-» – неспівпадання. З табл. 5.24 – 5.27 видно, що компоненти векторів співпадають з основами m_1, m_3, тобто шукана АС має вигляд

$$W_3(\tilde{A}) = \{m_1, m_3\}.$$

Таким чином, $W(\tilde{A}) > W'(\tilde{A})$. Отже, описаний метод гарантовано дозволяє підвищити інформацію про місце помилки в операнді $\tilde{A}$.

Таблиця 5.21

γ_3	Помилки	$W_i^{(\psi_i)}$
0	Ні	–
1	$\Delta a_2 = 1$ $\Delta a_3 = 1$	$W_3^{(1)}(\tilde{A}) = 0, 1, 1$
2	$\Delta a_1 = 1$ $\Delta a_2 = 1$ $\Delta a_3 = 2$	$W_3^{(1)}(\tilde{A}) = 0, 1, 2$
3	$\Delta a_1 = 1$ $\Delta a_2 = 2$ $\Delta a_3 = 3$	$W_3^{(1)}(\tilde{A}) = 0, 2, 3$
4	$\Delta a_2 = 2$ $\Delta a_3 = 4$	$W_3^{(1)}(\tilde{A}) = 0, 2, 4$

Таблиця 5. 22

γ_2	Помилки	$W_i^{(\psi_i)}$
0	$\Delta a_3 = 1$	$W_2^{(1)}(\tilde{A}) = \{0, 0, 1\}$
1	$\Delta a_1 = 1$, $\Delta a_3 = 1$ $\Delta a_2 = 1$	$W_2^{(1)}(\tilde{A}) = \{1, 0, 2\}$, $W_2^{(2)}(\tilde{A}) = \{0, 0, 3\}$
2	$\Delta a_3 = 4$	$W_2^{(1)}(\tilde{A}) = \{0, 0, 3\}$

Таблиця 5.23

γ_1	Помилки	$W_i^{(\psi_i)}$
0	$\Delta a_2 = 1$, $\Delta a_3 = 2$ $\Delta a_3 = 1$	$W_2^{(1)}(\tilde{A}) = \{0, 1, 1\}$, $W_1^{(2)}(\tilde{A}) = \{0, 0, 2\}$
1	$\Delta a2 = 2$, $\Delta a3 = 3$ $\Delta a3 = 3$	$W_1^{(1)}(\tilde{A}) = \{0, 2, 3\}$, $W_1^{(2)}(\tilde{A}) = \{0, 0, 4\}$

У геометричній інтерпретації цей метод, для заданої СЗК, буде реалізований таким чином (рис. 5.4). Розіб'ємо відрізок [0, 30) на відповідні числові інтервали [15, 30), [10, 15) і [12, 18). Визначимо номери інтервалів, в яких знаходиться операнд $\tilde{A} = (1, 2, 2)$.

$$T_{j_1} = [15,30),\ T_{j_2} = [10,20),\ T_{j_3} = [12,18).$$

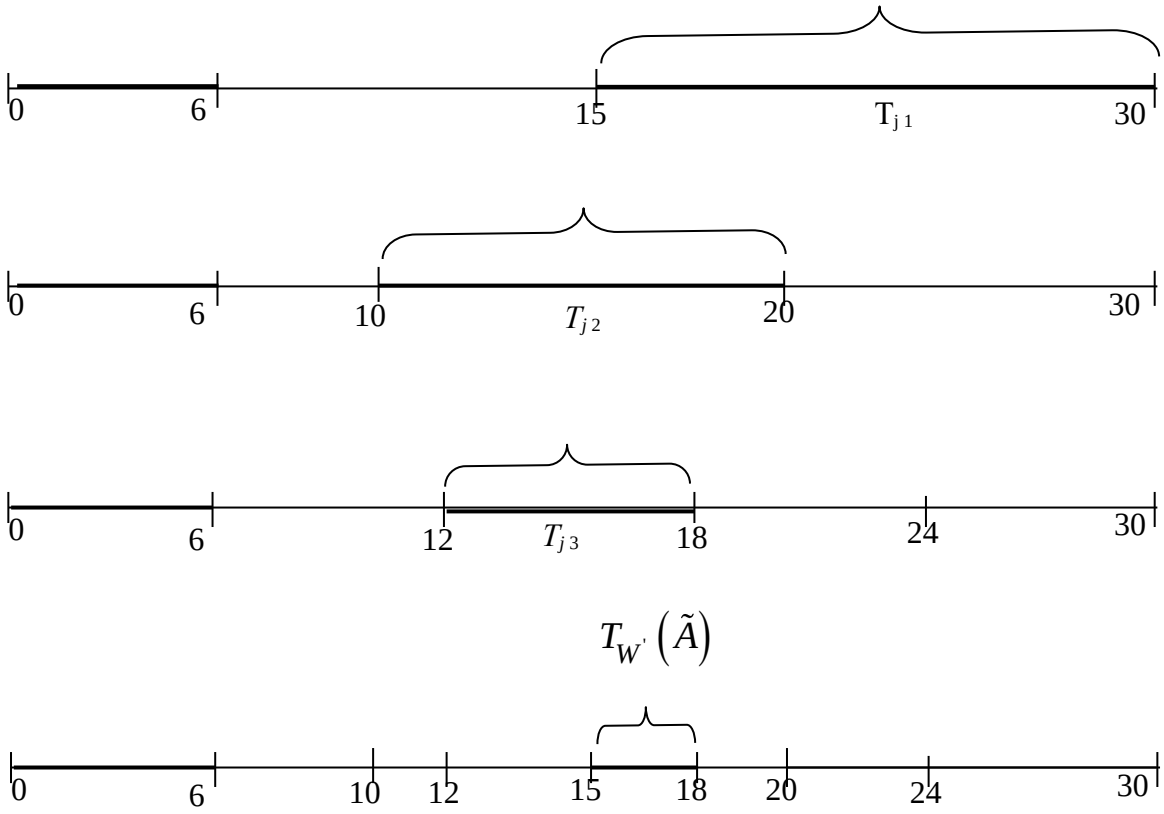

Рис. 5.4 Схема вибору шуканого інтервалу

Шуканий інтервал визначиться так:

$$T_{W'(\tilde{A})} = [15,18).$$

Інтервал $T_{W'(\tilde{A})}$ скорочується у порівнянні з T_{j_3} на три одиниці (на 50%), що призводить до скорочення кількості варіантів можливих помилок. Розроблений метод підвищує ефективність корекції помилок інформації у СЗК.

Таблиця 5.24

m_1	m_2	m_3
1	1	2
1	0	2
+	-	+

Таблиця 5.25

m_1	m_2	m_3
1	1	2
0	0	3
-	-	-

Таблиця 5.26

m_1	m_2	m_3
1	1	2
0	2	3
-	-	-

Таблиця 5.27

m_1	m_2	m_3
1	1	2
0	0	4
-	-	-

Цей метод найбільш ефективно застосовувати у ланцюзі обчислень, що не дозволяє провести усі намічені процедури стягування АС до помилкової основи, тобто у довгому ланцюзі обчислень КСКОЦД.

5.4 Метод оперативної діагностики непозиційних кодових структур на основі процедури інтервальних числових перерізів

Для усіх існуючих методів діагностування даних у СЗК, АС $W(\tilde{A}) = \left\{ m_{l_1}, m_{l_2}, ..., m_{l_\rho} \right\}$ неправильного числа $\tilde{A}_{СЗК} = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n \| a_{n+1})$ визначається в усьому інтервалі $[jM, (j+1)M)$ числової осі $0 \div M_0$, у якому міститься вихідне число $\tilde{A}_{СЗК} = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n \| a_{n+1})$. У цьому випадку АС $W(\tilde{A}) = \left\{ m_{l_1}, m_{l_2}, ..., m_{l_\rho} \right\}$ буде ідентичною для кожного з чисел $A_l \in [jM, (j+1)M)$, що знаходяться у цьому інтервалі.

Таким чином, при визначенні АС $W(A)$ числа A враховується тільки місце розташування інтервалу $[jM, (j+1)M)$ на числовій осі $0 - M_0$, у якому

лежить число A і не враховується місце розташування числа A усередині інтервалу $[jM,(j+1)M)$. Це призводить до того, що АС $W(\tilde{A})=\left\{m_{l_1},m_{l_2},...,m_{l_\rho}\right\}$ може містити надмірну кількість основ. Наявність в АС надмірної кількості основ призводить до необхідності залучення і використання додаткових часових та апаратних ресурсів для реалізації необхідних етапів визначення АС. Ця обставина у першу чергу обумовлює значний час діагностування даних у СЗК. Таким чином, для підвищення оперативності діагностування даних, що представлені у СЗК, необхідно позбавитися від частини надмірних основ, що містяться в АС $W(\tilde{A})=\left\{m_{l_1},m_{l_2},...,m_{l_\rho}\right\}$.

Суть пропонованого методу підвищення оперативності діагностування даних у СЗК полягає в тому, що АС $W(\tilde{A})=\left\{m_{l_1},m_{l_2},...,m_{l_\rho}\right\}$ визначається не в усьому інтервалі $[jM,(j+1)M)$, що містить неправильне число A_{COK}, а тільки в меншому за величиною числовому інтервалі $\Delta A^{(H)}=(A-A^{(H)})<M$, де $A_{СЗК}{}^{(H)}=(0\,||\,0\,||\,...\,||\,0\,||\,\gamma_{n+1})$ – нульовизоване число у СЗК. Суть процедури нульовизації чисел у СЗК полягає у переході від вихідного числа $\tilde{A}_{СЗК}=(a_1\,||\,a_2\,||\,...\,||\,a_{i-1}\,||\,a_i\,||\,a_{i+1}\,||\,...\,||\,a_n\,||\,a_{n+1})$ до числа $A^{(H)}=(0\,||\,0\,||\,...\,||\,0\,||\,\gamma_{n+1})$ за допомогою такої послідовності перетворень, при якій не має місця жоден вихід проміжного числа за робочий $0\div M-1$ діапазон. Як відмічалось у попередніх розділах, процедура нульовизації реалізується за допомогою різних методів. Геометрично операція нульовизації відповідає зміщенню початкового числа $\tilde{A}_{СЗК}=(a_1\,||\,a_2\,||\,...\,||\,a_{i-1}\,||\,a_i\,||\,a_{i+1}\,||\,...\,||\,a_n\,||\,a_{n+1})$ на лівий край $j\cdot M$ числового інтервалу $[jM,(j+1)M)$ його знаходження. Таким чином, для усунення надмірності АС $W(\tilde{A})=\left\{m_{l_1},m_{l_2},...,m_{l_\rho}\right\}$, за рахунок скорочення довжини

інтервалу знаходження числа $A_{СОК}$ пропонується визначити значення $A^{(H)} = (0 \| 0 \| ... \| 0 \| \gamma_{n+1})$ і $\Delta A^{(H)} = (A - A^{(H)})$. Відповідно до розподілу помилок по інтервалах робочого діапазону $[0, M)$, заздалегідь для кожного інтервалу $[jM, (j+1)M)$ складаються двовходові таблиці відповідностей $\overline{W}(A) = \Phi(\gamma_{n+1}, \Delta A^{(H)})$. В цьому випадку АС $W(\tilde{A}) = \left\{ m_{l_1}, m_{l_2}, ..., m_{l_\rho} \right\}$ визначається не в усьому інтервалі $[jM, (j+1)M)$, що містить неправильне число A, а тільки в числовому інтервалі $\Delta A^{(H)}$.

Розроблений метод оперативного діагностування даних, що представлені у СЗК, представлений на рис. 5.5.

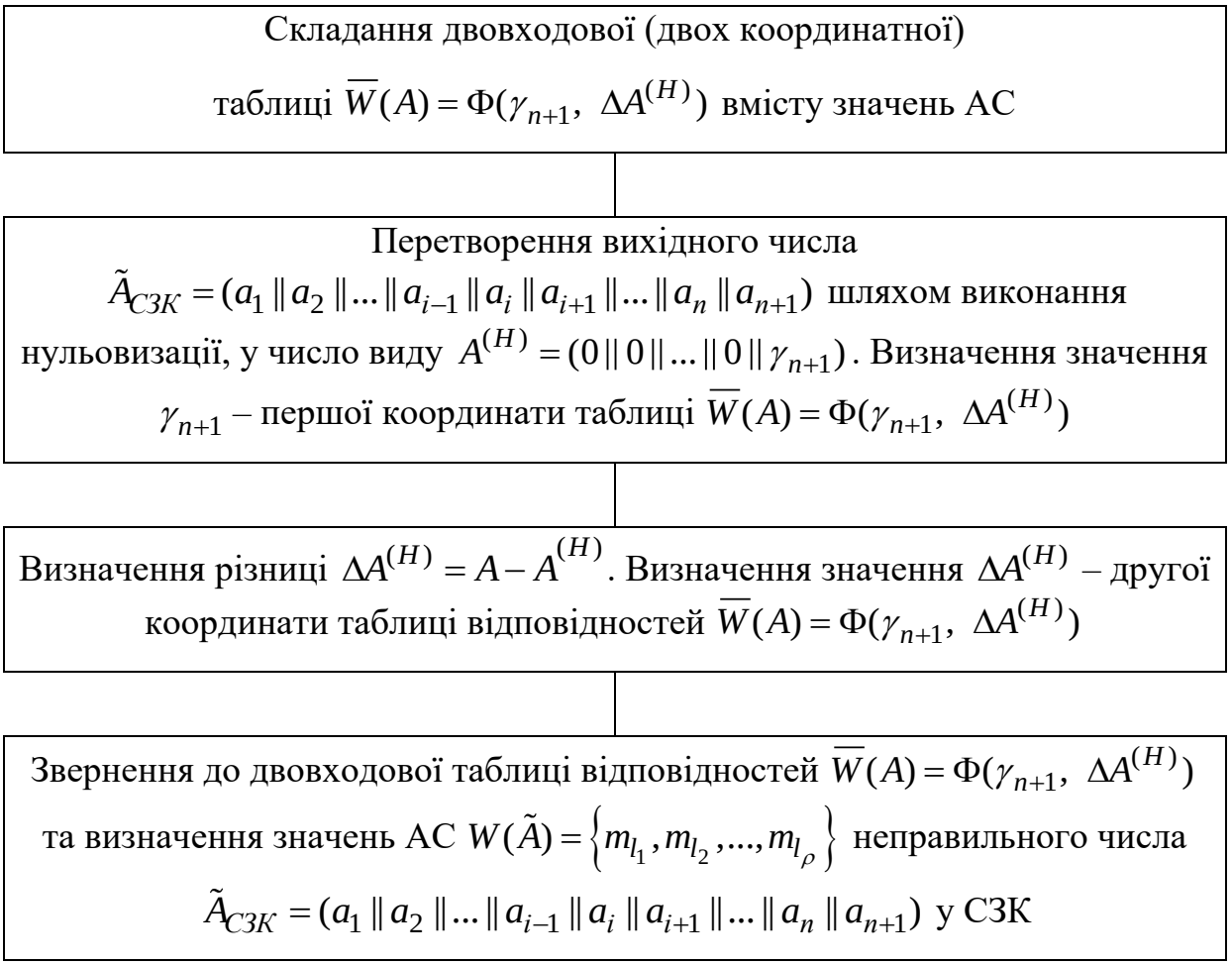

Рис. 5.5 Метод оперативного діагностування даних, що представлені у СЗК

Наведемо приклад діагностики НКС $A_{СЗК} = (0 \| 1 \| 2)$ запропонованим методом на основі використанні результату операції визначення альтернативної сукупності $W(\tilde{A}) = \{m_{l_1}, m_{l_2}, ..., m_{l_\rho}\}$ вихідного числа.

Нехай СЗК представлена основами $m_1 = 2,\ m_2 = 3,\ m_3 = m_{n+1} = 5$; $M = 2 \cdot 3 = 6;\ M_0 = 2 \cdot 3 \cdot 5 = 30.$

У табл. 5.10 представлені кодові слова у ПСЧ та у СЗК. У табл. 5.28 і 5.29 представлені значення КН, використання яких дозволяє вихідне число $A_{СЗК} = (0 \| 1 \| 2)$ привести до числа виду $\tilde{A}^{(H)} = (0 \| 0 \| \gamma_{n+1})$.

У табл. 5.30 представлена повна таблиця значень АС $W(\tilde{A})$ чисел $\tilde{A}$ для даної СЗК.

Таблиця 5.28

Константи нульовизації у СЗК по першій основі СЗК

a_1	КН
0	$(0 \| 0 \| 0)$
1	$(1 \| 1 \| 1)$

Таблиця 5.29

Константи нульовизації по другій основі СЗК

a_2	КН
0	$(0 \| 0 \| 0)$
1	$(0 \| 1 \| 4)$
2	$(0 \| 2 \| 2)$

Таблиця 5.30

Таблиця значень АС $W(\tilde{A})$

$\Delta\tilde{A}$		γ_{n+1}			
		Z_1		Z_2	
		1	2	3	4
Z_3	0	m_3	m_2, m_3	m_1, m_3	m_2, m_3
	1	m_3	m_2, m_3	m_1, m_3	m_2, m_3
	2	m_3	m_2, m_3	m_1, m_2, m_3	m_3
Z_4	3	m_3	m_1, m_2, m_3	m_2, m_3	m_3
	4	m_2, m_3	m_1, m_3	m_2, m_3	m_3
	5	m_2, m_3	m_1, m_3	m_2, m_3	m_3

Альтернативна сукупність $\overline{W}(A)$ числа $A_{СЗК} = (0 \| 1 \| 2)$ визначається таким чином. Різниця $\Delta A^{(H)} = (A - A^{(H)}) = (0 \| 1 \| 4)$ у десятковому коді дорівнює чотирьом (див. табл. 5.10), де $A^{(H)} = (0 \| 0 \| 3)$. По отриманих значеннях $\Delta A^{(H)} = 4$ та $\gamma_{n+1} = 3$ (табл. 5.30) визначимо АС $\overline{W}(A) = \{m_2, m_3\}$. Враховуючи що, для даної СЗК максимальне значення АС дорівнює $W(A) = \{m_1, m_2, m_3\}$, очевидна наступна нерівність $W(A) > \overline{W}(A)$.

Отже маємо, кількість основ в АС $\overline{W}(A) = \{m_2, m_3\}$, в порівнянні з максимально можливим, зменшується на $\approx 25\%$. Ця обставина дозволяє скоротити кількість перевірок основ СЗК на предмет визначення спотвореного залишку у числі $A_{СЗК} = (0 \| 1 \| 2)$, що знижує час діагностування НКС, підвищуючи оперативність діагностування даних у СЗК.

Проведемо оцінку часової складності розробленого методу

діагностування даних у СЗК. Оперативність діагностування даних є основною характеристикою для запропонованого методу.

У СЗК є можливість оцінити часову складність методу оперативного діагностування даних. Формула для оцінки підвищення (у відсотках), в порівнянні з відомими методами, оперативності (ОП) стягнення АС чисел у СЗК до однієї помилкової основи має наступний вигляд

$$ОП = \frac{1 - 1/M}{n+1} \cdot 100\%.$$

Результат розрахунку оперативності стягнення АС чисел у СЗК зведемо у табл. 5.31.

Таблиця 5.31

Розрахункові дані оперативності діагностування чисел у СЗК

Інформаційні основи СЗК m_i $(i = \overline{1,n})$	Контрольна m_{n+1} основа СЗК	Оператив-ність стягнення АС
$m_1 = 3,\ m_2 = 4,\ m_3 = 5,\ m_4 = 7$	$m_5 = 11$	19
$m_1 = 2,\ m_2 = 5,\ m_3 = 7,\ m_4 = 9,\ m_5 = 11,\ m_6 = 13$	$m_7 = 17$	14
$m_1 = 3,\ m_2 = 4,\ m_3 = 5,\ m_4 = 7,\ m_5 = 11,\ m_6 = 13,$ $m_7 = 17,\ m_8 = 19$	$m_9 = 23$	11
$m_1 = 2,\ m_2 = 3,\ m_3 = 5,\ m_4 = 7,\ m_4 = 11,\ m_5 = 13,$ $m_6 = 17,\ m_7 = 19,\ m_9 = 23,\ m_{10} = 29$	$m_{11} = 31$	9
$m_1 = 3,\ m_2 = 4,\ m_3 = 5,\ m_4 = 7,\ m_5 = 11,\ m_6 = 13,$ $m_7 = 17,\ m_8 = 19,\ m_9 = 23,\ m_{10} = 29,\ m_{11} = 31,$ $m_{12} = 37,\ m_{13} = 41,\ m_{14} = 43,\ m_{15} = 47,\ m_{16} = 53$	$m_{17} = 59$	6

Таким чином використання розробленого методу оперативної діагностики помилок даних, що представлені у СЗК, дозволяє підвищити оперативність стягнення АС, залежно від величини розрядної сітки від 6 до 19%.

Висновки до розділу 5

У п'ятому розділі вирішено **сьому та восьму** задачі досліджень та отримано **четвертий та п'ятий** наукові результати.

1. Вдосконалено метод визначення альтернативної сукупності непозиційних кодових структур, який заснований на реалізації функцій відповідності значень можливих помилок. Метод реалізований шляхом зменшення основ СЗК, що перевіряються, які входять в альтернативну сукупність чисел. Використання цього методу дозволяє підвищити оперативність діагностики помилок до 30 %.

2. Розроблено метод оперативної діагностики НКС на основі процедури інтервальних числових перерізів. Цей метод заснований на використанні процедури нульовизації і дає можливість виключити з альтернативної сукупності до 25 % надмірних основ, по яких можлива помилка. Ця обставина знижує час виявлення спотворених залишків НКС, що у свою чергу підвищує оперативність діагностування даних у СЗК.

3. На основі розроблених методів визначення альтернативної сукупності непозиційних кодових структур, синтезований алгоритм діагностування помилок на основі, якого отримано пристрій для його реалізації. На цей пристрій отримано патент України (Пат. 112731, МПК G06F 11/08 (2006.01).

4. Використання запропонованих методів оперативної діагностики даних підвищує загальну ефективність і доцільність використання в обчислювальних системах непозиційних кодових структур у СЗК.

Основні положення цього розділу викладені у публікаціях автора [156-158, 161-173].

РОЗДІЛ 6. МЕТОДИ ОПЕРАТИВНОЇ КОРЕКЦІЇ ПОМИЛОК У СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ

6.1 Теоретичні основи корекції помилок даних у СЗК

У загальному випадку, процес корекції (виявлення і виправлення) помилок в інформаційній кодовій структурі $\tilde{A}$ даних, що представлена у СЗК, складається з наступних основних етапів [44, 97, 175]:

– контроль даних (процес виявлення факту наявності помилки у непозиційній кодовій структурі $\tilde{A} = (a_1 \| a_2 \| ..., a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n)$ СЗК);

– діагностика даних (локалізація місця помилок із заданою глибиною діагностування);

– виправлення помилок у кодовій структурі даних (відновлення спотворених залишків $\tilde{a}_j (j = \overline{1,n})$ неправильного числа $\tilde{A}$ та отримання правильного числа A).

Розглянемо твердження, результати доказу якого можна покласти в основу методів корекції помилок даних, представлених у СЗК.

Твердження. Нехай у впорядкованій СЗК з n інформаційними і однією m_{n+1} контрольною основами число $A = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n \| a_{n+1})$ задовольняє наступній умові $M_{n+1} < A < M_i$, де: $M = M_{n+1} = \prod_{i=1}^{n} m_i$; $M_0 = \prod_{i=1}^{n+1} m_i = M \cdot m_{n+1}$; $M_i = M_0 / m_i$. У цьому випадку залишки $a_1, a_2, ..., a_i$ вважаються правильними (неспотвореними), якщо можлива тільки одноразова (у одному залишку числа A) помилка.

Спочатку, методом від протилежного, доведемо, що залишок a_i числа A не спотворений. Припустимо, що залишок a_i спотворений. У цьому випадку число A буде неправильним, тобто $A \geq M$. Позначимо неспотворений залишок як $\tilde{a}_i$, а правильне число як $\tilde{A} < M$. Вважаємо, що помилка ΔA має адитивний

характер, тобто

$$A = \tilde{A} + \Delta A. \qquad (6.1)$$

З урахуванням цього запишемо, що

$$A = (a_1 \| a_2 \| ... \| \tilde{a}_i \| ... \| a_n \| a_{n+1}) + (0 \| 0 \| ... \| \Delta a \| ... \| 0 \| 0) =$$
$$= (a_1 \| a_2 \| ... \| a_i \| ... \| a_n \| a_{n+1}), \text{ де } a_i = (\tilde{a}_i + \Delta a_i) \bmod m_i. \qquad (6.2)$$

Формулу (6.2) можна записати у наступному вигляді:

$$\Delta a_i = (a_i - \tilde{a}_i) \bmod m_i. \qquad (6.3)$$

На підставі співвідношень (6.1) і (6.3) оцінимо кількісне значення числа $\tilde{A}$ наступним чином:

$$\tilde{A} = A - \Delta\tilde{A}$$
$$\tilde{A} = A - \Delta a_i \cdot B_i,$$
$$\tilde{A} = A - [(a_i - \tilde{a}_i) \bmod m_i] \cdot \bar{m}_i \cdot M_i,$$
$$\tilde{A} = A + [(\tilde{a}_i - a_i) \bmod m_i] \cdot \bar{m}_i \cdot M_i, \qquad (6.4)$$

де $\bar{m}_i$ – вага i-го ортогонального базису B_i СЗК, який визначається з наступного співвідношення $B_i = \bar{m}_i \cdot M_i \equiv 1 (\bmod\ m_i)$. Максимально можливе значення величини $\{[(a_i - \tilde{a}_i) \bmod m_i] \cdot \bar{m}_i \cdot M_i\} \bmod M$ у записі вираження (6.4) визначиться таким чином:

$$\max(\{[(a_i - \tilde{a}_i) \bmod m_i] \cdot \bar{m}_i \cdot M_i\} \bmod M_0 = [(m_i - 1)/m_i] \cdot M_0. \qquad (6.5)$$

Дійсно, вираз $(\tilde{a}-a_i)\bmod m_i$ може набувати тільки значень від 0 до m_i-1. У цьому випадку $\max[(\tilde{a}_i-a_i)\bmod m_i]=m_i-1$, а $M_i=M_0/m_i$. Співвідношення (6.4) представиться у вигляді:

$$\tilde{A}=A+[(m_i-1)/m_i]\cdot M_0. \qquad (6.6)$$

Відповідно до умови твердження маємо, що $A<M_i=M_0/m_i$. У цьому випадку вираз (6.6) набере вигляду:

$$\tilde{A}<M_0/m_i+[(m_i-1)/m_i]\cdot M_0, \text{ або}$$
$$A<M_0\cdot[1/m_i+(m_i-1)/m_i],$$
$$\tilde{A}<M_0. \qquad (6.7)$$

Число $\tilde{A}$ може бути правильним ($\tilde{A} < M$), якщо від додавання величини Δa_i (див. вираз (6.3)) воно перевершило б значення M_0 [1]. Але, як видно з виразу (6.7), ніяким можливим виправленням неправильного залишку a_i, цього досягти не можливо, це суперечить допущенню, що залишок a_i числа A – не правильний. Таким чином, залишок a_i не спотворений, а число A – правильне. Оскільки $A<M_i$, то і тим більше $A<M_i<M_{i-1}<...<M_2<M_1$, звідки слідує правильність залишків $a_{i-1},...,a_2,a_1$. Відмітимо, що при $i=n$, тобто $M_{n+1}<A<M_n$, помилковий залишок буде a_{n+1}.

Можна показати, що завадостійкий R–код у СЗК може виявляти і виправляти число $t_{вияв.}$ і $t_{випр.}$ помилок більш високої кратності, ніж та, яка визначається загальною теорією кодування, тобто величиною $d_{мін.}^{(СЗК)}$ МКВ [176, 177].

Дійсно. Нехай для заданої СЗК МКВ визначається значенням $d_{мін.}^{(СЗК)}$. Припустимо, що у заданій СЗК є l основ, для яких виконується умова

$l > d_{мін.}^{(СЗК)}$ і при цьому $Q(l) = \prod_{j=1}^{l} m_{z_j} < R = M_0 / M$. У цьому випадку помилки у залишках числа $A_{СЗК}$ по цих основах можна достовірно виявити.

Покажемо це. Для вихідних даних, що розглядаються, у вектору помилки $\Delta A = (\tilde{A}_{СЗК} - A_{СЗК}) \bmod M = (0 \| 0 \| ... \| 0 \| \Delta a_{z_1} \| 0 \| ... \| 0 \| \Delta a_{z_l} \| 0 \| ... ... \| 0 \| 0)$ повинно бути не менше $(n-l)$ нульових залишків. Визначимо чисельне значення помилки $\Delta A = (B_{z_1} \cdot \Delta a_{z_1} + ... + B_{z_l} \cdot \Delta a_{z_l}) \bmod M_0$. З урахуванням того, що довільний ортогональний базис у СЗК представляється у вигляді $B_{z_i} = \bar{m}_{z_i} \cdot M_0 / m_{z_i}$ ($\bar{m}_{z_i}$ – вага i-го ортогонального базису B_{z_i} СЗК), то значення ΔA визначиться таким чином

$$\Delta A = \left(\frac{\bar{m}_{z_1} \cdot M_0}{m_{z_1}} \cdot \Delta a_{z_1} + ... + \frac{\bar{m}_{z_l} \cdot M_0}{m_{z_l}} \cdot \Delta a_{z_l} \right) \bmod M_0 =$$

$$= \left(\frac{\bar{m}_{z_1} \cdot M_0 \cdot Q_1(l)}{Q(l)} \cdot \Delta a_{z_1} + ... + \frac{\bar{m}_{z_l} \cdot M_0 Q_l(l)}{Q(l)} \cdot \Delta a_{z_l} \right) \bmod M_0,$$

де $Q_i(l) = \prod_{\substack{j=1; \\ j \neq 1.}}^{l} m_{z_j}$.

Таким чином, маємо, що

$$\Delta A = \frac{M_0}{Q(l)} \cdot \left(\bar{m}_{z_1} \cdot Q_1(l) \cdot \Delta a_{z_1} + ... + \bar{m}_{z_l} \cdot Q_l(l) \cdot \Delta a_{z_l} \right) \bmod M_0$$

або

$$\Delta A = \left(\frac{M_0}{Q(l)} \cdot \sum_{i=1}^{l} (\bar{m}_{z_i} \cdot Q_i(l) \cdot \Delta a_{z_i}) \right) \bmod M_0 .$$

Оскільки маємо, що $Q(l) < M_0 / M$ та $\sum_{i=1}^{l} (\bar{m}_{z_i} \cdot Q_i(l) \cdot \Delta a_{z_i}) \neq 0$, то $\Delta A \geq M$.

Очевидно, що сума $A_{СЗК} + \Delta A$ будь-якого правильного ($A_{СЗК} < M$) числа $A_{СЗК}$, та числа, що відповідає величині ΔA помилки, не може належати множині $[0, M)$ правильних чисел, тобто $\tilde{A}_{СЗК} = (A_{СЗК} + \Delta A) \bmod M_0 \geq M$. В цьому випадку у процесі контролю даних подібну помилку можна виявити (можна виявити спотворений залишок числа $\tilde{A}_{СЗК}$ по одній з основ СЗК). Виходячи з вищевикладеного можна стверджувати, що R-код у СЗК дозволяє достовірно виявляти усі помилки, що кратні $t_{вияв.} = 1$ до $t_{вияв.} = d_{мін.}^{(СЗК)} - 1$. Окрім цього, у [44] показано, що завадостійкий R–код у СЗК дозволяє виявляти і виправляти велику частину $\left((R-1)/R = 1 - M/M_0\right)$ помилок більш високої кратності, ніж це дозволяє значення $d_{мін.}^{(СЗК)}$ МКВ.

6.2 Метод виправлення помилок даних у СЗК

У загальному випадку процес корекції помилок даних у СЗК, як і у позиційній системі числення, складається з трьох етапів. Перший етап – контроль даних (визначення правильності або неправильності вихідного числа $A_{СЗК}$). Другий етап. Це діагноста неправильного $\tilde{A}_{СЗК}$ числа (визначення одного спотвореного залишку $\tilde{a}_i$ по основі m_i СЗК числа $\tilde{A}_{СЗК}$). І, нарешті, третій етап, виправлення неправильного залишку $\tilde{a}_i$ на істинне a_i число, тобто виправлення неправильного $\tilde{A}_{СЗК}$ числа (отримання правильного числа $A_{СЗК} = \tilde{A}_{випр.}$).

Ступінь R інформаційної надмірності (коригувальні здібності коду) оцінюється величиной МКВ $d_{\min}^{(ПСЧ)}$. У СЗК, як відзначалося вище, значення МКВ визначається співвідношенням $d_{\min}^{(СЗК)} = k + 1$, де k – кількість

контрольних основ у впорядкованому СЗК.

Розглянемо НКС $A_{СЗК} = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n \| ... \| a_{n+k})$ у СЗК з мінімальною $(k = 1)$ додатковою інформаційною надмірністю. У цьому випадку визначено, що $d_{\min}^{(СЗК)} = 2$. Відповідно до загальної теорії завадостійкого кодування у ПСЧ при мінімальній кодовій відстані $d_{\min}^{(ПСЧ)} = 2$ у кодовій структурі однозначно (достовірно) визначається одноразова помилка. У ПСЧ під одноразовою помилкою даних розуміється спотворення одного біта інформації типу $0 \to 1$ чи $1 \to 0$. Для виправлення цієї одноразової помилки в ПСЧ необхідно забезпечити умову, щоб $d_{\min}^{(ПСЧ)} = 3$.

У СЗК, на відміну від ПСЧ, під одноразовою помилкою розуміється спотворення одного залишку a_i по модулю m_i. Оскільки залишок a_i числа $A_{СЗК} = (a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n \| a_{n+1})$ по модулю m_i містить $z = \{[\log_2(m_i - 1)] + 1\}$ – двійкових розрядів, то формально можна вважати, що у СЗК при, $d_{\min}^{(СЗК)} = 2$ $(k = 1)$ у межах одного залишку a_i можна виявити пачку помилок не більше ніж із z двійкових розрядів. Проте у літературі [24] показано, що у деяких випадках при значенні $d_{\min}^{(СЗК)} = 2$ у СЗК є можливість виправлення одноразових помилок.

З урахуванням специфіки, властивостей і особливостей представлення НКС у СЗК можливість виправлення помилок при $d_{\min}^{(СЗК)} = 2$ можна спробувати пояснити таким чином.

1. Під одноразовою помилкою у ПСЧ та СЗК розуміються різні поняття. Це було показано вище. У зв'язку з цим МКВ $d_{\min}^{(ПСЧ)}$ для ПСЧ і $d_{\min}^{(СЗК)}$ для СЗК має різне смислове навантаження і кількісну оцінку.

2. Існуюча (у неявному виді) у НКС натуральна (первинна, природна) інформаційна надмірність, що присутня у залишках $\{a_i\}$ за рахунок процедури формування цих залишків, позитивно (з точки зору підвищення завадостійкості та достовірності передачі та обробки інформації) починає

проявлятися тільки за наявності штучної (вторинною) інформаційної надмірності. Штучна інформаційна надмірність вводиться у НКС за рахунок використання (додатково до n інформаційних) k контрольних основ СЗК. Відмітною особливістю СЗК є істотне проявлення первинної інформаційної надмірності тільки за наявності вторинної, за рахунок введення контрольних основ.

3. У [44, 47, 97] показано, що коригувальний код, у СЗК з попарно простими основами має значення МКВ, яка дорівнює величині $d_{\min}^{(СЗК)}$ тільки у тому випадку, якщо ступінь інформаційної надмірності не менше добутку будь-яких $d_{\min}^{(СЗК)}-1$ основ заданих СЗК.

Наявність і взаємодія первинної та вторинної інформаційної надмірності, при проведенні додаткових процедур (використання тимчасової надмірності) у процесі виправлення помилок, забезпечує, у деяких випадках, можливість виправлення одноразових помилок у СЗК при $d_{\min}^{(СЗК)}=2$ (при $k=1$).

Дійсно, для впорядкованої СЗК, можна зробити наступні висновки: при однії $(k=1)$ контрольній m_{n+1} основі СЗК НКС $A=(a_1 \| a_2 \| ... \| a_{i-1} \| a_i \| a_{i+1} \| ... \| a_n \| a_{n+1})$ може мати різне значення $d_{\min}^{(СЗК)}$. У даному випадку це залежить від величини контрольної m_{n+1} основи. Якщо для кожного окремого модуля СЗК виконується умова $m_i < m_{n+1}$ $(i=\overline{1,n})$, то тоді, можна зробити висновок, що $d_{\min}^{(СЗК)}=2$, тобто маємо, що $t_{вияв.}=1$. Якщо для сукупності $\{m_i\}$ інформаційних основ для довільної пари модулів виконується умова $m_i \cdot m_j < m_{n+1}$ $(i,\ j=\overline{1,n};\ \ i \neq j)$, то у цьому випадку $d_{\min}^{(СЗК)}=3$ та $t_{вияв.}=2$.

Таким чином, для НКС у СЗК з $k=1$, МКВ $d_{\min}^{(СЗК)}$ може бути різною залежно від величини контрольної m_{n+1} основи СЗК.

Нехай задана СЗК інформаційними основами $m_1=3$, $m_2=4$, $m_3=5$,

$m_4 = 7$ і нехай $m_k = m_{n+1} = m_5 = 11$. У цьому випадку можна провести достовірний контроль спотворення одного будь-якого залишку НКС.

Нехай, наприклад, $m_k = m_{n+1} = 61$. Для цього випадку складемо табл. 1 відповідностей інформаційних і контрольної основ.

З табл. 1 видно, що специфіка представлення чисел у СЗК дозволяє у ряді випадків не лише виявити помилку, але й знайти місце її виникнення, використовуючи тільки одну контрольну основу, що неможливо при існуючих методах контролю і корекції у ПСЧ.

Нехай у неправильному ($\tilde{A} \geq M$) числі $\tilde{A} = (a_1 \| a_2 \| \ldots \| a_{i-1} \| \tilde{a}_i \| a_{i+1} \| \ldots \| a_n \| a_{n+1})$, помилка $\tilde{a}_i = (a_i + \Delta a_i) \bmod m_i$ достовірно міститься у залишку $\tilde{a}_i$ по модулю m_i.

Таблиця 6.1

Результати досліджень коригувальних можливостей завадостійких кодів у СЗК ($l = 1$)

$m_k = m_{n+1} = m_5 = 61;\ d_{\min}^{(СЗК)} = k+1 = 2,\ \prod_{i=1}^{3} m_i \leq m_5$.							max кількість помилок даних, що виявляються, у СЗК	max кількість помилок даних, що виправляються, у СЗК
Інформаційні основи СЗК				$\prod_{r=1}^{k'} m_{i_r} \leq m_{n+1}$	k'	$d_{\min}^{(СОК)'} = k'+1$		
$m_1 = 3$	$m_2 = 4$	$m_3 = 5$	$m_4 = 7$					
+	–	–	–	$3 < 61$	1	2	1	0
–	+	–	–	$4 < 61$	1	2	1	0
–	–	+	–	$5 < 61$	1	2	1	0
–	–	–	+	$7 < 61$	1	2	1	0
+	+	–	–	$3 \cdot 4 = 12 < 61$	2	3	2	1
+	–	+	–	$3 \cdot 5 = 15 < 61$	2	3	2	1
+	–	–	+	$3 \cdot 7 = 21 < 61$	2	3	2	1
–	+	+	–	$4 \cdot 5 = 20 < 61$	2	3	2	1
–	+	–	+	$4 \cdot 7 = 28 < 61$	2	3	2	1
–	–	+	+	$5 \cdot 7 = 35 < 61$	2	3	2	1
+	+	+	–	$3 \cdot 4 \cdot 5 = 60 < 61$	3	4	3	2

Розглянемо співвідношення, за допомогою якого можна виправити помилку у цьому залишку $\tilde{a}_i$ [178].

Очевидно, що

$$\tilde{A} = \left(A + \Delta A\right) \bmod M_0 . \tag{6.13}$$

З урахуванням того, що величину помилки можна представити у виді $\Delta A = (0 \,\|\, 0 \,\|\, ... \,\|\, 0 \,\|\, \Delta a_i \,\|\, 0 \,\|\, ... \,\|\, 0 \,\|\, 0)$, тоді правильне ($A < M$) число A можна визначити у наступному вигляді:

$$A = (\tilde{A} - \Delta A) \bmod M_0 = \left[\left(a_1 \,\|\, a_2 \,\|\, ... \,\|\, a_{i-1} \,\|\, \tilde{a}_i \,\|\, a_{i+1} \,\|\, ... \,\|\, a_n \,\|\, a_{n+1}\right) - \right.$$

$$\left. - \left(0 \,\|\, 0 \,\|\, ... \,\|\, 0 \,\|\, \Delta a_i \,\|\, 0 \,\|\, ... \,\|\, 0 \,\|\, 0\right)\right] \bmod M_0 =$$

$$= [a_1 \,\|\, a_2 \,\|\, ... \,\|\, a_{i-1} \,\|\, (\tilde{a}_i - \Delta a_i) \bmod m_i \,\|\, a_{i+1} \,\|\, ... \,\|\, a_n \,\|\, a_{n+1}] \bmod M_0 .$$

Кількісно оцінимо значення A. Оскільки число A правильне, тобто знаходиться у числовому інтервалі [0, M), тоді повинна виконуватися наступна нерівність

$$A = \left(\tilde{A} - \Delta A\right) \bmod M_0 < M . \tag{6.14}$$

З урахуванням того, що величина ΔA помилки дорівнює значенню $\Delta A = \Delta a_i \cdot B_i$, то нерівність (6.14) матиме наступний вигляд:

$$\tilde{A} - \Delta a_i \cdot B_i - r \cdot M_0 < M \text{ або}$$

$$\tilde{A} - \Delta a_i \cdot B_i - r \cdot M_0 < M_0 / m_{n+1} (r = 1, 2, 3, ...),$$

$$\tilde{A} - (\tilde{a}_i - a_i) \cdot B_i - r \cdot M_0 < M_0 / m_{n+1},$$

$$\tilde{A} - (a_i - \tilde{a}_i) \cdot B_i - r \cdot M_0 < M_0 / m_{n+1},$$

$$(a_i - \tilde{a}_i) \cdot B_i < M_0 / m_{n+1} - \tilde{A} + r \cdot M_0,$$

$$a_i - \tilde{a}_i < (M_0 / m_{n+1}) / B_i - \tilde{A} / B_i + r \cdot M_0 / B_i,$$

$$a_i < \tilde{a}_i + (M_0 / m_{n+1}) / B_i - \tilde{A} / B_i + r \cdot M_0 / B_i. \qquad (6.15)$$

З урахуванням того, що ортогональний базис для модуля m_i СЗК представляється у вигляді $B_i = \bar{m}_i \cdot M_0 / m_i$, то вираз (6.15) набере вигляду:

$$a_i < \tilde{a}_i + (m_i + r \cdot m_i \cdot m_{n+1}) / (\bar{m}_i \cdot m_{n+1}) - \tilde{A} / B_i \qquad \text{або}$$

$$a_i < \tilde{a}_i + m_i (1 + r \cdot m_{n+1}) / (\bar{m}_i \cdot m_{n+1}) - \tilde{A} / B_i, \qquad (6.16)$$

де $\bar{m}_i$ – вага ортогонального базису ($\bar{m}_i \delta_i \equiv 1 (\mathrm{mod}\, m_i)$, $M_i = \dfrac{M}{m_i}$, $\dfrac{M_i}{m_i} \equiv \delta_i (\mathrm{mod}\, m_i)$).

Оскільки значення залишку a_i є натуральне число, то значення $m_i (1 + r \cdot m_{n+1}) / (\bar{m}_i \cdot m_{n+1}) - \tilde{A} / B_i$ у виразі (6.16) має бути цілим числом. Тому узявши цілу частину останнього співвідношення, отримаємо формулу для виправлення помилки у залишку $\tilde{a}_i$ числа $\tilde{A}$ у вигляді

$$a_i = \left(\tilde{a}_i + [m_i \cdot (1 + r \cdot m_{n+1}) / (\bar{m}_i \cdot m_{n+1}) - \tilde{A} / B_i] \right) \mathrm{mod}\, m_i. \qquad (6.17)$$

На рис. 6.1 представлений метод виправлення помилок даних у СЗК.

Розглянемо приклади контролю і корекції даних у СЗК.

Приклад 6.1. Здійснити контроль і, при необхідності, провести корекцію числа $A_{СЗК} = (0 \| 0 \| 0 \| 0 \| 5)$, яке задане у СЗК з інформаційними $m_1 = 3$, $m_2 = 4$, $m_3 = 5$, $m_5 = 7$ і контрольною $m_k = m_5 = 11$ основами. При

цьому $M = \prod_{i=1}^{n} m_i = \prod_{i=1}^{4} m_i = 420$ і $M_0 = M \cdot m_{n+1} = 420 \cdot 11 = 4620$. Ортогональні базиси B_i $(i = \overline{1, n+1})$ СЗК представлені у розділі 4 табл. 4.6.

Рис. 6.1 Метод виправлення помилок даних у СЗК

І. Контроль даних $A_{СЗК} = (0 \| 0 \| 0 \| 0 \| 5)$. Відповідно до процедури контролю визначимо значення

$$A_{ПСЧ} = \left(\sum_{i=1}^{n+1} a_i \cdot B_i \right) \bmod M_0 = \left(\sum_{i=1}^{5} a_i \cdot B_i \right) \bmod M_0 =$$

$$= (0 \cdot 1540 + 0 \cdot 3465 + 0 \cdot 3696 + 0 \cdot 2640 + 5 \cdot 2520) \bmod 4620 =$$

$$= (5 \cdot 2520) \bmod 4620 = 12600 (\bmod 4620) = 3360 > 420 .$$

При можливості виникнення тільки одноразових помилок, робиться висновок про те, що дане число $\tilde{A}_{3360} = (0 \,\|\, 0 \,\|\, 0 \,\|\, 0 \,\|\, 5)$ неправильне $(3360 > M = 420)$.

Для виправлення числа $\tilde{A}_{3360} = (0 \,\|\, 0 \,\|\, 0 \,\|\, 0 \,\|\, 5)$ спочатку необхідно провести діагностику даних, тобто визначити спотворений $\tilde{a}_i$ залишок. Після чого необхідно визначити істинне значення a_i залишку по модулю m_i і після чого провести виправлення спотвореного $\tilde{a}_i$ залишку.

II. Діагностика даних $\tilde{A}_{3360} = (0 \,\|\, 0 \,\|\, 0 \,\|\, 0 \,\|\, 5)$. Відповідно до методу проекцій описаному у розділі 5.2 робимо висновок. У процесі діагностики даних, що представлені НКС $\tilde{A} = (0 \,\|\, 0 \,\|\, 0 \,\|\, 0 \,\|\, 5)$ визначилися точно не спотворені залишки: $a_2 = 0$ і $a_3 = 0$. Помилковими можуть бути залишки по основах m_1, m_4 і m_5, тобто залишки $\bar{a}_1 = 0$, $\bar{a}_4 = 0$ та $\bar{a}_5 = 5$. У цьому випадку необхідно провести виправлення залишків $\bar{a}_1$, $\bar{a}_4$ та $\bar{a}_5$.

III. Виправлення помилок даних $\tilde{A}_{3360} = (0 \,\|\, 0 \,\|\, 0 \,\|\, 0 \,\|\, 5)$. По формулі проведемо виправлення можливо спотворених ($\bar{a}_1$, $\bar{a}_4$ і $\bar{a}_5$) залишків (a_1, a_4 і a_5) де $r = 1, 2, 3, \ldots$.

Так маємо, що

$$a_1 = \left(\bar{a}_1 + \left[\frac{m_1 \cdot (1 + r \cdot m_{n+1})}{m_{n+1} \cdot \bar{m}_1} - \frac{\tilde{A}}{B_1} \right] \right) \bmod m_1 = \left(0 + \left[\frac{3 \cdot (1 + r \cdot 11)}{11 \cdot 1} - \frac{3360}{1540} \right] \right) \bmod 3 =$$

$$= (0 + [3,27 - 2,18]) \bmod 3 = (0 + [1,09]) \bmod 3 = (0 + 1) \bmod 3 = 1;$$

$$a_4 = \left(\overline{a}_4 + \left[\frac{m_4 \cdot (1 + r \cdot m_{n+1})}{m_{n+1} \cdot \overline{m}_4} - \frac{\tilde{A}}{B_4} \right] \right) \bmod m_4 = \left(0 + \left[\frac{7 \cdot 12}{11 \cdot 4} - \frac{3360}{2640} \right] \right) \bmod 7 =$$

$$= (0 + [1,9 - 1,27]) \bmod 7 = (0 + [0,63]) \bmod 7 = (0 + 0) \bmod 7 = 0;$$

$$a_5 = \left(\overline{a}_5 + \left[\frac{m_{n+1} \cdot (1 + r \cdot m_{n+1})}{m_{n+1} \cdot \overline{m}_{n+1}} - \frac{\tilde{A}}{B_5} \right] \right) \bmod m_{n+1} = \left(5 + \left[\frac{11 \cdot (1 + 11)}{11 \cdot 6} - \frac{3360}{2520} \right] \right) \bmod 11 =$$

$$= (5 + [2 - 1,3]) \bmod 11 = (5 + [0,7]) \bmod 11 = (5 + 0) \bmod 5 = 0.$$

По отриманих залишках $a_1 = 1$, $a_4 = 0$ та $a_5 = 0$ відновлюємо (виправляємо) спотворене число $\tilde{A}_{3360} = (0 \,\|\, 0 \,\|\, 0 \,\|\, 0 \,\|\, 5)$ тобто правильне число матиме наступний вигляд: $\tilde{A}_{випр.} = (1 \,\|\, 0 \,\|\, 0 \,\|\, 0 \,\|\, 5)$.

Для перевірки правильності виправлення даних, по відомій формулі, визначимо значення числа $\tilde{A}_{випр.} = (1 \,\|\, 0 \,\|\, 0 \,\|\, 0 \,\|\, 5)$ таким чином

$$\tilde{A}_{випр.ПСЧ} = \left(\sum_{i=1}^{5} a_i \cdot B_i \right) \bmod M_0 =$$

$$= (1 \cdot 1540 + 0 \cdot 3465 + 0 \cdot 3696 + 0 \cdot 2640 + 5 \cdot 2520) \bmod 4620 =$$

$$= 14140 (\bmod 4620) = 280.$$

Оскільки $280 < M = 420$, то число $\tilde{A}_{280} = (1 \,\|\, 0 \,\|\, 0 \,\|\, 0 \,\|\, 5)$ – правильне.

З метою уточнення правильності процедури корекції числа $\tilde{A}_{3360}$ проведемо розрахунок та порівняння значень правильних залишків $a_2 = 0$ і $a_3 = 0$. У цьому випадку маємо $a_2 = \left(0 + \left[\frac{4 \cdot (1 + 11)}{11 \cdot 3} - \frac{3360}{3465} \right] \right) \bmod 4 = 0$ та $a_3 = \left(0 + \left[\frac{5 \cdot (1 + 11)}{11 \cdot 4} - \frac{3360}{3696} \right] \right) \bmod 5 = 0$.

Отримані результати $a_2 = 0$ та $a_3 = 0$ розрахунків залишків по модулях m_2 та m_3 СЗК, підтверджують правильність корекції неправильного числа

$\tilde{A}_{3360} = (0 \| 0 \| 0 \| 0 \| 5)$. Таким чином, вихідне число $\tilde{A}_{СЗК} = (0 \| 0 \| 0 \| 0 \| 5)$ є неправильним $\tilde{A}_{3360}$ у якому одноразова помилка $\Delta a_1 = 1$ сталася по модулю m_1. Ця помилка перевела правильне число A_{280} у неправильне $\tilde{A}_{3360}$.

Для того, щоб з'ясувати чи являється правильне число A_{280} істинним проведемо додаткові дослідження процесів спотворення та корекції числа A_{280} по основі $m_1 = 3$. Кількість $N_{НС}$ можливих неправильних (спотворених) $\tilde{A}_{СЗК}$ кодових слів (тільки при одноразовій помилці) для кожного правильного $A_{СЗК}$ числа дорівнює $N_{НС} = \sum_{i=1}^{n+1} m_i - (n+1)$.

Результати аналізу показали, що спотворення залишку a_1 по модулю $m_1 = 3$ правильного числа A_{280} може привести тільки до двох неправильних чисел $\tilde{A}_{3360} = (\tilde{0} \| 0 \| 0 \| 0 \| 5)$ і $\tilde{A}_{1820} = (\tilde{2} \| 0 \| 0 \| 0 \| 5)$. Цей факт говорить про те, що виправлене $A_{випр.} = A_{280} = (1 \| 0 \| 0 \| 0 \| 5)$ число є не лише правильним (що лежить в інтервалі [0, 420)), але й істинним. Істинність отриманого $A_{280} = (\hat{1} \| 0 \| 0 \| 0 \| 5)$ числа підтверджується тим, що тільки одноразова помилка $\Delta a_1 = 2$ по основі $m_1 = 3$ переводить це число

$$\tilde{A} = (A + \Delta A) \bmod M_0 = (1 \| 0 \| 0 \| 0 \| 5) + (2 \| 0 \| 0 \| 0 \| 0) =$$
$$= \left[(1+2) \bmod 3 \| 0 \| 0 \| 0 \| 5\right] = (\tilde{0} \| 0 \| 0 \| 0 \| 5)$$

у єдино неправильне число $\tilde{A}_{3360} = (\tilde{0} \| 0 \| 0 \| 0 \| 5)$ [179].

Приклад 6.2. Нехай правильне число дорівнює $A_{280} = (1 \| 0 \| 0 \| 0 \| 5)$ і нехай $\Delta a_1 = 1$. Тоді $\tilde{A} = (A + \Delta A) \bmod M_0 = (1 \| 0 \| 0 \| 0 \| 5) + (1 \| 0 \| 0 \| 0 \| 0) =$ $= \left[(1+1) \bmod 3 \| 0 \| 0 \| 0 \| 5\right] = (\tilde{2} \| 0 \| 0 \| 0 \| 5)$. Цьому числу у СЗК відповідає число 1820 у ПСЧ, тобто число $\tilde{A}_{1820}$ неправильне. Проведемо виправлення числа $\tilde{A}_{1820}$.

Перед виправленням числа $\tilde{A}_{1820}$ проведемо діагностику даних. Для цього заздалегідь складемо проекції A_j ($j=\overline{1,5}$) числа $\tilde{A}_{1820}=(2\,\|\,0\,\|\,0\,\|\,0\,\|\,5)$. Це будуть наступні кодові структури у СЗК: $\tilde{A}_1=(0\,\|\,0\,\|\,0\,\|\,5)$, $\tilde{A}_2=(2\,\|\,0\,\|\,0\,\|\,5)$, $\tilde{A}_3=(2\,\|\,0\,\|\,0\,\|\,5)$, $\tilde{A}_4=(2\,\|\,0\,\|\,0\,\|\,5)$ і $\tilde{A}_5=(2\,\|\,0\,\|\,0\,\|\,0)$.

Далі визначимо усі значення проекцій $\tilde{A}_{j\,ПСЧ}$:

$$\tilde{A}_{1\,ПСЧ}=(5\cdot 980)\bmod 1540=280<420=M;$$

$$\tilde{A}_{2\,ПСЧ}=(2\cdot 385+5\cdot 231)\bmod 1155=1925\left(\bmod 1155\right)=770>420=M;$$

$$\tilde{A}_{3\,ПСЧ}=(2\cdot 616+5\cdot 672)\bmod 924=4592\left(\bmod 924\right)=896>420=M;$$

$$\tilde{A}_{4\,ПСЧ}=(2\cdot 220+5\cdot 540)\bmod 660=3140\left(\bmod 660\right)=500>420=M;$$

$$\tilde{A}_{5\,ПСЧ}=2\cdot 280(\bmod 420)=560\left(\bmod 420\right)=140<420=M.$$

Оскільки $\tilde{A}_{2\,ПСЧ}$, $\tilde{A}_{3\,ПСЧ}$ і $\tilde{A}_{4\,ПСЧ}>420$, тоді робиться висновок про те, що залишки $a_2=0$, $a_3=0$ і $a_4=0$ числа $\tilde{A}_5=(2\,\|\,0\,\|\,0\,\|\,0\,\|\,5)$ не спотворені. Спотвореними $\overline{a}_1=2$ і $\overline{a}_5=5$ можуть бути тільки залишки a_1 і a_5. Спочатку проведемо виправлення залишку $\overline{a}_1=2$.

Маємо, що

$$a_1=\left(\overline{a}_1+\left[\frac{m_1\cdot(1+r\cdot m_{n+1})}{m_{n+1}\cdot\overline{m}_1}-\frac{\tilde{A}}{B_1}\right]\right)\bmod m_1=\left(2+\left[\frac{3\cdot(1+11)}{11\cdot 1}-\frac{1820}{1540}\right]\right)\bmod 3=$$

$$=\left(2+[3{,}27-1{,}18]\right)\bmod 3=\left(2+[2{,}09]\right)\bmod 3=(2+2)\bmod 3=4(\bmod 3)=1.$$

Таким чином, виправлений залишок по модулю m_1 дорівнює $a_1=1$.

Аналогічним чином отримаємо значення $a_5=5$. По отриманих залишках a_1, a_5 виправляємо неправильне число $\tilde{A}_{1820}=(\tilde{2}\,\|\,0\,\|\,0\,\|\,5)$.

Зрештою у процесі корекції отримаємо правильне $A_{280} = (1 \| 0 \| 0 \| 0 \| 5)$ число.

Приклад 6.3. Здійснити контроль числа $A_{СЗК} = (0 \| 0 \| 0 \| 2 \| 1)$. У разі його спотворення, провести діагностику і корекцію даних.

І. Контроль даних $A_{СЗК} = (0 \| 0 \| 0 \| 2 \| 1)$. Відповідно до відомої процедури контролю визначимо $A_{ПСС}$ по формулі

$$A_{ПСЧ} = \left(\sum_{i=1}^{n+1} a_i \cdot B_i \right) \bmod M_0 = (0 \cdot 1540 + 0 \cdot 3465 + 0 \cdot 3696 + 2 \cdot 2640 +$$

$$+1 \cdot 2520) \bmod 4620 = 7800 (\bmod 4620) = 3180 > 420 .$$

Це число неправильне $\tilde{A}_{3180}$.

ІІ. Діагностика даних $\tilde{A}_{3180} = (0 \| 0 \| 0 \| 2 \| 1)$. Складемо усі можливі проекції $\tilde{A}_j$ числа $\tilde{A}_{3180}$: $\tilde{A}_1 = (0 \| 0 \| 2 \| 1)$, $\tilde{A}_2 = (0 \| 0 \| 2 \| 1)$, $\tilde{A}_3 = (0 \| 0 \| 2 \| 1)$, $\tilde{A}_4 = (0 \| 0 \| 0 \| 1)$ і $\tilde{A}_5 = (0 \| 0 \| 0 \| 2)$.

Визначимо значення величин усіх п'яти проекцій $\tilde{A}_j$ у ПСЧ:

$$\tilde{A}_{1СЗК} = (0 \| 0 \| 2 \| 1) = \tilde{A}_{1ПСС} = (a_1 \cdot B_{11} + a_2 \cdot B_{21} + a_3 \cdot B_{31} + a_4 \cdot B_{41}) \bmod M_1 =$$

$$= (0 \cdot 385 + 0 \cdot 616 + 2 \cdot 1100 + 1 \cdot 980) \bmod 1540 = 100 < M = 420 ;$$

$$\tilde{A}_{2СЗК} = (0 \| 0 \| 2 \| 1) = \tilde{A}_{2ПСС} = (a_1 \cdot B_{12} + a_2 \cdot B_{22} + a_3 \cdot B_{32} + a_4 \cdot B_{42}) \bmod M_2 =$$

$$= (0 \cdot 385 + 0 \cdot 231 + 2 \cdot 330 + 1 \cdot 210) \bmod 1155 = 870 > M = 420 ;$$

$$\tilde{A}_{3СЗК} = (0 \| 0 \| 2 \| 1) = \tilde{A}_{3ПСС} = (a_1 \cdot B_{13} + a_2 \cdot B_{23} + a_3 \cdot B_{33} + a_4 \cdot B_{43}) \bmod M_3 =$$

$$= (0 \cdot 616 + 0 \cdot 693 + 2 \cdot 792 + 1 \cdot 672) \bmod 924 = 418 < M = 420 ;$$

$$\tilde{A}_{4СЗК} = (0 \| 0 \| 0 \| 1) = \tilde{A}_{4ПСС} = (a_1 \cdot B_{14} + a_2 \cdot B_{24} + a_3 \cdot B_{34} + a_4 \cdot B_{44}) \bmod M_4 =$$

$$= (0 \cdot 220 + 0 \cdot 165 + 2 \cdot 396 + 1 \cdot 540) \bmod 660 = 540 > M = 420 ;$$

$$\tilde{A}_{5СЗК} = (0 \| 0 \| 0 \| 2) = \tilde{A}_{5ПСС} = (a_1 \cdot B_{15} + a_2 \cdot B_{25} + a_3 \cdot B_{35} + a_4 \cdot B_{45}) \bmod M_5 =$$

$$= (0 \cdot 280 + 0 \cdot 105 + 2 \cdot 336 + 1 \cdot 120) \bmod 420 = 240 < M = 420 .$$

У результаті розрахунків значень $\tilde{A}_{j\,ПСЧ}$ і порівняння їх з величиною $M = 420$ довжини інтервалу $[0,420)$ обробки правильних чисел $A_{СЗК}$ у СЗК отримаємо наступне. Сукупність залишків $a_2 = 0$, $a_4 = 0$ є правильною (залишки не спотворені), а залишки $\bar{a}_1 = 0$, $\bar{a}_3 = 0$ і $\bar{a}_5 = 1$ неправильного числа $\tilde{A}_{3180} = (0 \,\|\, 0 \,\|\, 0 \,\|\, 2 \,\|\, 1)$ можуть бути спотворені (можуть бути неправильними).

III. Виправлення можливо спотворених $\bar{a}_1$, $\bar{a}_3$ і $\bar{a}_5$ залишків числа $\tilde{A}_{3180}$.

Необхідно виправити, можливо, спотворені залишки $\bar{a}_1 = 0$, $\bar{a}_3 = 0$ і $\bar{a}_5 = 1$ по формулі $a_i = \left(\tilde{a}_i + \left[\frac{m_i \cdot (1 + r \cdot m_{n+1})}{m_{n+1} \cdot \bar{m}_i} - \frac{\tilde{A}}{B_i} \right] \right) \bmod m_i$. Тоді маємо, що

$$a_1 = \left(\bar{a}_1 + \left[\frac{m_1 \cdot (1 + r \cdot m_{n+1})}{m_{n+1} \cdot \bar{m}_1} - \frac{\tilde{A}}{B_1} \right] \right) \bmod m_1 = \left(0 + \left[\frac{3 \cdot (1 + r \cdot 11)}{11 \cdot 1} - \frac{3180}{1540} \right] \right) \bmod 3 =$$

$$= \left(0 + \left[3{,}27 - 2{,}06\right]\right) \bmod 3 = \left(0 + \left[1{,}21\right]\right) \bmod 3 = \left(0 + 1\right) \bmod 3 = 1.$$

Таким чином $a_1 = 1$.

Для значення $\bar{a}_3$ маємо

$$a_3 = \left(\tilde{a}_3 + \left[\frac{m_3 \cdot (1 + r \cdot m_{n+1})}{m_{n+1} \cdot \bar{m}_3} - \frac{\tilde{A}}{B_3} \right] \right) \bmod m_3 = \left(0 + \left[\frac{5 \cdot (1 + r \cdot 11)}{11 \cdot 4} - \frac{3180}{3696} \right] \right) \bmod 5 =$$

$$= \left(0 + \left[1{,}36 - 0{,}86\right]\right) \bmod 5 = \left(0 + \left[0{,}5\right]\right) \bmod 5 = \left(0 + 0\right) \bmod 5 = 0.$$

В цьому випадку $a_3 = 0$.

Для значення залишку $\bar{a}_5$ отримаємо

$$a_5 = \left(\tilde{a}_5 + \left[\frac{m_5 \cdot (1 + r \cdot m_{n+1})}{m_{n+1} \cdot \bar{m}_5} - \frac{\tilde{A}}{B_5} \right] \right) \bmod m_5 = \left(1 + \left[\frac{11 \cdot (1 + r \cdot 11)}{11 \cdot 6} - \frac{3180}{2520} \right] \right) \bmod 11 =$$

$$= \left(1 + \left[2 - 1,26\right]\right) \bmod 11 = \left(1 + \left[0,74\right]\right) \bmod 11 = \left(1 + 0\right) \bmod 11 = 1.$$

Маємо, що $a_5 = 1$.

По отриманих значеннях $a_1 = 1$, $a_3 = 0$ і $a_5 = 1$ відновлених залишків виправляємо спотворене число $\tilde{A}_{СЗК} = (0 \| 0 \| 0 \| 2 \| 1)$ на правильне $A_{СЗК} = (1 \| 0 \| 0 \| 2 \| 1)$ число. Перевірка $100 < 420$.

Наявність у НКС одночасно первинної і вторинної інформаційної надмірності, у деяких випадках, може забезпечити можливість виправлення одноразових помилок у СЗК при МКВ, яка дорівнює $d_{\min}^{(KB)} = 2$.

Використання запропонованого методу виправлення помилок у НКС, що представлена у СЗК, дозволяє за рахунок паралельного виправлення помилок структури, що діагностується, у k разів підвищити оперативність корекції у СЗК. Де k – кількість можливих залишків НКС у яких сталися помилки.

6.3 Метод корекції помилок даних, що представлені у СЗК з двома контрольними основами

Розглянемо можливості коригувальних кодів за наявності двох контрольних основ. До системи основ $m_1, m_2, ..., m_n, m_{n+1}$ додамо основу $m_{n+2} > m_{n+1}$ і будемо представляти числа, що лежать у робочому діапазоні $[0, M]$, у системі, що має діапазон $[0, M_1)$, де

$$M_1 = m_{n+1} \cdot m_{n+2} \cdot M$$

Надалі діапазон M_1 називатимемо повним діапазоном системи з двома контрольними основами. Правильними вважатимемо, числа, що лежать у діапазоні $[0, M]$.

Перейдемо до розгляду методів, що забезпечують коригувальні можливості прийнятої системи.

Назвемо число A_{ij}, що отримане з A викреслюванням цифр по основам m_i та m_j – проекцією числа A по основам m_i та m_j. Якщо у системі основ $m_1, m_2, ..., m_n, m_{n+1}, m_{n+2}$ дві основи m_{n+1} та m_{n+2} є контрольними і, якщо число $A = (a_1 \| a_2 \| ... \| a_n \| a_{n+1} \| a_{n+2})$ є правильним, то усі проекції числа A по основам m_i та m_j рівні між собою і співпадають з величиною числа A, тобто $A_{ij} = A < M$ (при i, $j = 1, 2, ..., n+2, i \neq j$) і обернено, якщо усі проекції A_{ij} числа A рівні між собою і співпадають за величиною з числом A, то число A правильне.

Відмітимо, якщо у системі $m_1, m_2, ..., m_n, m_{n+1}, m_{n+2}$ з двома контрольними основами задано неправильне число $\tilde{A} = (\tilde{a}_1 \| \tilde{a}_2 \| ... \| \tilde{a}_i \| ... \| \tilde{a}_n \| \tilde{a}_{n+1} \| \tilde{a}_{n+1})$, то необхідною і достатньою умовою помилковості цифри $\tilde{a}_i$ у $\tilde{A}$, являється правильність його проекції $\tilde{A}_i$ по основі m_i.

З характеру розглянутих кодів видно їх повна арифметичність, тобто введені додатково основи включені у загальну систему основ і коди, що містять цифри по усіх як основних, так і контрольних розрядах, беруть участь у будь-якій операції арифметичного пристрою, обробка основних і додаткових цифр здійснюється абсолютно однаковим чином, без якої-небудь відмінності.

Це дозволяє вважати, що обробка інформації, що представлена у такого роду спеціальному коді, може вестись без контролю кожного окремого коду, лише поетапно, причому величина кожного етапу може визначатися у кожному окремому випадку, або по закінченому циклу обробки, або відповідно до ймовірності виникнення поодинокої помилки.

Кінцевий результат кожного етапу може бути підданий контролю і його правильність підтверджує правильність проведення усіх операцій цього

етапу.

У разі виявлення помилки робиться корекція і виправлений результат бере участь у подальших етапах. Можливість такого режиму обробки інформації еквівалентна подвійному прорахунку для виявлення помилки і потрійному прорахунку для її виправлення.

Розглянемо особливості контролю і корекції помилок при реалізації основних арифметичних операцій. Їх слід розглядати як двокомпонентні. Тобто позначимо i –ту елементарну операцію через E_i, а її компоненти – через A_i та B_i і запишемо операцію у виді

$$E_i = f_i(A_i, B_i)$$

(зокрема, може мати місце $A_i = B_i$).

Назвемо ланцюгом F сукупність операцій над компонентами $F(a_1 \| a_2 \| \ldots \| a_n)$, яка може бути представлена у вигляді суперпозиції таких двокомпонентних операцій з можливими повтореннями як самих a_j так і проміжних результатів виконання двокомпонентних операцій.

Передбачається, що у ланцюзі операцій відсутні розриви, розуміючи під цим той факт, що, за винятком кінцевого результату, не існує ніякого проміжного результату, який у подальшому не входив би у якості компонента принаймні в одну двокомпонентну операцію.

Так, наприклад,

$$F(a_1 \| a_2 \| \ldots \| a_n) = a_1 a_2 + a_2 a_3 + \ldots + a_{n-1} a_n$$

є ланцюгом в тому сенсі, як це було визначено вище. Дійсно, можна F записати у вигляді суперпозиції двокомпонентних операцій

$$F = f_2\{\ldots f_2\{ f_2[f_1(a_1, a_2),\ f_1(a_2, a_3)] f_1(a_3, a_4),\}\ldots\},$$

де f_1 – операція множення, f_2 – операція додавання.

Природно ввести у визначення ланцюга обмовку, що саме результат обчислення по усьому ланцюгу є кінцевим результатом, якій нас цікавить, а усі інші, що утворюються в ході обчислень – проміжні результати, що не мають самостійного значення і цікавлять нас постільки, поскільки вони беруть участь у формуванні кінцевого результату.

Тому, якщо у проміжних результатах містяться помилки, які можуть бути виправлені зрештою, можна обмежитися виправленням тільки цього останнього результату, не звертаючись до історії його отримання і не роблячи відновлення істинних значень проміжних результатів. Інакше кажучи, у ході роботи обчислювальної машини має бути забезпечене набуття істинного значення тільки кінцевого результату обчислення ланцюга.

З урахуванням вище сказаного при реалізації ланцюга може мати місце помилка тільки у цифрі по одній основі, тобто довжина ланцюга така, що при існуючих характеристиках надійності роботи апаратури арифметичного пристрою вірогідна наявність збою або відмови тільки по одній з основ. При цьому байдуже, чи мав місце по цій основі одиничний збій або сталося декілька збоїв.

При цьому стан кінцевого результату ланцюга характеризується таким чином. Нехай виконується деякий ланцюг раціональних операцій, істинний результат якого у разі відсутності помилок у ході обчислень має бути правильним числом, і нехай у процесі обчислення мали місце один або декілька збоїв по одній з основ системи. Тоді кінцевий результат ланцюга або неправильний, або істинний.

Дійсно, нехай прийнято представлення у системі основ $m_1, m_2, ..., m_n, m_{n+1}$ та істинним результатом має бути число $K = (\chi_1 \| \chi_2 \| ... \| \chi_i \| ... \| \chi_{n+1})$, а отримано число $A = (a_1 \| a_2 \| ... \| a_n \| a_{n+1})$.

Якщо збій мав місце по основі m_i, то $a_1 = \chi_1$, $a_2 = \chi_2$, ..., $a_{i-1} = \chi_{i-1}$, $\chi_{i+1} = \chi_{i+1}$, ..., $a_{n+1} = \chi_{n+1}$.

Що стосується a_i, то можливі два варіанти:

1. $a_i \neq \chi_i$;

2. $a_i = \chi_i$.

У варіанті 1 число A – неправильне, а у варіанті 2 число A – правильне, і при цьому співпадає з K, тобто A є істинним значенням кінцевого результату ланцюга.

Встановлений факт, здавалося б дуже простий, має, проте, важливе значення для організації контролю у КСКОЦД, яка працює у системі залишкових класів. Він свідчить про те, що у кінцевий результат обчислення ланцюга не може проникнути невиявлена помилка, оскільки це могло б статися тільки у тому випадку, коли результат обчислень був би правильним, але у той же час не істинним числом. Проте правильним числом може бути тільки істинний результат.

Таким чином, помилка, якщо вона на якому-небудь етапі реалізації ланцюга мала місце, або збережеться до кінця обчислення ланцюга і проявить себе неправильністю кінцевого результату, що легко виявляється, або у процесі подальших, після свого виникнення, обчислень самоусунеться і тоді буде отриманий потрібний кінцевий результат.

Самоусунення помилки може статися не лише у разі накладення декількох збоїв по цій основі, але також і при одиничному збої. Так, наприклад, якщо на якому-небудь етапі обчислення ланцюга вже після виникнення збою по основі m_i проміжний результат множився на число, що має нульову цифру по m_i, то, очевидно, добуток вийде істинним числом і таким вже увійде до подальших обчислень, що за відсутності подальших збоїв, природно, приведе до отримання істинного кінцевого результату.

6.4 Метод оперативної корекції помилок у СЗК у динаміці обчислювального процесу КСКОЦД

Як відзначалось у попередніх розділах, якщо СЗК впорядкована ($m_k < m_{k+1}$), то $d_{\min} = k+1$, а якщо СЗК розширюється шляхом додавання k основ і кожна основа більше будь-якої інформаційної основи, то мінімальна відстань коду автоматично збільшується на величину k. Збільшити $d_{\min}$ можна також за рахунок зменшення числа інформаційних основ, тобто за рахунок переходу до обчислень з меншою точністю. Таким чином, між коригувальними можливостями *R*-кодів і точністю обчислень існує обернено пропорційна залежність. Один і той же обчислювач може виконувати арифметичні операції з високою точністю, але невеликою надійністю або з меншою точністю, але з більш високою надійністю і швидкістю (швидкодія виконання основних операцій у СЗК обернено пропорційно до числа інформаційних основ).

З характеру розглянутого *R*-коду видно його повна арифметичність:

– введені основи включені у загальну систему основ СЗК і коди, що містять цифри по усіх як основних, так і контрольних розрядах беруть участь у будь-якій операції;

– обробка основних і додаткових цифр здійснюється абсолютно однаково, без якої-небудь різниці.

Це дозволяє вважати, що обробка інформації у СЗК може вестись без контролю кожного отриманого проміжного результату. Величина (довжина) етапу контролю визначається у кожному окремому випадку або по закінченому циклу обробки масиву інформації, або відповідно до ймовірності виникнення поодинокої помилки. Кінцевий результат обчислень кожного етапу може бути підданий контролю і його правильність підтверджує правильність проведення усіх операцій цього етапу. Відмітимо, що введення тільки однієї контрольної основи дозволяє виявити не лише

будь-яку поодиноку помилку, як і у позиційній системі числення, але і велику частину подвійних.

Відмітною особливістю СЗК, являється істотний прояв первинної інформаційної надмірності при введенні вторинної $Q(l)$ (за рахунок наявності контрольних основ СЗК)

$$Q(l) = \prod_{j=1}^{l} m_{Z_i} .$$

Покажемо, що R–код може виявляти деяке число помилок більш високої кратності, ніж та, яка допускається загальною теорією кодування, тобто значенням $d_{\min}$. Нехай для СЗК мінімальна кодова відстань визначається значенням $d_{\min}$. Припустимо, що у СЗК є такі основи, число яких $l \geq d_{\min}$, при цьому

$$Q(l) = \prod_{j=1}^{l} m_{Z_i} < R = M_1 / M.$$

Тоді у вектору помилки $\Delta A = \tilde{A} - A$ повинно бути не менше $n - l$ нульових компонент. Представимо вектор ΔA у вигляді

$$\Delta A = \left(0 \,\|\, 0 \,\|\, \ldots \,\|\, \Delta\alpha_{Z_1} \,\|\, \ldots \,\|\, 0 \,\|\, \Delta\mathrm{A}\alpha_{Z_l} \,\|\, \ldots \,\|\, 0\right).$$

У позиційній системі числення ΔA визначається як

$$\Delta A = B_{Z_1} a_{Z_1} + \ldots + B_{Z_l} a_{Z_l} .$$

Враховуючи, що $B_{Z_l} = \bar{m}_{Z_l} M_1 / m_{Z_l}$, де $\bar{m}_{Z_l}$ – вага l–ортогонального

базису, запишемо

$$\Delta A = \frac{\bar{m}_{Z_1} M_1}{m_{Z_1}} a_{Z_1} + \cdots + \frac{\bar{m}_{Z_l} \mathrm{M}_l}{m_{Z_l}} \alpha_{Z_l} = R\Delta R \cdot Z, \qquad (6.19)$$

де

$$R \cdot \Delta R = \frac{M_1}{Q(l)};\ Z = \sum_{j=1}^{l} \bar{m}_{Z_j} Q_j(l)$$

та

$$Q_j(l) = \frac{Q(l)}{m_{Z_j}} \left(\mathrm{M}_1 = R \cdot \Delta R \cdot Q_j(l) \cdot m_{Z_j} \right).$$

З виразу (6.19) очевидно, що

$$\Delta A = 0 \left[\mathrm{mod}\, \mathrm{M}_1 / \alpha(l) \right],$$

тоді

$$\Delta \mathrm{A} / Z_0 = R\Delta R = \mathrm{M}_1 / Q(l) \geq \mathrm{M}_1 / R = \mathrm{M}, \qquad (6.20)$$

де

$$Z_0 = 1, 2, \ldots$$

З (6.20) витікає, що $\Delta A \geq M$ і, таким чином

$$\tilde{A} = A - \Delta A \geq M . \qquad (6.21)$$

Нерівність (6.21) показує, що сума будь-якого числа A і числа того, що відповідає вектору помилки ΔA, не може належати множині M, тобто подібну помилку можна виявити. Відмітимо, що навіть в тих випадках, коли $Q(l) > R$ серед помилок ΔA знайдуться такі, які задовольняють нерівності (6.21). Це можливо за рахунок наявності вторинної інформаційної надмірності ΔR. Специфіка представлення чисел у СЗК дозволяє у ряді випадків не лише виявити помилку, але і знайти місце її виникнення, використовуючи тільки контрольну основу, що неможливо при існуючих методах контролю і корекції у ПСЧ, наприклад, при контролю по модулю.

Виходячи з цього, розглянемо алгоритм виправлення помилок КСКОЦД у СЗК. Введемо ще одну контрольну основу $m_{n+2} > m_{n+1}$. У цьому випадку повний діапазон СЗК визначається як $M_2 = M_1 m_{n+2}$.

1. Обчислюються усі проекції числа

$$\tilde{A} = (\alpha_1 \| \alpha_2 \| \ldots \| \alpha_n \| \alpha_{n+1} \| \alpha_{n+2})$$

по усіх основах СЗК

$$\tilde{A}_1 = (\alpha_2 \| \alpha_3 \| \ldots \| \alpha_n \| \alpha_{n+1} \| \alpha_{n+2}),$$
$$\tilde{A}_2 = (\alpha_1 \| \alpha_3 \| \ldots \| \alpha_n \| \alpha_{n+1} \| \alpha_{n+2}),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\tilde{A}_{n+1} = (\alpha_1 \| \alpha_2 \| \ldots \| \alpha_n \| \alpha_{n+2}),$$
$$\tilde{A}_{n+2} = (\alpha_1 \| \alpha_2 \| \ldots \| \alpha_n \| \alpha_{n+1}).$$

2. Отримані проекції $\tilde{A}_i$ $(i = \overline{1, n+2})$ порівнюються з робочим діапазоном M.

3. Визначаємо проекцію числа, для якої $\tilde{A}_i < M$, і виправляємо помилковий залишок по формулі

$$\alpha_i = \left(\tilde{\alpha}_i + \left[\frac{m_i \left(1 + j m_{n+1}\right)}{m_{n+1} m_i} - \frac{\tilde{\mathrm{A}}}{\mathrm{B}_i} \right] \right) \bmod m_i .$$

6.5 Метод оперативної корекції помилок даних у СЗК, яка представлена взаємно непростими основами

Якщо відомо, що R-коди мають добрі коригуючі можливості, то L-коди потребують додаткових досліджень їх практичного застосування.

У літературі L-коди описуються швидше якісно, чим кількісно. Річ у тому, що до теперішнього часу ніхто не займався глибоким вивченням властивостей систем залишкових класів, основи яких не є взаємно простими числами. Подібна система теж має певні коригувальні властивості, що обумовлює необхідність оцінки можливості і доцільності застосування таких систем для підвищення надійності КСКОЦД [44, 180, 181].

Сума, різниця і добуток будь-яких векторів лінійного коду є кодовими словами. У цьому випадку некодовим словам не можна поставити у відповідність деякі натуральні числа. Покажемо, що корекція помилок у СЗК за допомогою L-кодів призводить до апаратурної надмірності, еквівалентної резервуванню. Всі методи та алгоритми контролю та корекції даних у СЗК, що представлена за допомогою L-кодів, основуються на сукупності наступних наукових тверджень [44]. Розглянемо твердження 6.2.

Твердження 6.2. Для того, щоб L-код мав мінімальну відстань $d_{\min}$ необхідно і достатньо, щоб ступінь надмірності задовольняла співвідношенню

$$R = M^{d_{\min}-1}.$$

З твердження 6.2 витікає, що корекція довільних помилок інформації у СЗК за допомогою L-кодов призводить до великої надмірності, еквівалентної резервуванню.

Таким чином, малоефективно використати лінійні коди для корекції помилок, яким з рівною імовірністю відповідають довільні спотворення залишків кодових слів у СЗК. Проте, якщо обмежити клас можливих помилок в окремих залишках кодових слів, можливості L-кодов істотно розширюються.

Розглянемо лему 6.1. Для будь-якого цілого числа $A=(a_1 \| a_2 \| ... \| a_n)$ у системі залишкових класів з основами m_i $(i=\overline{1,n})$ і для будь-якої пари основ m_i і m_j повинна виконуватися умова

$$(a_i - a_j) \equiv 0 (\mathrm{mod}\, d_{ij})$$

де $d_{ij}(m_i, m_j)$ найбільший загальний дільник основ m_i та m_j $(i, j=\overline{1,n}$; $i \neq j)$.

Для визначення необхідних і достатніх умов для виявлення одноразових помилок за допомогою L-кодів за результатами леми 6.1 сформульовано і доведено наступне твердження.

Твердження 6.3. Для виявлення помилок у залишку по довільній основі m_i $(i=\overline{1,n})$ числа $A=(a_1 \| a_2 \| ... \| a_n)$, яке задано у системі залишкових класів з основами $m_1, ..., m_n$ необхідно, щоб основа m_i мала хоч б один, відмінний від одиниці, загальний дільник з іншими основами m_i $(i \neq j)$.

Доказ. Нехай НЗД $d_{ij}(m_i, m_j)$ визначений для довільних основ СЗК $(i \neq j)$ і помилка сталася по основі m_i, тобто $a_i = a_i + \Delta a_i$. Покажемо, що

вираз $(a_i - a_j) \bmod d_{ij}$ еквівалентний $\Delta a_i (\bmod d_{ij})$. Згідно з лемою виконується наступна рівність

$$(a_i - a_j) = 0 (\bmod d_{ij}).$$

Запишемо вираз

$$a_i + \Delta a_i = a_i (\bmod m_i)$$

у виді

$$a_i + \Delta a_i = m \cdot m_i + a_i,$$

де m – ціле число.

З останнього виразу визначимо спотворений залишок

$$a_i = a_i + \Delta a_i - m \cdot m_i.$$

Тоді можна записати

$$a_i - a_j = \left[(a_i - a_j) + (-mkd_{ij}) + \Delta a_i \right].$$

Оскільки

$$(a_i - a_j) \equiv 0 (\bmod d_{ij}) \text{ і } -mkd_{ij} \equiv 0 (\bmod d_{ij}),$$

де $m_i = kd_{ij}$, а k – натуральне число, то

$$(a_i - a_j) \equiv \Delta a_i (\mathrm{mod}\, d_{ij}).$$

Очевидно, що за відсутності загальних дільників, тобто якщо $d_{ij} = 1$, тоді $\Delta a_i \equiv (\mathrm{mod}\, d_{ij})$. Це і доводить необхідну умову теореми.

Необхідна умова теореми є достатньою, якщо помилка не кратна дільникові d_{ij}.

Дійсно,

$$(md_{ij} + a_{ij}) \neq 0 (\mathrm{mod}\, d_{ij}),$$

для $0 < a_{ij} < d_{ij}$.

Твердження 6.3 можна сформулювати ще таким чином.

Для виявлення помилки у залишку по довільній основі m_i числа $A = (a_1 \| a_2 \| ... \| a_n)$, яке задане у СЗК, необхідно і достатньо, щоб помилка Δa_i була не кратна дільникам d_{ij} і $d_i = (d_{i1}, d_{i2}, ..., d_{in})$, де d_i – НЗД дільників $d_i = (d_{i1}, d_{i2}, ..., d_{in})$.

На підставі результатів твердження 6.3 складемо алгоритм виявлення помилок.

1. Перевіряємо залишок по основі m_i. Для цього визначимо сукупність значень

$$a_1 - a_2 = a_{12} (\mathrm{mod}\, d_{12}),$$
$$a_1 - a_3 = a_{13} (\mathrm{mod}\, d_{13}),$$
$$a_1 - a_n = a_{1n} (\mathrm{mod}\, d_{1n}).$$

Якщо $a_{1i} = (\mathrm{mod}\, d_{1i})$, то перевіряється другий залишок і т. д.

2. Для набуття значень a_{ij} $(i \neq j)$ складаємо матрицю

$$G = \begin{vmatrix} a_{12} & a_{13} \ldots & a_{1n} \\ a_{21} & a_{23} \ldots & a_{23} \\ & \ldots & \\ a_{n1} & a_{n2} \ldots & a_{nn-1} \end{vmatrix}$$

При складанні матриці G не обов'язково вказувати істинне числове значення a_{ij}, досить представити його відмітну ознаку

$$a_{ij} = \begin{cases} 0, \textit{ якщо } a_i - a_j = 0 (\mathrm{mod}\, d_{ij}), \\ 1, \textit{ якщо } a_i - a_j \neq 0 (\mathrm{mod}\, d_{ij}). \end{cases}$$

3. Якщо визначник матриці $|G| = 0$, то число $A = (a_1 \| a_2 \| \ldots \| a_n)$ – правильне, а якщо $|G| \neq 0$, то число A – неправильне.

Розглянемо міркування, що дозволяють спростити наведений вище алгоритм.

Виходячи з того, що

$$a_i - a_j \equiv [d_{ij} - (a_i - a_j)] (\mathrm{mod}\, d_{ij}),$$

визначник $|G|$ можна не знаходити. Досить визначити діагональні елементи матриці G і додати одне значення a_{n1}, тобто

$$a_{12} \| a_{23} \| a_{34} \| \ldots \| a_{n-1n} \| a_{n1}.$$

Легко перевірити, що при таких значеннях a_{ij}, можливо встановити не лише факт спотворення кодового слова, але і визначити номер спотвореного

залишку.

З метою визначення необхідних і достатніх умов для виправлення одноразових помилок за допомогою L-кодов сформульоване і доведене наступне твердження.

Твердження 6.4. Для виправлення помилки у залишку по довільній основі m_i числа $A=(a_1 \| a_2 \| ... \| a_n)$, яке задано у системі залишкових класів з основами $m_1, m_2, ..., m_n$ необхідно, щоб виконувалася умова [44]

$$(d_{ik}-1)(d_{ij}-1) \geq m_i - 1 - (K_{d_{ik}} + K_{d_{ij}} - K_{[d_{ik},d_{ij}]}), \qquad (6.22)$$

де $d_{ik}=(m_i, m_k)$, $d_{ij}=(m_i, m_j)$, $K_{d_{ik}}$ – кількість дільників, кратних d_{ik};

$K_{d_{ij}}$ – кількість дільників, кратних d_{ij};

$K_{[d_{ik},d_{ij}]}$ – кількість дільників, кратних найменшому загальному кратному (НЗК) $[d_{ik}, d_{ij}]$ дільників d_{ik} та d_{ij}, $i \neq j$.

Доказ. Вичислимо значення a_{ij}, a_{ik}, a_{jk}. Якщо помилка сталася по основі m_i, то $a_{ik}=0$, а $a_{ij} \neq 0$ та $a_{ik} \neq 0$. Число різних комбінацій a_{ij}, a_{ik} дорівнює $(d_{ij}-1)\cdot(d_{ik}-1)$, де $(d_{ij}-1)$ – число можливих значень величини a_{ij} $(a_{ij} \neq 0)$, $(d_{ik}-1)$ – число можливих значень a_{ik} $(a_{ik}=0)$, а число можливих значень помилок по основі m_i дорівнює $m_i - 1$ $(\Delta a_i \neq 0)$ за вирахуванням числа невиявлених помилок. Число невиявлених помилок складається з числа помилок, кратних дільникові $d_{ik} - K_{d_{ik}}$ і кратних дільникові $d_{ik} - K_{d_{ik}}$. Таким чином, число можливих значень помилок, що виявляються, дорівнює

$$m_i - 1 - (K_{d_{ik}} + K_{d_{ij}} - K_{[d_{ik},d_{ij}]}).$$

Для забезпечення відповідності можливим значенням помилок по

основі m_i необхідно виконання нерівності (6.22).

Що і вимагалося довести.

Необхідна умова твердження 6.4 є достатнім, якщо різним значенням помилок Δa_i відповідають різні значення добутку $a_{ik} \cdot a_{ij}$ і навпаки. Дійсно, у цьому випадку між можливими значеннями Δa_i і значеннями добутку $a_{ik} \cdot a_{ij}$ існує взаємно однозначна відповідність, що і визначає можливість однозначно визначити величину помилки.

На підставі твердження 6.4 представимо метод та алгоритм корекції помилок по довільній основі m_i:

1. Визначимо номер спотвореного залишку. Для цього вичислимо значення

$$a_1 - a_2 = a_{12} (\mathrm{mod}\, d_{12}),$$
$$a_2 - a_3 = a_{23} (\mathrm{mod}\, d_{23}),$$
$$\dots$$
$$a_{n-1} - a_n = a_{n-1n} (\mathrm{mod}\, d_{n-1n}),$$
$$a_n - a_1 = a_{n2} (\mathrm{mod}\, d_{n1}).$$

Якщо усі залишки $a_{ij} = 0 (\mathrm{mod}\, d_{ij})$, то число A правильне. Якщо помилка сталася по основі m_i, то $a_{ij} \neq 0$ та $a_{ik} \neq 0$ і, таким чином, число, що перевіряється $A = (a_1 \| a_2 \| \dots \| a_i \| \dots \| a_n)$ є неправильним.

2. По значеннях a_{ij} та a_{ik} звертаємося у блок констант помилок, де вибираємо відповідне значення Δa_i.

3. Проводимо корекцію числа A у залишку a_i і отримуємо правильне число $A = A - \Delta A$, тобто

$$A = (a_1 \| a_2 \| \dots \| a_i \| \dots \| a_n).$$

Якщо у скороченій СЗК за рахунок виключення основи, по якій сталася помилка, можна однозначно представити число A, то замість визначення по значеннях a_{ij} і a_{ik} величини помилки Δa_i, безпосередньо обчислимо значення правильного залишку a_i.

Розглянемо цей алгоритм корекції помилок.

1. Обчислимо значення залишків $a_{12}, a_{23}, ..., a_{n1}$.

2. Визначимо номер спотвореного залишку. Нехай помилка сталася по m_i основі. У цьому випадку ця основа виключається, а число A представляється по основах $m_1, m_2, ..., m_n$, тобто

$$A = (a_1 \,||\, a_2 \,||\, ... \,||\, a_{i-1} \,||\, a_{i+1} \,||\, ... \,||\, a_n).$$

3. Зробимо згортку числа A у позиційний код.

4. Визначимо істинне значення спотвореного залишку

$$a_i = A - \left[A / m_i\right] m_i,$$

де $[x]$ – ціла частина x, що не перевершує x. Виправлене число

$$A_{випр.} = (a_1 \,||\, a_2 \,||\, ... \,||\, a_i \,||\, ... \,||\, a_n).$$

Визначимо умови, при яких можливе виключення з СЗК деяких основ. Для цього представимо основи вихідної СЗК у канонічному вигляді

$$m_1 = \beta_{11}^{a_{11}} \beta_{12}^{a_{12}} \ldots \beta_{1l_1}^{a_{1l_1}},$$

$$m_2 = \beta_{21}^{a_{21}} \beta_{22}^{a_{22}} \ldots \beta_{2l_2}^{a_{2l_2}},$$

…

$$m_n = \beta_{n1}^{a_{n1}} \beta_{n2}^{a_{n2}} \dots \beta_{nl_n}^{a_{nl_n}},$$

$$M = \beta_1^{a_1} \beta_2^{a_2} \dots \beta_k^{a_k}.$$

Для однозначного визначення числа A, яке задане у СЗК з основами $m_1, m_2, ..., m_n$ і, що лежить у діапазоні $[0, M)$ можна виключити тільки ті основи, для яких $\beta_m = \beta_{il_i}$, ($m = \overline{1,k}$, $i = \overline{1,n}$). При цьому необхідно, щоб $a_m \geq a_{il_i}$.

Таким чином, визначені необхідні і достатні умови корекції помилок методом виключення спотвореної основи. Цими умовами є одночасне виконання рівності і нерівності

$$\beta_m = \beta_{il_i},\ a_m \geq a_{il_i} \tag{6.23}$$

Нехай задана СЗК основами $m_1 = 4$, $m_2 = 6$, $m_3 = 12$, $m_4 = 18$. При цьому $M = [4, 6, 12, 18] = 36$. Відповідно до умови можливості корекції помилок визначимо ті основи СЗК, які можна виключити.

Представимо основи СЗК у канонічному вигляді: $m_1 = 2^2$, $m_2 = 2 \cdot 3$, $m_3 = 2^2 \cdot 3$, $m_4 = 2 \cdot 3^2$ і $M = 2^2 \cdot 3^2$. Очевидно, що шукані основи – m_1, m_2, m_3. Зробимо перевірку, для чого складемо окремі значення НЗК :

$$M_1 = [6, 12, 18] = 36,$$

$$M_2 = [4, 12, 18] = 36,$$

$$M_3 = [4, 6, 18] = 36,$$

$$M = [4, 6, 12] = 36.$$

Окреме значення НЗК $M_4 < 36$, що підтверджує правильність визначення основ, що виключаються, із заданої СЗК.

Вище був викладений алгоритм виявлення і виправлення помилок у СЗК за допомогою L-кодов. Нехай при обчисленні значень $(a_k - a_{k+1}) \bmod d_{kk+1}$ визначено, що $a_{i-1\,i} \neq 0$, $a_{i\,i+1} \neq 0$, а усі інші значення дорівнюють

$$a_{k\,k+1} = (a_k - a_{k+1}) \bmod d_{k\,k+1} = 0 .$$

Тоді стверджується, що число A неправильне, а помилка є присутньою у залишку по основі m_i тобто

$$A = (a_1 \| a_2 \| \ldots \| a_i \| \ldots \| a_n) .$$

Звертаючись по значеннях $a_{i-1\,i}$ та $a_{i\,i+1}$ у блок констант помилок визначимо значення помилки Δa_i і далі визначимо істинне значення залишку

$$a_{i\,випр.} = a_i - \Delta a_i .$$

Виправлене число представиться у вигляді

$$A_{випр.} = (a_1 \| a_2 \| \ldots \| a_{i\,випр.} \| \ldots \| a_n) .$$

Щоб виправити помилку за допомогою розробленого методу корекції, необхідно, щоб помилка Δa_i була одночасно не кратна двом дільникам $d_{i-1\,i}$ і $d_{i\,i+1}$, що обмежує клас коригувальних помилок.

Таким чином, виникає необхідність у розробці ефективних методів і алгоритмів, що дозволяють розширити клас можливих коригувальних помилок.

Метод корекції одноразових помилок, що дозволяє виправляти

помилки, кратні одному з дільників $d_{i-1\ i}$ або $d_{i\ i+1}$ полягає у наступному.

Нехай задана СЗК із взаємно не простими основами, тобто НЗД

$$(m_1, m_2, ..., m_n) \geq 2.$$

І нехай задано число у СЗК

$$A_{випр.} = (a_1 \| a_2 \| ... \| a_n).$$

Визначимо усі значення $a_{k\,k+1}$, тобто $a_{12}, a_{23}, a_{34}, ..., a_{n-1\ n}, a_{n\ 1}$. Не порушуючи спільності міркувань, вважатимемо, що $a_{i\ i+1} \neq 0$, а усі інші значення $a_{k\ k+1} \neq 0$. Оскільки

$$a_{i\ i+1} = (a_i - a_{i+1}) \bmod d_{i\ i+1} \neq 0,$$

то помилка може бути присутньою тільки у залишках по основах m_i або m_{i+1}. У зв'язку з цим можливі дві гіпотези:

- помилка є присутньою у залишку a_i;

- помилка є присутньою у залишку a_{i+1}.

Перш ніж розглянути процес корекції помилок методом, що пропонується, сформулюємо і доведемо теорему, результат доказу якої використаємо при визначенні процесу збіжності сукупності чисел виду

$$A^{(k_i)} = (a_1 \| ... \| a_{i-1} \| a_{ik_i} \| a_{i+1} \| ... \| a_n)$$

до правильного числа

$$A^{(\rho)} = (a_1 \,||\, ... \,||\, a_{i-1} \,||\, a_{i\rho} \,||\, a_{i+1} \,||\, ... \,||\, a_n).$$

Заздалегідь розглянемо лему.

Лема 6.2. Сума, різниця і добуток будь-яких кодових слів L-коду є кодовими словами.

Твердження 6.5. Нехай у впорядкованій $(m_{i-1} < m_i; i = \overline{1, n})$ системі залишкових класів з основами $m_1, m_2, ..., m_n$ задано неправильне (спотворене в одному залишку) число

$$A = (a_1 \,||\, a_2 \,||\, ... \,||\, a_{i-1} \,||\, a_i \,||\, a_{i+1} \,||\, ... \,||\, a_n)$$

і нехай

$$\Delta a_i = a_i - a_i = k_i d_{i-1\,i}.$$

Тоді у сукупності значень

$$a_{ik_i} = (a_i - k_i d_{i-1\,i}) \bmod m_i$$

існує таке єдине значення $a_{i\rho}$, при якому число

$$A^{(\rho)} = (a_1 \,||\, a_2 \,||\, a_{i\rho} \,||\, ... \,||\, a_n)$$

є правильним числом, де $d_{i-1\,i}(m_{i-1}, m_i)$, а k_i може набувати значень $k_i = 1, 2, ..., m_i / d_{i-1\,i} - 1$.

Доказ. Покажемо, що існує таке значення $a_{i\rho_1}$, при якому число

$$A = (a_1 \,||\, a_2 \,||\, ... \,||\, a_{i\rho} \,||\, ... \,||\, a_n)$$

є правильним. За умовою теореми помилка Δa_i кратна дільникові $d_{i-1\,i}$. Вираз $k_i d_{i-1\,i}$ містить усі можливі числа, що кратні $d_{i-1\,i}$.

Таким чином, знайдеться хоч би одне значення $k_i = \rho_1$ при якому

$$\Delta a_{i\rho_1} = \rho_1 d_{i-1\,i}, \text{ а}$$

$$a_{1\rho_1} = a_i - \Delta a_{i\rho_1}.$$

Покажемо, що $A^{(\rho_1)}$ єдине правильне число з сукупності чисел виду $A^{(k_i)}$.

Припустимо, що існує таке значення

$$a_{1\rho_2} = a_i - \rho_2 d_{i-1\,i},$$

при якому число $A^{(\rho_2)}$ також є правильним. Тоді відповідно до леми 6.2 число

$$A^{(\rho_1)} - A^{(\rho_2)} = (0 \,||\, ... \,||\, a_{i\,\rho_1} - a_{i\,\rho_2} \,||\, ... \,||\, 0)$$

є правильним. Якщо число $A^{(\rho_1)} - A^{(\rho_2)}$ правильне, то відповідно до леми 6.1 маємо

$$(\rho_2 - \rho_1) d_{i-1\,i} \equiv 0 (\mathrm{mod}\, d_{1-i}),$$
$$(\rho_2 - \rho_1) d_{i-1\,i} \equiv 0 (\mathrm{mod}\, d_{2-i}),$$
$$\dots$$

$$(\rho_2 - \rho_1) d_{i-1\,i} \equiv 0 (\mathrm{mod}\, d_{n-i}).$$

Якщо $i \neq n$, то єдиним правильним числом $A^{(\rho_1)} - A^{(\rho_2)}$ буде нульове кодове слово. Це обумовлено тим, що $d_{i-1\,i} \neq 0$ і $d_{i-1\,i}$ не дорівнює НЗК дільників $d_{1i}, d_{2i}, ..., d_{ni}$.

Причому нерівність $d_{i-1\,i} \neq [d_{1i}, d_{2i}, ..., d_{ni}]$ суперечить умові довільного вибору основ $m_1, m_2, ..., m_n$. Отже, виконується наступна рівність

$$A^{(\rho_1)} - A^{(\rho_2)} = (0 \,\|\, 0 \,\|\, ... \,\|\, 0 \,\|\, ... \,\|\, 0).$$

Таким чином, $\rho_1 = \rho_2$, що підтверджує єдиність існування ρ_1 при якому

$$A^{(\rho_1)} = (a_1 \,\|\, a_2 \,\|\, ... \,\|\, a_{i\rho_1} \,\|\, ... \,\|\, a_n)$$

є правильним. Що і вимагалося довести.

Розробимо алгоритм корекції помилок, яки заснований на результаті доведеного твердження 6.5.

Розглянемо першу гіпотезу. Оскільки $a_{i-1\,i} = 0$, то помилка кратна дільникові $d_{i-1\,i}$. Тому помилка по основі може набувати значень

$$\Delta a_i = k d_{i-1\,i},$$

для $k_i = 1, 2, ..., m_i / d_{i-1\,i} - 1$.

Вичислимо сукупність значень

$$a_{ik_1} = (a_i - k_i d_{i-1\,i}) \,\mathrm{mod}\, m_i.$$

Якщо у цій сукупності знайдеться таке значення a_{im} при якому

$$A^{(m)} = (a_1 \| a_2 \| ... \| a_{im} \| ... \| a_n)$$

правильне число, то перша гіпотеза справедлива, тобто помилка є присутньою у залишку по основі m_i. У цьому випадку виправленим числом є

$$A_{випр.} = A^{(m)},$$

де

$$a_{im} = (a_i - md_{i-1\,i}) \bmod m_i.$$

Якщо при усіх значення a_{ik_i} число $A^{(k_i)}$ неправильне, то значення a_i істинно, а помилка сталася у залишку по основі m_{i+1}. Оскільки $a_{i+1\ i+2} = 0$, то помилка по основі m_{i+1} кратна дільникові $d_{i+1\ i+2}$ тобто

$$\Delta a_{i+1} = k_{i+1} d_{i+1\ i+2},$$

де $k_{i+1} = 1, 2, ..., m_{i+1} / d_{i+1 i+2} - 1$.

Визначимо сукупність значень

$$a_{i+1\,k_{i+1}} = (a_{i+1} - k_{i+1} d_{i+1\ i+2}) \bmod m_{i+1}.$$

За твердженням 6.5 у цій сукупності обов'язково знайдеться така однина $a_{i+1\,N}$, при якій $A^{(N)} = (a_1 \| a_2 \| ... \| a_{i+1\,N} \| ... \| a_n)$ правильне число.

Відмітимо, що черговість перевірки гіпотез довільна і не впливає на імовірність корекції помилок. Проте з метою підвищення швидкодії визначення номера спотвореного залишку у першу чергу необхідно перевірити гіпотезу, для якої значення $m_k / d_{k-1\,k}$ $(k = i, i+1)$ буде найменшим.

Розглянемо приклад реалізації розробленого алгоритму корекції помилок за допомогою L-кодов.

Нехай задана СЗК основами $m_1 = 4$, $m_2 = 6$, $m_3 = 12$, $m_4 = 18$. При цьому $M = 36$, $d_{12} = 2$, $d_{23} = 6$, $d_{34} = 6$, $d_{41} = 2$. Об'єм кодових слів представлений у табл. 6.2.

Необхідно визначити правильність числа $A = (3 \| 5 \| 7 \| 7)$ і у разі спотворення, виправити його.

1. Визначимо значення $a_{12} = 0$, $a_{23} = 2$, $a_{34} = 0$, $a_{41} = 0$. Оскільки $a_{23} \neq 0$, те число A неправильне, і помилка сталася у другому або у третьому залишках.

2. Оскільки $m_2 / d_{12} > m_3 / d_{34}$, то перша гіпотеза полягає у тому, що помилка передбачається у залишку по основі m_3.

3. Обчислимо значення $a_{3k_3} = a_3 - k_3 d_{23}$ для $k_3 = 1$.

Отримаємо $a_{3k_3} = a_3 - k_3 d_{23} = 7 - 1 \cdot 6 = 1$. При цьому отримане число $A^{(1)} = (3 \| 5 \| 1 \| 7)$ не є кодовим словом, тобто перша гіпотеза не вірна. Помилка сталася у залишку по основі m_2.

4. Виправимо число A. Для цього по значеннях $k_3 = 1, 2$ визначимо шукане значення $a_{2k_2} = a_2 - k_2 d_{21}$

$$k_2 = 1,\ a_{2k_2} = a_2 - k_2 d_{21} = 5 - 1 \cdot 2 = 3,$$

$$k_2 = 3,\ a_{2k_2} = a_2 - k_2 d_{21} = 5 - 2 \cdot 2 = 2.$$

Таблиця 6.2

Таблиця кодових слів

Число A у десятковому коді	Число A у СЗК			
	m_1	m_2	m_3	m_4
0	0	0	0	0
1	1	1	1	1
2	2	2	2	2
3	3	3	3	3
4	0	4	4	4
5	1	5	5	5
6	2	0	6	6
7	3	1	7	7
8	0	2	8	8
9	1	3	9	9
10	2	4	10	10
11	3	5	11	11
12	0	0	0	12
13	1	1	1	13
14	2	2	2	14
15	3	3	3	15
16	0	4	4	16
17	1	5	5	17
18	2	0	6	0
19	3	1	7	1
20	0	2	8	2
21	1	3	9	3
22	2	4	10	4
23	3	5	11	5
24	0	0	0	6
25	1	1	1	7
26	2	2	2	8
27	3	3	3	9
28	0	4	4	10

Таким чином, отримаємо два кодові слова: $A^{(1)} = (3 \| 3 \| 7 \| 7)$ і $A^{(2)} = (3 \| 1 \| 7 \| 7)$.

З табл. 6.2 видно, що єдино правильним кодовим словом є значення $A^{(2)}$, тобто $A_{випр.} = A^{(2)} = (3 \| 1 \| 7 \| 7)$.

Таким чином, розроблений метод корекції помилок у СЗК дозволяє розширити клас коригувальних помилок. Це істотно розширює коригувальні можливості L-кодів у СЗК.

Алгоритми корекції помилок у СЗК зі взаємно попарно непростими основами дозволяють відносно просто реалізувати процедуру виявлення та виправлення однократних помилок. Основні переваги L- кодів у СЗК полягають у простоті процедури виявлення місця помилки та її локалізації. За простоті декодуючих схем - коди не мають аналогів, як у ПСЧ, так і у СЗК.

Висновки до розділу 6

1. У розділі приведені теоретичні основи корекції (виправлення) помилок даних у СЗК. Використовуючи основні теоретичні положення корекції непозиційних кодових структур, у розділі представлені методи виправлення помилок у СЗК. Ці методи засновані на використанні взаємно простих основ, а також сукупності частинних робочих основ СЗК та частинних ортогональних базисів. Використання запропонованих методів виправлення помилок у НКС, дозволяє за рахунок паралельного виправлення помилок структури, що діагностується, у ρ раз підвищити оперативність корекції помилок у СЗК. Де ρ – кількість можливих залишків НКС, у яких відбулися помилки. Очевидно, що зі збільшенням розрядної сітки оброблюваних чисел ефективність використання розглянутих методів виправлення помилок зростає.

2. Розглянуто варіант використання розробленого методу оперативної

корекції для вирішення задачі виправлення помилок у реальному часі. Цей метод заснований на використанні альтернативної сукупності непозиційних кодових структур, шляхом паралельної незалежної обробки залишків чисел, які представлені у СЗК. На основі розробленого методу синтезовано алгоритм контролю і корекції помилок на основі, якого отримані пристрої для його реалізації. На ці пристрої отримані патенти України (Пат. 47563 Україна, МПК (2009) G 06 F 11/08; Пат. 105436 Україна, МПК G06F 11/08 (2006.01).).

3. Показано, що використання кодів з взаємно непростими основами (L-кодів), дозволяє розширити клас помилок, що коректуються. Це істотно розширює коригувальні можливості L-кодів у СЗК. Такі алгоритми корекції помилок у СЗК дозволяють відносно просто реалізувати процедуру виявлення та виправлення однократних помилок. Основні переваги L – кодів у СЗК полягають у простоті процедури виявлення місця помилки та її локалізації. За простотою схем декодують, L – коди не мають аналогів, як у ПСЧ, так і у СЗК.

Основні положення цього розділу викладені у публікаціях автора [176, 177, 179-181].

ВИСНОВКИ

У дисертації сформульована і вирішена важлива та актуальна науково-технічна проблема по розробці методів оперативного контролю та діагностики даних компонентів комп'ютерної системи, що функціонують у залишкових класах.

У процесі рішення часткових задач проблеми дисертації отримані наступні результати.

1. У процесі дослідження методів підвищення оперативності контролю, діагностики та корекції цілочислових даних, представлених у СЗК, у роботі систематизовані можливі галузі науки і техніки, де є необхідність у швидких, достовірних та високоточних цілочислових обчисленнях. Показано, що існуючі методи контролю, діагности та корекції цілочислових даних у СЗК не завжди відповідають вимогам, що пред'являються до їх оперативності. Ця обставина істотно обмежує сферу ефективного застосування СЗК в якості системи числення КСКОЦД. Це, у свою чергу, визначає основну концепцію розвитку КСКОЦД у СЗК і вимагає рішення наступних часткових задач: дослідити методи підвищення оперативності контролю та діагности цілочислових даних, що представлені у системі залишкових класів, без зниження продуктивності обробки інформації; дослідити вплив властивостей системи залишкових класів на структуру і процес функціонування компонентів комп'ютерної системи обробки цілочислових даних; дослідити коригувальні властивості непозиційних кодових структур у системі залишкових класів; розробити метод контролю даних у системі залишкових класів, який заснований на принципі паралельної нульовизації; розробити метод контролю даних у системі залишкових класів, який заснований на використанні позиційної ознаки непозиційної кодової структури; розробити метод підвищення достовірності оперативного контролю даних, що представлені у системі залишкових класів; удосконалити метод визначення альтернативної сукупності непозиційних кодових структур у системі

залишкових класів; удосконалити метод оперативної діагностики даних представлених в системі залишкових класів.

Використання розроблених методів і засобів оперативного контролю, діагности та корекції помилок даних дозволять усунути конфліктну ситуацію між існуючою можливістю значного підвищення швидкодії виконання цілочислових арифметичних операцій у СЗК і низькою оперативністю існуючих систем і засобів контролю та діагности результатів обчислень у СЗК.

Підвищення оперативності контролю та діагностики даних компонент комп'ютерної системи, що функціонують у системі залишкових класів досягається за рахунок результатів рішення сформульованої науково-технічної проблеми. Це здійснюється шляхом усунення протиріччя між високою швидкодією реалізації цілочислових арифметичних операцій і низькою (недостатньою) оперативністю контролю та діагностики даних.

2. З метою визначення можливості створення ефективних методів, систем та засобів оперативного контролю та діагностики даних у СЗК у роботі сформульовані принципи побудови НКС. На підставі сформульованих принципів побудови НКС проведені дослідження впливу властивостей СЗК на структуру і процес функціонування компонентів комп'ютерної системи обробки цілочислових даних. Результати дослідження лягли в основу формулювання принципів технічної реалізації цілочислових арифметичних операцій у СЗК.

У роботі сформульовані три принципи технічної реалізації арифметичних цілочислових операцій: суматорний (на основі використання малорозрядних двійкових суматорів по модулю СЗК); принцип кільцевого зсуву (на основі використання кільцевих регістрів зсуву) і табличний (матричний) принцип, який заснований на використанні постійних запам'ятовуючих пристроїв. Методи обробки даних, що засновані на цих принципах, впливають на оперативність систем і засобів контролю у СЗК.

На основі результатів досліджень показана можливість створення

ефективних методів, систем і засобів контролю та діагностики даних у СЗК.

3. З метою розробки та вдосконалення методів підвищення оперативності контролю та діагностики помилок цілочислових даних, які представлені у СЗК, у роботі досліджені загальні коригувальні властивості непозиційних кодових структур. Сформульовані основні положення та виводи теорії завадостійкого кодування даних у СЗК. Це дало можливість створити процедуру варіювання коригувальними здібностями завадостійкого коду СЗК у динаміці обчислювального процесу.

4. У роботі досліджені методи контролю даних у СЗК, які засновані на принципі нульовизації. На основі результатів аналізу існуючих методів контролю даних у СЗК, розроблено метод контролю даних, який заснований на принципі паралельної нульовизації з попереднім аналізом подальших симетричних залишків числа, що контролюється. Цей метод, у порівнянні з існуючими методами, які засновані на принципі нульовизації, дозволяє, залежно від довжини машинного слова КСКОЦД, на 25-60 % підвищити оперативність контролю даних.

5. На основі використання сформованої позиційної ознаки НКС, розроблено метод контролю даних у СЗК. Цей метод дозволяє проводити контроль даних, які представлені у СЗК тільки в інформаційному числовому інтервалі, а також у першому інтервалі, що знаходиться після значення M інтервалі, який розташований на відрізку 0-М. Це у свою чергу зменшує кількість констант, що визначаються у записі $K_{N_i}^{(n_A)} = \left\{ Z_{N_i-1}^{(A)} \; Z_{N_i-2}^{(A)} \; \ldots \; Z_1^{(A)} \; Z_0^{(A)} \right\}$ ОК. Цей метод, у порівнянні з існуючими методами дозволяє до 60 % підвищити оперативність контролю даних представлених у СЗК.

6. Розроблено метод підвищення достовірності контролю даних, що представлені у СЗК, який заснований на використанні позиційної ознаки НКС. Показано, що для підвищення достовірності контролю даних, необхідно, вибирати максимальну за величиною інформаційну основу m_n. Використання цього методу забезпечує отримання достовірного результату

контролю з точністю до одиниці довжини числового інтервалу.

7. У роботі вдосконалено метод визначення альтернативної сукупності непозиційних кодових структур, який заснований на реалізації функцій відповідності значень можливих помилок, шляхом формування таблиць відповідності правильного числа можливій сукупності неправильних чисел, що дозволяє підвищити оперативність діагностики помилок НКС у СЗК. Розроблений метод зменшує кількість основ СЗК, що перевіряються, які входять в альтернативну сукупність чисел. Використання цього методу дозволяє підвищити оперативність діагностики та корекції помилок до 30 %.

8. У роботі вдосконалено метод оперативної діагностики непозиційних кодових структур, який заснований на процедурі інтервальних числових перерізів. Метод будується на процедурі згортки таблиці відповідності значень можливих помилок і дозволяє підвищити оперативність стягування альтернативної сукупності залежно від величини розрядної сітки КСКОЦД від 6 до 19%. Запропонований метод дозволяє зменшити час діагностики помилок даних, представлених у СЗК, що підвищує оперативність діагностики. Використання запропонованого методу оперативної діагностики даних підвищує загальну ефективність і доцільність використання в обчислювальних системах непозиційних кодових структур у СЗК.

9. У роботі приведені теоретичні основи корекції (виправлення) помилок даних у СЗК. Використовуючи основні теоретичні положення корекції непозиційних кодових структур, представлені методи виправлення помилок у СЗК. Ці методи засновані на використанні як взаємно простих (R–коди) так і взаємно непростих (L–коди) основ. Використання методів виправлення помилок у НКС представлених R–кодами, дозволяє за рахунок паралельного виправлення помилок структури, що діагностується, у ρ раз підвищити оперативність корекції помилок у СЗК. Де ρ – кількість можливих залишків НКС, у яких відбулися помилки. У свою чергу використання L-кодів, дозволяє розширити клас помилок, що коректуються.

Це істотно розширює коригувальні можливості L-кодів у СЗК. Такі алгоритми корекції помилок у СЗК дозволяють відносно просто реалізувати процедуру виявлення та виправлення однократних помилок. Основні переваги L – кодів у СЗК полягають у простоті процедури виявлення місця помилки та її локалізації. За простотою схем декодують, L – коди не мають аналогів, як у ПСЧ, так і у СЗК.

10. На основі розроблених і вдосконалених методів, синтезовані алгоритми контролю, діагности та корекції помилок на основі, якої отримані 35 патентів України.

Наукова новизна результатів дисертації

1. **Вперше** представлено метод контролю даних у системі залишкових класів, який на відміну від відомих, заснований на принципі паралельної нульовизації, шляхом поєднання у часі операцій нульовизації симетричних залишків непозиційної кодової структури, що контролюється та визначення констант нульовизації, що дозволяє підвищити оперативність контролю даних.

2. **Вперше** представлено метод контролю даних у системі залишкових класів, який на відміну від відомих, заснований на використанні позиційної ознаки непозиційної кодової структури, шляхом паралельного віднімання встановлених констант, що дозволяє підвищити оперативність контролю даних.

3. **Вперше** представлено метод підвищення достовірності оперативного контролю даних, які представлені у системі залишкових класів, який на відміну від відомих, заснований на використанні позиційної ознаки непозиційної кодової структури, шляхом застосування відповідної основи, яка кратна загальному модулю системи залишкових класів, що підвищує достовірність контролю даних.

4. **Вдосконалено** метод визначення альтернативної сукупності НКС у системі залишкових класів, який заснований на використанні функції

відповідності значень можливих помилок, шляхом зменшення числа основ, що перевіряються, які входять в альтернативну сукупність чисел, що підвищує оперативність діагностики помилок даних.

5. **Удосконалено** метод оперативної діагностики даних, що представлені у системі залишкових класів, який заснований на формуванні числових інтервалів та ознак даних квадрантів знаходження альтернативних сукупностей чисел, шляхом згортки таблиці відповідності значень можливих помилок, це зменшує час вибірки основ, що перевіряються та підвищує оперативність діагностики помилок даних.

Практичне значення результатів дисертації

1. Результати рішення сформульованої у дисертації важливої та актуальної науково-технічної проблеми можуть бути покладені в основу науково-методологічного апарату для практичного створення високопродуктивних КСКОЦД, які функціонують у СЗК.

2. Розроблені та удосконалені у дисертаційній роботі методи контролю та діагности помилок даних доцільно використовувати при створенні системи контролю та корекції помилок для перспективних КСКОЦД у СЗК.

3. Застосування запропонованих у дисертації методів оперативного контролю даних у СЗК, які засновані на використанні принципу нульовизації і позиційній ознаці непозиційної кодової структури, дозволяє на 25-60% (у порівнянні з існуючими методами контролю) скоротити час контролю, що підвищує оперативність процедури контролю.

4. Запропоновані методи оперативної діагностики даних у СЗК дозволяють до 30% (у порівнянні з існуючими методами діагностики) скоротити час контролю, що підвищує оперативність процедури діагностики.

5. Розглянуті методи оперативного виправлення помилок даних у СЗК сприяли розробці засобів, які на відміну від існуючих дозволяють у ρ раз підвищити оперативність корекції помилок у СЗК. Де ρ – кількість можливих залишків НКС, в яких сталися помилки.

6. На підставі запропонованих методів обробки даних у дисертації розроблені алгоритми для їх реалізації у відповідності, з якими синтезовані засоби обробки даних у СЗК у вигляді пристроїв, на які отримано 35 патентів України. Це підтверджує актуальність, новизну та практичну значущість отриманих у дисертації результатів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Материалы Международной научно-технической конференции "50 лет модулярной арифметике" // МИЭТ, г. Зеленоград, Моск. обл. 23-25 ноября 2005. С. 101-130.

2. Patterson D. A., Hennessy J. L. Computer organization and design, fifth edition: the hardware/software interface (The Morgan Kaufmann series in computer architecture and design) 5th edition. Morgan Kaufmann, 2013. 800 p.

3. Юдицкий Д. И. Созидатели отечественной электроники / ред. Б. М. Малашевич [и др.]. Москва: Техносфера, 2011. Вып. 2. 320 с.

4. Солонина А. И., Улахович Д. А., Яковлев Л. А. Алгоритмы и процессоры цифровой обработки сигналов. СПб.: БХВ-Петербург, 2001. 464 с.

5. Бройдо В. Л., Ильина О. П. Вычислительные системы, сети и телекоммуникации: учебник для вузов. 4-е изд. СПб.: Питер, 2011. 560 с.

6. Shiva S. G. Computer Organization, Design, and Architecture: fourth edition. Taylor & Francis, 2000. 736 p.

7. Малашевич Б. М. 50 лет отечественной микроэлектроники. Москва: Техносфера, 2013. Вып. 5. 800 с.

8. 50 лет модулярной арифметике // Электроника и информатика: сб. науч. тр. Юбилейная международная научно-техн. конф. Москва: ОАО "Ангстрем", МИЭТ, 2006. 775 с.

9. Hsu J. Y. Computer Architecture: Software Aspects, Coding, and Hardware. CRC Press, 2017. 456 p.

10. Сиора А. А., Краснобаев В. А., Харченко В. С. Отказоустойчивые системы с версионно-информационной избыточностью в АСУ ТП: монография. Харьков: МОН, НАУ им. Н. Е. Жуковского (ХАИ), 2009. 320с.

11. Барсов В. И., Краснобаев В. А., Сиора А. А., Авдеев И. В. Методы многоверсионной обработки информации в модулярной арифметике: монографія. Харьков: МОН, УИПА, 2008. 460с.

12. Модулярные параллельные вычислительные структуры нейропроцессорных систем / под. ред. Н. И. Червякова. М.: Физматлит, 2003. 288 с.

13. Iou I. Y., Abraham J. A. Fault-tolerant matrix arithmetic and signal processing on lightly concurrent computing structures // Proc. IEEE, May. 1996. P. 732-741.

14. Hongbin LI, Qing Zhao, Zhenyu Yang. Reliability modeling of fault tolerant control systems // Int. J. Appl. Math. Comput. Sci. 2007. Vol. 17, No. 4. P. 491–504.

15. Parhami B. Computer arithmetic: algorithms and hardware designs. Oxford University Press, 2000. 490 p.

16. Дианов Н. Н. Диагностика и надежность автоматических систем: учебное пособие. 2-е изд. Москва: МГИУ, 2005. 160 с.

17. Vears R. E. Microprocessor based systems for the higher technician. Newnes, 2016. 298 p.

18. Patterson D. A., Hennessy J. L. Computer Organization and Design: The Hardware Software Interface: ARM Edition (The Morgan Kaufmann Series in Computer Architecture and Design) 1st Edition: Morgan Kaufmann, 2016. 720 p.

19. Краснобаев В. А., Янко А. С., Гроза П. Н., Кошман С. А., Гроза А. П., Бендес Ю. П. Расчет и сравнительный анализ производительности компьютерной системы обработки целочисленных данных, функционирующей в системе остаточных классов // Системи обробки інформації: збірник наукових праць. Харків. 2015. № 1(126). С. 111-117.

20. Краснобаев В. А., Янко А. С., Кошман С. А., Сомов С. А., Бендес Ю. П. Исследование производительности компьютерной системы обработки целочисленных данных, функционирующей в системе остаточных классов // Збірник наукових праць Харківського університету Повітряних Сил. Харків. 2015. Вип. 1(42). С. 48-52.

21. Краснобаев В. А., Янко А. С., Кошман С. А., Курчанов В. Н., Бендес Ю. П. Расчет и сравнительный анализ производительности

компьютерной системы обработки целочисленных данных, представленных в системе остаточных классов // Системи обробки інформації: збірник наукових праць. Харків. 2015. Вип. 3(128). С. 57-61.

22. Николайчук Я. Н., Касянчук М. Н., Якименко И. З. Теоретические основы модифицированной совершенной формы системы остаточных классов. // Кібернетика і системний аналіз. 2016. Том 52, № 2. С. 51–55.

23. Краснобаев В. А., Кошман С. А., Сомов С. В., Крючко Е. А. Метод быстрой обработки криптографической информации в модулярной системе счисления // Системи обробки інформації: збірник наукових праць. Харків. 2013. № 6(113). С. 194-198.

24. Koshman S., Krasnobayev V., Kuznetsov A., Rassomakhin S., Zamula A., Kavun S. Effective Data Processing in Coding, Digital Signals and Cryptography: monograph. ASC Academic Publishing, 2018, 352 p.

25. Краснобаєв В. А., Кошман С. О. Застосування системи залишкових класів у машинній арифметиці // Вісник Харківського державного технічного університету сільського господарства. Проблеми енергозабезпечення та енергозбереження в АПК України. 2003. Вип. 19. С. 134-136.

26. Фурман І. О., Краснобаєв В. А., Кошман С. О. Аналіз табличних алгоритмів реалізації модульних операцій у автоматизованих системах обробки цифрової інформації // Вісник Харківського державного технічного університету сільського господарства. Проблеми енергозабезпечення та енергозбереження в АПК України. 2004. Вип. 27. С. 174-178.

27. Кошман С. А., Деренько Н. С. Метод реализации арифметических операций в модулярной арифметике на основе использования малоразрядных двоичных сумматоров // Радіоелектронні і комп'ютерні системи. 2007. № 7 (26). С. 219-221.

28. Кошман С. О. Концепція підвищення продуктивності обробки інформації у реальному часі // Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка. Проблеми

енергозабезпечення та енергозбереження в АПК України. 2011. Вип. 117. С. 63-65.

29. Кошман С. А., Краснобаев В. А., Маврина М. А. Методы оптимального резервирования в модулярной системе счисления // Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка. Проблеми енергозабезпечення та енергозбереження в АПК України. 2012. Вип. 129. С. 105-108.

30. Краснобаев В. А., Кошман С. А., Тыртышников А. И., Гаркавенко Н. С. Концепция создания отказоустойчивых компьютерных систем обработки информации в системе остаточных классов на основе применения ПЛИС // Системи обробки інформації: збірник наукових праць. Харків. 2013. № 7(114). С. 79-82.

31. Кошман С. А., Загумённая Е. В. Анализ особенностей функционирования автоматизированной системы управления турбоустановками // Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка. Проблеми енергозабезпечення та енергозбереження в АПК України. 2011. Вип. 116. С. 117-120.

32. Кошман С. О., Мартиненко С. О., Краснобаєв В. А., Замула О. А., Деренько М. С. Метод технічної реалізації арифметичних операцій модулярній системі числення на основі використання принципу кільцевого зсуву // Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка. Проблеми енергозабезпечення та енергозбереження в АПК України. 2009. Вип. 87. С. 71-73.

33. Koshman S. A., Barsov V. I., Krasnobayev V. A., Yaskova K. V., Derenko N. S. Method of bit-by-bit tabular realization of arithmetic operations in the system of residual classes // Радіоелектронні і комп'ютерні системи. 2009. № 5 (39). С. 44-48.

34. Krasnobayev V. A., Koshman S. A. Method of realization of

cryptographic RSA transformations on the basis of application of modular number system // Biomedical Soft Computing and Human Sciences. 2011. Vol. 17, № 2. P. 31-36.

35. Кошман С. О. Дослідження методів оптимізації структур систем обробки формації // Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка. Проблеми енергозабезпечення та енергозбереження в АПК України. 2007. Вип. 57. С. 111-116.

36. Кошман С. О. Алгоритм оптимізації обладнання систем обробки інформації АСКОЕ, що функціонують у модулярній арифметиці // Вісник Харківського державного технічного університету сільського господарства. Проблеми енергозабезпечення та енергозбереження в АПК України. 2005. Вип. 37. С. 240-244.

37. Кошман С. А., Фурман И. А., Краснобаев В. А. Вариант синтеза процессора в системе остаточных классов // Радиотехника и Информатика. 2003. №2. С. 94-96.

38. Краснобаев В. А., Маврина М. А., Кошман С. А., Курчанов В. Н. Концепция создания компьютерных средств обработки данных на основе использования кодов класса вычетов // Системи обробки інформації: збірник наукових праць. Харків. 2013. № 4(111). С. 133-138.

39. Кошман С. А. Концепция создания системы обработки цифровой информации на основе использования системы остаточных классов // Радіоелектронні і комп'ютерні системи. 2010. № 7 (48). С. 138-141.

40. Фет Я. Н. Параллельные процессоры для цифровых систем. Москва: Энергоатомиздат, 1981. 160 с.

41. Фурман И. А., Краснобаев В. А., Малиновский М. Л., Кошман С. А., Бовчалюк С. Я. Концепция, методы и средства моделирования на ПЛИС контроллеров и процессоров с параллельной архитектурой // Сборник научных трудов Харьковского национального автодорожного университета. Автомобильный транспорт в 21 веке. 2005. Вып. 16. С. 338-341.

42. Финько О. А. Сверхпараллельные логические вычисления методами модулярной арифметики // Искусственные интеллектуальные системы (IEEE AIS'02) и Интеллектуальные САПР (CAD-2002): междунар. конф. Москва: Наука, Физматлит, 2002. С. 448 455.

43. Yadin A. Computer Systems Architecture. CRC Press, 2016. 526 p.

44. Торгашев, В. А. Система остаточных классов и надежность ЦВМ. Москва: Сов. радио, 1973. 118 с.

45. Журавлев Ю. П., Кателюк Л. А., Циклинский Н. И. Надежность и контроль ЭВМ. Москва: Сов. Радио. 1978. 416 с.

46. Краснобаев В. А. Методы повышения надежности специализированных ЭВМ систем и средств связи / под. ред. В. А. Краснобаева. Харьков: ХВВКИУ РВ, 1990. 172с.

47. Акушский И. Я., Юдицкий Д. И. Машинная арифметики в остаточных классах. Москва: Радио и связь, 1968. 444 с.

48. Амербаев, В. М. Теоретические основы машинной арифметики. Алма-Ата: Наука, 1976. 324 с.

49. Долгов А. И. Диагностика устройств, функционирующих в системе остаточных классов. Москва: Радио и связь, 1982. 64 с.

50. Барсов В. И., Сорока Л. С., Краснобаев В. А. Методология параллельной обработки информации в модулярной системе счисления. Харьков: УИПА, 2009. 268 с.

51. Барсов В. И., Сорока Л. С., Краснобаев В. А., Хери А. А. Модели и методы повышения отказоустойчивости и производительности управляющих вычислительных комплексов специализированных систем управления реального времени на основе применения непозиционных кодовых структур модулярной арифметики. Харьков: УИПА, 2008. 147 с.

52. Финько О. А. Параллельные логические вычисления, использующие избыточные представления чисел // Идентификация систем и задачи управления. Вторая Международная конференция. Москва: Институт проблем управления им. В.А. Трапезникова, РАН, 2003. С. 1716-1728.

53. Фурман И. А., Краснобаев В. А., Малиновский М. Л., Панченко С. В. Контроллеры и процессоры с параллельной архитектурой: учебник для ВУЗов / ред. Г. И. Загарий. Харьков: УкрГАЖТ, 2006. 416 с.

54. Лосев Ю. И., Шматков С. И., Руккас К. М. Методы и модели обмена информацией в распределенных адаптивных вычислительных сетях с временной параметризацией параллельных процессов. Харьков: ХНУ им. В. Н. Каразина, 2011. 204 с.

55. Инютин С. А. Параллельные вычисления в сверхбольших компьютерных диапазонах // Параллельные вычисления и задачи управления: тезисы докл. I Международная конференция, 29-31 января 2001 г. Москва. 2001. С. 76-87.

56. Кошман С. А. Концепция реализации немодульных операций в модулярной системе счисления // Проблеми інформації: тези доп. Другої міжнародної науково-технічної конференції, Київ: ДУТ; Полтава: ПНТУ; Катовище: Катовицький економічний університет; Париж: Університет Париж VII Вєнсент-Сен-Дєні; Білгород: "БДУ"; Черкаси: ЧДТУ; Харків: ХНДІТМ, 12–13 квітня 2014 року. Харків, 2014. С. 94-95.

57. Amir Sabbagh Molahosseini, Leonel Seabra de Sousa, Chip-Hong Chang. Embedded Systems Design with Special Arithmetic and Number Systems. Springer International Publishing, 2017. 389p.

58. Ойстин О. Приглашение в теорию чисел: пер. с англ. 2-е изд. Москва: Едиториал УРСС, 2003. 128 с.

59. Omondi A., Premkumar B. Residue Number Systems: Theory and Implementation (Advances in Computer Science and Engineering Texts). London: Imperial College Press, 2007. 312 p.

60. Krasnobayev V. A., Yanko A. S., Kurchanov V. N., Koshman S. A. The analysis of the tasks and algorithms of data integer processing in the residual classes system // Радіоелектронні і комп'ютерні системи. 2016. № 1 (75). С. 19-28.

61. Koshman S., Yanko A., Krasnobayev V. Algorithms of data

processing in the residual classes system // Problems of Infocommunications Science and Technology PIC S&T 2017: abstr. 4th International Scientific-Practical Conference. Kharkiv, 2017. P. 117-121.

62. Olivier Bordellès. Arithmetic Tales. London: Springer-Verlag, 2006. 556 p.

63. Gbolagade K. A., Cotofana S. D. An 0(n) Residue Number System to Mixed Radix Conversion technique // IEEE International Symposium on Circuits and Systems, 24–27 May, 2009. New York: IEEE, 2009. P. 521-524.

64. Князьков В. С., Волченская Т. В. Компьютерная арифметика: теоретические основы и методы вычислений / LAP Lambert Academic Publishing, 2012. 260 с.

65. Краснобаев В. А., Маврина М. А., Кошман С. А. Контроль, диагностика и исправление ошибок данных, представленных кодом класса вычетов // Системи обробки інформації: збірник наукових праць. Харків. 2013. № 2(109). С. 48-54.

66. Foster I., Kesselman C. The Grid: Blueprint for a New Computing Infrastructure (2nd Edition). San Francisco, Calif.: Morgan Kaufmann, 2004. 748 p.

67. Борисенко О. А. Цифрова схемотехніка: підручник. Суми: Сумський державний університет, 2016. 200 с.

68. Мельник А. О. Архітектура комп’ютера. Наукове видання. Луцьк: Волинська обласна друкарня, 2008. 470 с.

69. Исупов К. С., Князьков В. С. Система остаточных классов как инструмент для выполнения параллельных высокоточных численных расчетов // Математическое моделирование развивающейся экономики, экологии и биотехнологий (ЭКОМОД-2010): сб. тр. V Всероссийской науч. конф., 5–11 июля 2010 г., г. Киров. Киров: ВятГУ, 2010. С. 79-88.

70. Элементы применения компьютерной математики и нейроинформатики / под ред. Н. И. Червякова. М.: ФИЗМАТЛИТ, 2003. 216 с.

71. Michael D. Fried, Moshe Jarden. Fried. Field Arithmetic. Berlin Heidelberg: Springer-Verlag, 2008. 792 p.

72. Операційний пристрій системи обробки інформації по довільному модулю P системи залишкових класів: пат. 83427 Україна. № a 2006 11353; заявл. 27.10.06; опубл. 10.07.08, Бюл. № 13. 15 с.

73. Хеннесси Д., Паттерсон Д. Компьютерная архитектура. Количественный подход: пер. с англ. М. В. Таранчевой / под. ред. А. К. Кима. Москва: Техносфера, 2016. 936 с.

74. Галанина Н. А., Песошин В. А., Иванова Н. Н. Разработка КИХ-фильтров с использованием модульных и немодульных операций системы остаточных классов // Вестник Чувашского университета. 2012. № 3. С. 197–202.

75. Иванс Д. Системы параллельной обработки. Москва: Мир, 1996. 408 с.

76. Пристрій додавання і віднімання чисел за модулем m модулярної системи числення на основі кільцевого зсуву: пат. 55454 Україна. № u 2010 08060; заявл. 29.06.2010; опубл. 10.12.2010, Бюл. № 23. 5 с.

77. Пристрій для додавання та віднімання чисел за модулем m модулярної системи числення на основі кільцевого зсуву: пат. 56858 Україна. № u 2010 09485; заявл. 29.07.2010; опубл. 25.01.2011, Бюл. № 2. 6 с.

78. Пристрій для додавання і віднімання чисел за модулем m модулярної системи числення на основі кільцевого зсуву з контролем помилок: пат. 56684 Україна. № u 2010 07759; заявл. 21.06.2010; опубл. 25.01.2011, Бюл. № 2. 6 с.

79. Krasnobayev V. A., Tyrtyshnikov O. I., Sliusar I. I., Kurchanov V. N., Koshman S. A. The model and the method of implementation of integer arithmetic operations within the RSA crypto algorithms // Системи обробки інформації: збірник наукових праць. Харків. 2014. № 1(117). С. 117-122.

80. Krasnobayev V., Yanko A., Koshman S. Conception of realization of cryptographic RSA transformations with using of the residue number system //

Computer science and cybersecurity. 2016. Issue 2(2). P. 5–12. URL: http://periodicals.karazin.ua/cscs/ issue/viewIssue/454/517. (call date: 26.12.2016)

81. Кошман С. А., Деренько С. Н., Краснобаев В. А. Табличный метод обработки цифровой информации в классе вычетов // Радіоелектронні і комп'ютерні системи. 2006. № 5 (17). С. 171-175.

82. Кошман С. О., Барсов В. І., Краснобаєв В. А. Диверсність табличних методів реалізації арифметичних операцій у системі залишкових класів // Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка. Проблеми енергозабезпечення та енергозбереження в АПК України. 2008. Вип. 73. С. 70-72.

83. Краснобаев В. А., Кошман С. А. Метод быстрой реализации криптографических преобразований на основе поразрядной табличной реализации // Системи обробки інформації. 2009. № 7 (79). С. 63-68.

84. Krasnobayev V. A., Tyrtyshnikov O. I., Somov S. V., Koshman S. A., Sokol G. V., Rvachova N. V. Mathematical model and tabular method implementation of modular arithmetic operations with crypto transformations in the residue class // Системи обробки інформації: збірник наукових праць. Харків. 2014. № 2(118). С. 119-123.

85. Краснобаев В. А., Янко А. С., Кошман С. А. Метод табличной реализации операции умножения в классе вычетов // Системи обробки інформації: збірник наукових праць. Харків. 2014. № 4(120). С. 121-127.

86. Krasnobayev V., Koshman S., Yanko A. Method of tabular realization of arithmetic operations in the system of residual classes // Computer science and cybersecurity. 2016. Issue 3(3). P. 28–35. URL: http://periodicals.karazin.ua/cscs/issue/view/533. (call date: 26.12.2016).

87. Пристрій для множення по довільному модулю: пат. 75965 Україна. № 20040403153; заявл. 27.04.04; опубл. 15.06.06, Бюл. № 6. 5 с.

88. Пристрій для множення у системі залишкових класів по модулю Рі: пат. 27631 Україна. № u 2007 06918; заявл. 19.06.2007; опубл. 12.11.2007,

Бюл. № 18. 6 с.

89. Пристрій для додавання і віднімання чисел за модулем m модулярної системи численн: пат. 58949 Україна. № u 2010 12782; заявл. 28.10.2010; опубл. 26.04.2011, Бюл. № 8. 4 с.

90. Табличний пристрій для множення у ласі лишків: пат. 68803 Україна. № u 2011 11631; заявл. 03.10.2011; опубл. 10.04.2012, Бюл. № 7. 6 с.

91. Табличний пристрій для множення двох чисел у класі лишків: пат. 70442 Україна. № u 2011 14342; заявл. 05.12.2011; опубл. 11.06.2012, Бюл. № 11. 8 с.

92. Пристрій для табличної реалізації арифметичних операцій множення та додавання чисел за модулем mi класу лишків: пат. 106343 Україна. № a 2013 15558; заявл. 30.12.2013; опубл. 11.08.2014, Бюл. № 15. 9 с.

93. Кошман С. О., Деренько М. С. Задача оптимального резервування в класі залишків // Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка. Проблеми енергозабезпечення та енергозбереження в АПК України. 2006. Вип. 43. С. 153-156.

94. Кошман С. А., Сиора А. А., Khere Ali Abdullah, Краснобаев В. А. Повышение надёжности высокопроизводительных процессоров в системе остаточных классов // Радіоелектронні і комп'ютерні системи. 2008. № 7 (34). С. 124-128.

95. Кошман С. А. Метод динамического резервирования в модулярной системе счисления // Інформаційно-керуючі системи на залізничному транспорті: тези доп. Матеріали стендових доповідей та виступів учасників конференції, №4 (приложение). Алушта, Крим. Алушта, 2012. С. 61-62.

96. Информационные системы. Табличная обработка информации / под. ред. Е. П. Балашова, В. Б. Смочова. Ленинград: Энергоиздат, 1985. 184 с.

97. Ananda Mohan. Residue Number Systems. Birkhäuser Basel: 2016. 351 p.

98. Червяков Н. И., Краснобаев В. А. Функциональные блоки и узлы отказоустойчивых и высокопроизводительных систем. Ставрополь: СВВИУС, 1989. 95 с.

99. Исупов К. С., Князьков В. С. Табличный метод прямого преобразования двоичных чисел в систему остаточных классов с модулями {2F 1} // Фундаментальные исследования. 2012. Ч. 4, № 9. С. 909–917.

100. Коляда А. А. О нормированном ядре числа в системе остаточных классов и его вычислениях // Вест. Бел. университета. Сер.1. 1983. №3. С. 12-16.

101. Инютин С. А. Параллельные вычисления в сверхбольших компьютерных диапазонах // Параллельные вычисления и задачи управления (PACO-2001): I международн. конф. Москва: Институт проблем управления им. В. А. Трапезникова, РАН, 2001. С. 76-87.

102. Кошман С., А., Краснобаев В. А., Мороз С. А., Курчанов В. Н., Янко А. С. Модели и методы обработки данных в системе остаточных классов: монография. Харьков: ООО "В деле", 2017. 197 с.

103. Valvano J. Embedded Systems: Real-Time Operating Systems for Arm Cortex M Microcontrollers: 2nd ed. edition. CreateSpace Independent Publishing Platform, 2017. 486 p.

104. Жихарев В. Я., Илюшко Я. В., Кравец Л. Г., Краснобаев В. А. Методы и средства обработки информации в непозиционной системе счисления в остаточных классах. Житомир: Волынь, 2005. 220 с.

105. Барсов В. И., Краснобаев В. А., Фурман И. А. Модели и методы параллельной реализации логических операций в АСУ ТП: монография. Харьков: МОНУ, УИПА, 2009. 140 с.

106. Коляда А. П., Пак. И. Т. Модулярные структуры конвейерной обработки цифровой информации. Минск: Университетское, 1992. 256 с.

107. Краснобаев В. А., Янко А. С., Кошман С. А. Математические модели и алгоритмы возведения целых чисел в квадрат по произвольному модулю класса вычетов // Збірник наукових праць Харківського університету Повітряних Сил. Харків. 2014. Вип. 1(38). С. 132-137.

108. Загумённая Е. В., Кошман С. А., Маврина М. А., Краснобаев В. А. Метод арифметического сравнения чисел в классе вычетов // Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка. Проблеми енергозабезпечення та енергозбереження в АПК України. 2012. Вип. 130. С. 72-75.

109. Исупов К. С. Способ уточненного вычисления приближенной позиционной характеристики для выполнения немодульных операций в системе остаточных классов // Фундаментальные исследования. 2013. № 4. С. 796-800.

110. Пристрій для обчислення двоточкового зрізаного перетворення Фур'є в полі GF(216): пат. 33447 Україна. № u 2008 01389; заявл. 04.02.08; опубл. 25.06.08, Бюл. № 12. 5 с.

111. Пристрій для порівняння даних, що представлені у непозиційній системі числення класу лишків: пат. 79587 Україна. № u 2012 12654; заявл. 05.11.2012; опубл. 25.04.2013, Бюл. № 8. 11 с.

112. Кухарев Г. А. Алгоритмы и систолические процессоры для обработки многозначных данных. Минск: Наука и техника, 1990. 295 с.

113. Пристрій для арифметичного та алгебраїчного порівняння двох чисел у класу лишків: пат. 92069 Україна. № u 2014 02480; заявл. 12.03.2014; опубл. 25.07.2014, Бюл. № 14. 13 с.

114. Пристрій для реалізації операції множення та ділення чисел у системі залишкових класів: пат. 112034 Україна. № a 2015 07299; заявл. 20.07.2015; опубл. 11.07.2016, Бюл. № 13. 13 с.

115. Пристрій для визначення лишків дійсних та комплексних чисел у системі залишкових класів: пат. 114063 Україна. № a 2016 06697; заявл. 21.06.2016; опубл. 10.04.2017, Бюл. № 7. 9 с.

116. Noura H., Theilliol D., Ponsart J.-C., Chamseddine A. Fault-tolerant Control Systems. Design and Practical Applications // Series: Advances in Industrial Control. 1st Edition., 2009. P. 233.

117. Романихин А. В., Кухарев Г. А. Применение нетрадиционных

арифметик в аппаратуре цифровой обработки сигналов. Москва: РУМБ, 1991. 44 с.

118. Исупов К. С. Алгоритм вычисления интервально-позиционной характеристики для выполнения немодульных операций в системах остаточных классов // Вестник ЮУрГУ. Компьютерные технологии, управление, радиоэлектроника. 2014. Т. 14, № 1. С. 89–97.

119. Пристрій для множення комплексних чисел у модулярній системі числення: пат. 33672 Україна. № u 2008 01356; заявл. 04.02.08; опубл. 10.07.08, Бюл. № 13. 6 с.

120. Пристрій для піднесення чисел до квадрата за модулем m: пат. 39493 Україна. № u 2008 12512; заявл. 24.10.08; опубл. 25.02.09, Бюл. № 4. 4 с.

121. Пристрій для складання і віднімання чисел за модулем m системи залишкових класів: пат. 39417 Україна. № u 2008 11616; заявл. 29.09.08; опубл. 25.02.09, Бюл. № 4. 8 с.

122. Суматор по модулю m системи залишкових класів: пат. 86637 Україна. № a 2007 01744; заявл. 19.02.07; опубл. 12.05.09, Бюл. № 9. 5 с.

123. Пристрій для піднесення комплексних чисел в квадрат за комплексним модулем у модулярній системі числення: пат. 40905 Україна. № u 2008 14308; заявл. 12.12.08; опубл. 27.04.09, Бюл. № 8. 4 с.

124. Пристрій для визначення лишків за довільним модулем m модулярної системи числення: пат. 41005 Україна. № u 2008 15174, заявл. 29.12.08; опубл. 27.04.09, Бюл. 8. 3 с.

125. Пристрій для піднесення чисел до довільного степеня за модулем три модулярної системи числення: пат. 41267 Україна. № u 2008 15194; заявл. 29.12.08; опубл. 12.05.09, Бюл. № 9. 3 с.

126. Краснобаев В. А., Кошман С. А., Янко А. С. Методы оперативного контроля данных в системе остаточных классов, основанные на принципе параллельной нулевизации // Прикладная радиоэлектроника: научно-технический журнал. 2016. Том 15, № 3. С. 253-265.

127. Краснобаев В. А., Кошман С. А., Янко А. С. Метод оперативного

контроля данных в системе остаточных классов, основанный на принципе последовательной нулевизации // Радіоелектронні і комп'ютерні системи. 2017. № 1 (81). С. 57-68.

128. Пристрій для контролю помилок даних у комп’ютерних пристроях комутаційно-комунікаційного вузла інформаційно-телекомунікаційної системи, що функціонують у класі лишків: пат. 105742 Україна. № а 2013 08773; заявл. 12.07.2013; опубл. 10.06.2014, Бюл. № 11. 10 с.

129. Пристрій для контролю даних комп’ютерних пристроїв телекомунікаційної системи, що функціонують у класі лишків: пат. 105455 Україна. № а 2013 07289; заявл. 10.06.2013; опубл. 12.05.2014, Бюл. № 9. 8 с.

130. Краснобаев В. А., Кошман С. А., Курчанов В. Н., Гарамась А. В. Метод контроля криптографической информации, представленной в модулярной системе счисления // Збірник наукових праць Харківського університету Повітряних Сил ім. І. Кожедуба. Харків. 2013. Вип. 3(36). С. 104-107.

131. Краснобаев В. А., Янко А. С., Бендес Ю. П., Кошман С. А. Метод контроля данных в системе остаточных классов // Оралдын Гылым Жаршысы (Уральский научный вестник): Научно-теоретический и практический журнал. Уральск (Казахстан): ТОО "Уралнаучкнига", 2015. Вып. 5(136). С. 103-117.

132. Krasnobayev V., Yanko A., Koshman S. The method of error detection and correction in the system of residual classes // Computer science and cybersecurity. 2016. Issue 1(1). P. 58–66. URL: http://periodicals.karazin.ua/cscs/issue/viewIssue/453/510 (call date: 26.12.2016).

133. Кудряшов Б. Д. Основы теории кодирования: учеб. пособие. СПб.: БХВ-Петербург, 2016. 400 с.

134. Cook J. W. Methods in Written Arithmetic (Classic Reprint). Fb&c Limited, 2015. 188 p.

135. Chervyakov N. I. Residue-to-binary conversion for general moduli sets based on approximate Chinese remainder theorem // International Journal of

Computer Mathematics. 2017. Т. 94, №. 9. С. 1833-1849.

136. ISCI’2017: Information Security in Critical Infrastructures: monograph: / Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov. ASC Academic Publishing, USA, 2017. 207 p.

137. Пристрій для контролю даних комп’ютерних пристроїв телекомунікаційної системи, що функціонують у класі лишків: пат. 79673 Україна. № u 2012 13145; заявл. 19.11.2012; опубл. 25.04.2013, Бюл. № 8. 9 с.

138. Пристрій для контролю та корекції помилок даних комп’ютерних пристроїв комутаційно-комунікаційного вузла телекомунікаційної мережі, що функціонують у класі лишків: пат. 105436 Україна. № a 2013 00476; заявл. 14.01.2013; опубл. 12.05.2014, Бюл. № 9. 11 с.

139. Кошман С. А. Методы контроля, диагностики и коррекции ошибок данных, представленных в системе остаточных классов // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління: тези доп. Четвертої міжнародної науково-технічної конференції, Полтава: ПНТУ; Баку: ВА ЗС АР; Бєлгород: НДУ "БєлДУ"; Кіровоград: КЛА НАУ; Харків: ДП "ХНДІ ТМ". Харків, 2014. С. 66.

140. Krasnobayev V. A., Koshman S. A., Mavrina M. A. A method for increasing the reliability of verification of data represented in a residue number system // Cybernetics and Systems Analysis. November 2014. Vol. 50, Issue 6. PP 969-976.

141. Самсонов Б. Б., Плохов Е. М., Филоненков А. И. Компьютерная математика. Ростов-на-Дону: Феникс, 2002. 512 с.

142. Червяков Н. И., Бабенко М. Г., Ляхов П. А. Аналитический обзор методов определения позиционных характеристик в системе остаточных классов // Нейрокомпьютеры: разработка, применение. 2012. № 12. С. 27–30.

143. Пристрій для контролю та діагностики даних, що представлені у системі залишкових класів: пат. 112731 Україна. № a 2015 10904; заявл. 09.11.2015; опубл. 10.10.2016, Бюл. № 19. 15 с.

144. Чернов В. М. Арифметические методы синтеза быстрых

алгоритмов дискретных ортогональных преобразований. ФИЗМАТЛИТ, 2007. 264 с.

145. Chervyakov N. I. Use of modular coding for high-speed digital filter design //Cybernetics and Systems Analysis. 1998. Т. 34, №. 2. С. 254-260.

146. Жмакин А. П. Архитектура ЭВМ: 2-е изд., перераб. и доп.: учеб. пособие. СПб.: БХВ-Петербург, 2010. 352 с.

147. Николайчук Я. М., Волинський О. І., Кулина С. В. Швидкодіючий алгоритм та процесор порівняння чисел у системі залишкових класів базису Крестенсона // Искусственный интеллект. 2008. № 3. С. 348–352.

148. Tariq Jamil. Complex Binary Number System. Algorithms and Circuits. India: Springer, 2013. 83 p.

149. Ирхин В. П. Проектирование непозиционных специализированных процессоров. Воронеж: Воронежский государственный университет, 1999. 136 с.

150. Patterson D. A. The Morgan Kaufmann Series in Computer Architecture and Design: 1 edition. Morgan Kaufmann, 2016. 914 p.

151. Таненбаум Э., Остин Т. Архитектура компьютера: 6-е изд. / перевод с англ. Е. Матвеев. Санкт-Петербург: Питер, 2013. 816 с.

152. Mi Lu. Arithmetic and Logic in Computer Systems. John Wiley & Sons. 2005. 246 p.

153. Кошман С. А. Особенности матричного способа реализации процессора в СОК // Інтегровані комп’ютерні технології в машинобудуванні ІКТМ-2005: тези доп. Міжнародної науково-технічної конференції. Харків, 2005. С. 314.

154. Кошман С. А. Метод поразрядной табличной реализации арифметических операций в системе остаточных классов // Радиоэлектроника и молодёжь в XXI веке: тезисы докл. 13-го международного молодёжного форума. Харьков, 2009. Ч. 1. С. 128.

155. Краснобаев В. А. Быстрая реализация криптографических

преобразований на эллиптических кривых // Системи обробки інформації: тези доп. II міжнародної науково-практичної конференції. Харків, 2009. Вип. 7(79). С. 135–136.

156. Пристрій для множення двох лишків за довільним модулем класу лишків: пат. 92403 Україна. № u 2014 03259; заявл. 31.03.2014; опубл. 11.08.2014, Бюл. № 15. 7 с.

157. Пристрій для піднесення цілих чисел, що представлені у класі лишків, до ступеня натурального числа: пат. 95060 Україна. № u 2014 06854; заявл. 18.06.2014; опубл. 10.12.2014, Бюл. № 23. 4 с.

158. Пристрій для реалізації операції модульного множення двох чисел, які представлені у системі залишкових класів: пат. 108828 Україна. № a 2014 10608; заявл. 29.09.2014; опубл. 10.06.2015, Бюл. № 11. 14 с.

159. Пристрій для підсумовування в модулярній системі числення за модулем три: пат. 42437 Україна. № u 2008 14704; заявл. 22.12.2008; опубл. 10.07.09, Бюл. № 13. 3 с.

160. Пристрій для виявлення та виправлення помилок у модулярній системі числення: пат. 47563 Україна. № u 2009 09006; заявл. 31.08.2009; опубл. 10.02.2010, Бюл. № 3. 5 с.

161. Пристрій для реалізації операції множення двох чисел у класі лишків: пат. 91321 Україна. № u 2014 01726; заявл. 24.02.2014; опубл. 25.06.2014, Бюл. № 12. 10 с.

162. Кошман С. О. Методи реалізації арифметичних операцій у системі залишкових класів // Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка. Проблеми енергозабезпечення та енергозбереження в АПК України. 2010. Вип. 102. С. 77-79.

163. Краснобаев В. А., Кошман С. А., Маврина М. А. Метод повышения достоверности контроля данных, представленных в системе остаточных классов // Кибернетика и системный анализ. 2014. Том. 50, № 6. С. 167-175.

164. Кошман С. А., Краснобаев В. А. Метод оперативного диагностирования данных, представленных в системе остаточных классов // Кибернетика и системный анализ. 2018. Том. 54, № 2. С. 182–192.

165. Krasnobayev V. A., Yanko A. S., Koshman S. A. The method of error correction in the system of residual classes // Nauka i studia. 2015. NR 5(136). P. 51-62.

166. Krasnobayev V., Kuznetsov A., Koshman S., Moroz S. Improved method of determining the alternative set of numbers in residue number system // Recent Developments in Data Science and Intelligent Analysis of Information. Proceedings of the XVIII International Conference on Data Science and Intelligent Analysis of Information, June 4–7, 2018. Kyiv, 2018. P. 319-328.

167. Кошман С. А., Краснобаев В. А., Янко А. С. Усовершенствованный метод определения альтернативной совокупности чисел в системе остаточных классов // Радиотехника. Всеукраинский межведомственный научно-технический сборник. Харьков: ХНУРЭ. 2017. Вип. 189. С. 29-37.

168. Krasnobayev V. A., Yanko A. S., Koshman S. A. Method for arithmetic comparison of data represented in a residue number system // Cybernetics and Systems Analysis. January 2016. Vol. 52, Issue 1. P. 145-150.

169. Пристрій для множення лишків ai та bi числа за довільним модулем mi системи залишкових класів: пат. 110901 Україна. № a 2015 01377; заявл. 18.02.2015; опубл. 25.02.2016, Бюл. № 4. 8 с.

170. Пристрій для множення лишків ai та bi чисел за модулем mi: пат. 110913 Україна. № a 2015 05097; заявл. 25.05.2015; опубл. 25.02.2016, Бюл. № 4. 11 с.

171. Кошман С. А. Особенности применения табличных методов обработки информации в модулярной системе счисления // Новітні технології для захисту повітряного простору: тези доп. Десятої наукової конференції Харківського університету Повітряних Сил імені Івана Кожедуба, 9–10 квітня 2014 р. Харків, 2014. С. 185.

172. Koshman S. A., Krasnobayev V. A. A method for operational diagnosis of data represented in a residue number system // Cybernetics and Systems Analysis. March 2018. Vol. 54, Issue 2. P. 336-344.

173. Кошман С. А. Контроль, диагностика и коррекция данных, представленных в системе остаточных классов // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління: тези доп. Четвертої міжнародної науково-технічної конференції, Полтава: ПНТУ; Баку: ВА ЗС АР; Бєлгород: НДУ "БєлДУ"; Кіровоград: КЛА НАУ; Харків: ДП "ХНДІ ТМ". Харків, 2017. С. 42.

174. Dukkipati R. V. Numerical Methods. New Age International, 2010. 352 p.

175. Евдокимов Л. Л., Тихонов Э. Е. Защита данных в облачных технологиях: монография. Невинномысск: Издательство НИЭУП, 2015г. 102 с.

176. Краснобаев В. А., Чернецкая И. А., Кошман С. А., Мартыненко А. М. Метод обработки данных в классе вычетов // Збірник наукових праць Харківського університету Повітряних Сил. Харків. 2014. Вип. 2(39). С. 121-126.

177. Краснобаев В. А., Янко А. С., Кошман С. А. Метод арифметического сравнения данных, представленных в системе остаточных классов // Кибернетика и системный анализ. 2016. Том. 52, № 1. С. 157–162.

178. Краснобаев В. А., Кошман С. А., Маврина М. А. Метод исправления однократных ошибок данных, представленных кодом класса вычетов // Электронное моделирование. 2013. Том 35, № 5. С. 43-56.

179. Краснобаев В. А., Янко А. С., Кошман С. А. Метод возведения остатков целых чисел по произвольному модулю системы остаточных классов в степень натурального числа // Радіоелектронні і комп'ютерні системи. Харків. 2015. № 1(71). С. 54–63.

180. Кошман С. А. Разработка и исследование методов нулевизации в системе остаточных классов // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління: тези доп. П'ятої

міжнародної науково-технічної конференції, Полтава: ПНТУ; Баку: ВА ЗС АР; Бєлгород: НДУ "БєлДУ"; Кіровоград: КЛА НАУ; Харків: ДП "ХНДІ ТМ". Харків, 2015. С. 39.

181. Кошман С. А. Методы нулевизации чисел в системе остаточных классов // Проблеми інформатизації: тези доп. Третьої міжнародної науково-технічної конференції, Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН; Полтава: ПНТУ. Харків, 2015. С. 45.

Додаток А

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації

Монографії:

1. Кошман С. А., Краснобаев В. А., Мороз С. А., Курчанов В. Н., Янко А. С. Модели и методы обработки данных в системе остаточных классов: монография. Харьков: ООО "В деле", 2017. 197 с. (*Особистий внесок здобувача: розроблено методи обробки даних, що представлені у СЗК*).

2. ISCI’2017: Information Security in Critical Infrastructures: monograph: / Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov. ASC Academic Publishing, USA, 2017. 207 p. (*Особистий внесок здобувача: розроблено методи обробки даних, що представлені у СЗК*).

3. Koshman S., Krasnobayev V., Kuznetsov A., Rassomakhin S., Zamula A., Kavun S. Effective Data Processing in Coding, Digital Signals and Cryptography: monograph. ASC Academic Publishing, 2018. 352 p. (*Особистий внесок здобувача: розроблено методи обробки даних, що представлені у СЗК*).

Публікації у фахових виданнях України:

4. Кошман С. А. Концепция создания системы обработки цифровой информации на основе использования системы остаточных классов // Радіоелектронні і комп'ютерні системи. 2010. № 7 (48). С. 138-141.

5. Кошман С. О. Метод реалізації арифметичних операцій у системі залишкових класів // Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка. Проблеми енергозабезпечення та енергозбереження в АПК України. 2010. Вип. 102. С. 77-79.

6. Кошман С. А., Загумённая Е. В. Анализ особенностей

функционирования автоматизированной системы управления турбоустановками // Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка. Проблеми енергозабезпечення та енергозбереження в АПК України. 2011. Вип. 116. С. 117-120. (*Особистий внесок здобувача: досліджені особливості проектування КСКОЦД реального часу*).

7. Кошман С. О. Концепція підвищення продуктивності обробки інформації у реальному часі // Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка. Проблеми енергозабезпечення та енергозбереження в АПК України. 2011. Вип. 117. С. 63-65.

8. Кошман С. А., Краснобаев В. А., Маврина М. А. Методы оптимального резервирования в модулярной системе счисления // Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка. Проблеми енергозабезпечення та енергозбереження в АПК України. 2012. Вип. 129. С. 105-108. (*Особистий внесок здобувача: вдосконалено метод оптимального резервування КСКОЦД у СЗК*).

9. Загумённая Е. В., Кошман С. А., Маврина М. А., Краснобаев В. А. Метод арифметического сравнения чисел в классе вычетов // Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка. Проблеми енергозабезпечення та енергозбереження в АПК України. 2012. Вип. 130. С. 72-75. (*Особистий внесок здобувача: розроблено метод арифметичного порівняння чисел у СЗК*).

10. Краснобаев В. А., Маврина М. А., Кошман С. А. Контроль, диагностика и исправление ошибок данных, представленных кодом класса вычетов // Системи обробки інформації: збірник наукових праць. Харків. 2013. № 2(109). С. 48-54. (*Особистий внесок здобувача: досліджено коригувальні властивості кодів, що представлені у СЗК*).

11. Краснобаев В. А., Маврина М. А., Кошман С. А., Курчанов В. Н. Концепция создания компьютерных средств обработки данных на основе

использования кодов класса вычетов // Системи обробки інформації: збірник наукових праць. Харків. 2013. № 4(111). С. 133-138. (*Особистий внесок здобувача: досліджено особливості застосування кодів у СЗК при побудові КСКОЦД*).

12. Кошман С. А., Краснобаев В. А., Сомов С. В., Крючко Е. А. Метод быстрой обработки криптографической информации в модулярной системе счисления // Системи обробки інформації: збірник наукових праць. Харків. 2013. № 6(113). С. 194-198. (*Особистий внесок здобувача: розроблено метод швидкої обробки інформації, що представлена у СЗК*).

13. Кошман С. А., Краснобаев В. А., Тыртышников А. И., Гаркавенко Н. С. Концепция создания отказоустойчивых компьютерных систем обработки информации в системе остаточных классов на основе применения ПЛИС // Системи обробки інформації: збірник наукових праць. Харків. 2013. № 7(114). С. 79-82. (*Особистий внесок здобувача: досліджено шляхи підвищення продуктивності та достовірності обробки даних у КСКОЦД)*.

14. Краснобаев В. А., Кошман С. А., Курчанов В. Н., Гарамась А. В. Метод контроля криптографической информации, представленной в модулярной системе счисления // Збірник наукових праць Харківського університету Повітряних Сил ім. І. Кожедуба. Харків. 2013. Вип. 3(36). С. 104-107. (*Особистий внесок здобувача: розроблено метод контролю, який заснований на принципі нульовизації даних у СЗК*).

15. Краснобаев В. А., Кошман С. А., Маврина М. А. Метод исправления однократных ошибок данных, представленных кодом класса вычетов // Электронное моделирование. 2013. Том 35, № 5. С. 43-56. (*Особистий внесок здобувача: вдосконалено метод виправлення одноразових помилок даних у СЗК*).

16. Краснобаев В. А., Кошман С. А., Маврина М. А. Метод повышения достоверности контроля данных, представленных в системе остаточных классов // Кибернетика и системный анализ. 2014. Том. 50, № 6.

С. 167-175. (*Особистий внесок здобувача: дано обґрунтування низької достовірності контролю даних представлених у СЗК*).

17. Koshman S. A., Krasnobayev V. A., Tyrtyshnikov O. I., Sliusar I. I., Kurchanov V. N. The model and the method of implementation of integer arithmetic operations within the RSA crypto algorithms // Системи обробки інформації: збірник наукових праць. Харків. 2014. № 1(117). С. 117-122. (*Особистий внесок здобувача: вдосконалено метод реалізації цілочислових арифметичних операцій)*.

18. Кошман С. А., Краснобаев В. А., Янко А. С. Математические модели и алгоритмы возведения целых чисел в квадрат по произвольному модулю класса вычетов // Збірник наукових праць Харківського університету Повітряних Сил. Харків. 2014. Вип. 1(38). С. 132-137. (*Особистий внесок здобувача: вдосконалені математичні моделі піднесення цілих чисел у квадрат за довільним модулем класу лишків)*.

19. Krasnobayev V. A., Tyrtyshnikov O. I., Somov S. V., Koshman S. A., Sokol G. V., Rvachova N. V. Mathematical model and tabular method implementation of modular arithmetic operations with crypto transformations in the residue class // Системи обробки інформації: збірник наукових праць. Харків. 2014. № 2(118). С. 119-123. (*Особистий внесок здобувача: вдосконалено метод табличної обробки даних у СЗК)*.

20. Краснобаев В. А., Янко А. С., Кошман С. А. Метод табличной реализации операции умножения в классе вычетов // Системи обробки інформації: збірник наукових праць. Харків. 2014. № 4(120). С. 121-127. (*Особистий внесок здобувача: вдосконалено метод реалізації арифметичних операцій у СЗК*).

21. Кошман С. А., Краснобаев В. А., Чернецкая И. А., Мартыненко А. М. Метод обработки данных в классе вычетов // Збірник наукових праць Харківського університету Повітряних Сил. Харків. 2014. Вип. 2(39). С. 121-126. (*Особистий внесок здобувача: вдосконалено метод обробки даних у СЗК*).

22. Краснобаев В. А., Янко А. С., Гроза П. Н., Кошман С. А., Гроза А. П., Бендес Ю. П. Расчет и сравнительный анализ производительности компьютерной системы обработки целочисленных данных, функционирующей в системе остаточных классов // Системи обробки інформації: збірник наукових праць. Харків. 2015. № 1(126). С. 111 - 117. (*Особистий внесок здобувача: проведено розрахунок продуктивності комп'ютерних систем у СЗК*).

23. Краснобаев В. А., Янко А. С., Кошман С. А., Сомов С. А., Бендес Ю. П. Исследование производительности компьютерной системы обработки целочисленных данных, функционирующей в системе остаточных классов // Збірник наукових праць Харківського університету Повітряних Сил. Харків. 2015. Вип. 1(42). С. 48-52. (*Особистий внесок здобувача: виведені аналітичні вирази для розрахунку продуктивності комп'ютерних систем обробки цілочислових даних у СЗК*).

24. Краснобаев В. А., Янко А. С., Кошман С. А., Курчанов В. Н., Бендес Ю. П. Расчет и сравнительный анализ производительности компьютерной системы обработки целочисленных данных, представленных в системе остаточных классов // Системи обробки інформації: збірник наукових праць. Харків. 2015. Вип. 3(128). С. 57-61. (*Особистий внесок здобувача: досліджено вплив властивостей СЗК на продуктивність комп'ютерних систем*).

25. Краснобаев В. А., Янко А. С., Кошман С. А. Метод возведения остатков целых чисел по произвольному модулю системы остаточных классов в степень натурального числа // Радіоелектронні і комп'ютерні системи. Харків. 2015. № 1(71). С. 54–63. (*Особистий внесок здобувача: розроблено метод піднесення залишків за довільним модулем СЗК у ступінь натурального числа)*.

26. Krasnobayev V. A., Yanko A. S., Kurchanov V. N., Koshman S. A. The analysis of the tasks and algorithms of data integer processing in the residual classes system // Радіоелектронні і комп'ютерні системи. 2016. № 1 (75). С. 19-

28. (*Особистий внесок здобувача: проведено аналіз задач та алгоритмів реалізації цілочислових арифметичних операції у СЗК)*.

27. Краснобаев В. А., Янко А. С., Кошман С. А. Метод арифметического сравнения данных, представленных в системе остаточных классов // Кибернетика и системный анализ. 2016. Том. 52, № 1. С. 157–162. (*Особистий внесок здобувача: вдосконалено метод арифметичного порівняння даних у СЗК*).

28. Краснобаев В. А., Кошман С. А., Янко А. С. Метод оперативного контроля данных в системе остаточных классов, основанный на принципе последовательной нулевизации // Радіоелектронні і комп'ютерні системи. 2017. № 1 (81). С. 57-68. (*Особистий внесок здобувача: розроблено метод оперативного контролю даних у СЗК на основі принципу нульовизації)*.

29. Кошман С. А., Краснобаев В. А. Метод оперативного диагностирования данных, представленных в системе остаточных классов // Кибернетика и системный анализ. 2018. Том. 54, № 2. С. 182–192. (*Особистий внесок здобувача: розроблено метод оперативного діагностування даних у СЗК*).

***Наукові праці, в яких опубліковані основні наукові результати дисертації у зарубіжних спеціалізованих виданнях*:**

30. Krasnobayev V. A., Koshman S. A. Method of realization of cryptographic RSA transformations on the basis of application of modular number system // International Journal of Biomedical Soft Computing and Human Sciences. 2011. Vol. 17, № 2. P. 31-36. (*Особистий внесок здобувача: вдосконалення методу реалізації криптографічних перетворень на основі використання СЗК*).

31. Krasnobayev V. A., Koshman S. A., Mavrina M. A. A method for increasing the reliability of verification of data represented in a residue number system // Cybernetics and Systems Analysis. November 2014. Vol. 50, Issue 6.

P. 969-976. (*Особистий внесок здобувача: розроблено метод підвищення достовірності контролю даних представлених у СЗК)*. (Видання входить до міжнародної наукометричної бази Scopus).

32. Краснобаев В. А., Янко А. С., Бендес Ю. П., Кошман С. А. Метод контроля данных в системе остаточных классов // Оралдын Гылым Жаршысы (Уральский научный вестник): Научно-теоретический и практический журнал. Уральск (Казахстан): ТОО "Уралнаучкнига", 2015. Вып. 5(136). С. 103-117. (*Особистий внесок здобувача: удосконалено метод контролю даних у СЗК)*.

33. Krasnobayev V. A., Yanko A. S., Koshman S. A. The method of error correction in the system of residual classes // Nauka i studia. 2015. NR 5(136). P. 51-62. (*Особистий внесок здобувача: досліджено методи корекції помилок даних у СЗК*).

34. Krasnobayev V. A., Yanko A. S., Koshman S. A. Method for arithmetic comparison of data represented in a residue number system // Cybernetics and Systems Analysis. January 2016. Vol. 52, Issue 1. P. 145-150. (*Особистий внесок здобувача: вдосконалено метод арифметичного порівняння даних у СЗК*). (Видання входить до міжнародної наукометричної бази Scopus).

35. Koshman S. A., Krasnobayev V. A. A method for operational diagnosis of data represented in a residue number system // Cybernetics and Systems Analysis. March 2018. Vol. 54, Issue 2. P. 336-344. (*Особистий внесок здобувача: розроблено метод оперативного діагностування даних у СЗК*). (Видання входить до міжнародної наукометричної бази Scopus)

Патенти:

36. Пристрій додавання і віднімання чисел за модулем *m* модулярної системи числення на основі кільцевого зсуву: пат. 55454 Україна. № u 2010 08060; заявл. 29.06.2010; опубл. 10.12.2010, Бюл. № 23. 4 с. (*Особистий внесок здобувача: алгоритм роботи пристрою для додавання і віднімання*

чисел за модулем m модулярної системи числення на основі кільцевого зсуву).

37. Пристрій для додавання та віднімання чисел за модулем *m* модулярної системи числення на основі кільцевого зсуву: пат. 56858 Україна. № u 2010 09485; заявл. 29.07.2010; опубл. 25.01.2011, Бюл. № 2. 6 с. (*Особистий внесок здобувача: алгоритм роботи пристрою для додавання та віднімання чисел за модулем m на основі кільцевого зсуву*).

38. Пристрій для додавання і віднімання чисел за модулем *m* модулярної системи числення на основі кільцевого зсуву з контролем помилок: пат. 56684 Україна. № u 2010 07759; заявл. 21.06.2010; опубл. 25.01.2011, Бюл. № 2. 6 с. (*Особистий внесок здобувача: алгоритм роботи пристрою для додавання і віднімання чисел за модулем m модулярної системи числення на основі кільцевого зсуву з контролем помилок*).

39. Пристрій для додавання і віднімання чисел за модулем *m* модулярної системи числення: пат. 58949 Україна. № u 2010 12782; заявл. 28.10.2010; опубл. 26.04.2011, Бюл. № 8. 4 с. (*Особистий внесок здобувача: алгоритм роботи пристрою для додавання і віднімання чисел за модулем m модулярної системи числення)*.

40. Табличний пристрій для множення у класі лишків: пат. 68803 Україна. № u 2011 11631; заявл. 03.10.2011; опубл. 10.04.2012, Бюл. № 7. 6 с. (*Особистий внесок здобувача: алгоритм роботи табличного пристрою для множення у класі лишків*).

41. Табличний пристрій для множення двох чисел у класі лишків: пат. 70442 Україна. № u 2011 14342; заявл. 05.12.2011; опубл. 11.06.2012, Бюл. № 11. 6 с. (*Особистий внесок здобувача: алгоритм роботи табличного пристрою для множення двох чисел у класі лишків*).

42. Пристрій для порівняння даних, що представлені у непозиційній системі числення класу лишків: пат. 79587 Україна. № u 2012 12654; заявл. 05.11.2012; опубл. 25.04.2013, Бюл. № 8. 6 с. (*Особистий внесок здобувача: алгоритм роботи пристрою для порівняння даних, що представлені у непозиційній системі числення класу лишків)*.

43. Пристрій для контролю даних комп'ютерних пристроїв телекомунікаційної системи, що функціонують у класі лишків: пат. 79673 Україна. № u 2012 13145; заявл. 19.11.2012; опубл. 25.04.2013, Бюл. № 8. 4 с. (*Особистий внесок здобувача: алгоритм роботи пристрою для контролю даних комп'ютерної системи, що функціонує у класі лишків)*.

44. Пристрій для контролю та корекції помилок даних комп'ютерних пристроїв комутаційно-комунікаційного вузла телекомунікаційної мережі, що функціонують у класі лишків: пат. 105436 Україна. № a 2013 00476; заявл. 14.01.2013; опубл. 12.05.2014, Бюл. № 9. 6 с. (*Особистий внесок здобувача: алгоритм роботи пристрою для контролю та корекції помилок даних компонентів комп'ютерних систем, що функціонують у класі лишків)*.

45. Пристрій для контролю даних комп'ютерних пристроїв телекомунікаційної системи, що функціонують у класі лишків: пат. 105455 Україна. № a 2013 07289; заявл. 10.06.2013; опубл. 12.05.2014, Бюл. № 9. 6 с. (*Особистий внесок здобувача: метод контролю даних комп'ютерних пристроїв, що функціонують у СЗК*).

46. Пристрій для контролю помилок даних у комп'ютерних пристроях комутаційно-комунікаційного вузла інформаційно-телекомунікаційної системи, що функціонують у класі лишків: пат. 105742 Україна. № a 2013 08773; заявл. 12.07.2013; опубл. 10.06.2014, Бюл. № 11. 6 с. (*Особистий внесок здобувача: алгоритм роботи пристрою для контролю помилок даних у комп'ютерних пристроях комутаційно-комунікаційного вузла інформаційно-телекомунікаційної системи, що функціонують у класі лишків*).

47. Пристрій для реалізації операції множення двох чисел у класі лишків: пат. 91321 Україна. № u 2014 01726; заявл. 24.02.2014; опубл. 25.06.2014, Бюл. № 12. 4 с. (*Особистий внесок здобувача: алгоритм роботи пристрою для реалізації операції множення двох чисел у класі лишків*).

48. Пристрій для арифметичного та алгебраїчного порівняння двох чисел у класу лишків: пат. 92069 Україна. № u 2014 02480; заявл. 12.03.2014;

опубл. 25.07.2014, Бюл. № 14. 6 с. (*Особистий внесок здобувача: алгоритм роботи пристрою для арифметичного та алгебраїчного порівняння двох чисел у класу лишків)*.

49. Пристрій для табличної реалізації арифметичних операцій множення та додавання чисел за модулем m_i класу лишків: пат. 106343 Україна. № a 2013 15558; заявл. 30.12.2013; опубл. 11.08.2014, Бюл. № 15. 6 с. (*Особистий внесок здобувача: алгоритм роботи пристрою для табличної реалізації арифметичних операцій множення та додавання чисел за модулем m класу лишків*).

50. Пристрій для множення двох лишків за довільним модулем класу лишків: пат. 92403 Україна. № u 2014 03259; заявл. 31.03.2014; опубл. 11.08.2014, Бюл. № 15. 4 с. (*Особистий внесок здобувача: алгоритм роботи пристрою для множення двох лишків за довільним модулем класу лишків*).

51. Пристрій для піднесення цілих чисел, що представлені у класі лишків, до ступеня натурального числа: пат. 95060 Україна. № u 2014 06854; заявл. 18.06.2014; опубл. 10.12.2014, Бюл. № 23. 4 с. (*Особистий внесок здобувача: алгоритм роботи пристрою для піднесення цілих чисел, що представлені у класі лишків, до ступеня натурального числа*).

52. Пристрій для реалізації операції модульного множення двох чисел, які представлені у системі залишкових класів: пат. 108828 Україна. № a 2014 10608; заявл. 29.09.2014; опубл. 10.06.2015, Бюл. № 11. 6 с. (*Особистий внесок здобувача: алгоритм роботи пристрою для реалізації операції модульного множення двох чисел, які представлені у системі залишкових класів*).

53. Пристрій для множення лишків a_i та b_i числа за довільним модулем m_i системи залишкових класів: пат. 110901 Україна. № a 2015 01377; заявл. 18.02.2015; опубл. 25.02.2016, Бюл. № 4. 6 с. (*Особистий внесок здобувача: алгоритм роботи пристрою для множення лишків a_i та b_i числа за довільним модулем m_i системи залишкових класів*).

54. Пристрій для множення лишків a_i та b_i чисел за модулем m_i: пат.

110913 Україна. № а 2015 05097; заявл. 25.05.2015; опубл. 25.02.2016, Бюл. № 4. 6 с. (*Особистий внесок здобувача: алгоритм роботи пристрою для множення лишків a_i та b_i чисел за модулем m_i*).

55. Пристрій для реалізації операції множення та ділення чисел у системі залишкових класів: пат. 112034 Україна. № а 2015 07299; заявл. 20.07.2015; опубл. 11.07.2016, Бюл. № 13. 6 с. (*Особистий внесок здобувача: алгоритм роботи пристрою для реалізації операції множення та ділення чисел у системі залишкових класів*).

56. Пристрій для контролю та діагностики даних, що представлені у системі залишкових класів: пат. 112731 Україна. № а 2015 10904; заявл. 09.11.2015; опубл. 10.10.2016, Бюл. № 19. 6 с. (*Особистий внесок здобувача: алгоритм роботи пристрою для контролю та діагностики даних, що представлені у системі залишкових класів*).

57. Пристрій для визначення лишків дійсних та комплексних чисел у системі залишкових класів: пат. 114063 Україна. № а 2016 06697; заявл. 21.06.2016; опубл. 10.04.2017, Бюл. № 7. 6 с. (*Особистий внесок здобувача: алгоритм роботи пристрою для визначення лишків дійсних та комплексних чисел у системі залишкових класів)*.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

58. Кошман С. А. Метод динамического резервирования в модулярной системе счисления // Інформаційно-керуючі системи на залізничному транспорті: тези доп. Матеріали стендових доповідей та виступів учасників конференції, №4. Алушта, Крим. Алушта, 2012. С. 61-62.

59. Кошман С. А. Особенности применения табличных методов обработки информации в модулярной системе счисления // Новітні технології для захисту повітряного простору: тези доп. Десятої наукової конференції Харківського університету Повітряних Сил імені Івана Кожедуба, 9–10 квітня 2014 р. Харків, 2014. С. 185.

60. Кошман С. А. Концепция реализации немодульных операций в модулярной системе счисления // Проблеми інформації: тези доп. Другої міжнародної науково-технічної конференції, Київ: ДУТ; Полтава: ПНТУ; Катовище: Катовицький економічний університет; Париж: Університет Париж VII Вєнсент-Сен-Дєні; Білгород: "БДУ"; Черкаси: ЧДТУ; Харків: ХНДІТМ, 12–13 квітня 2014 року. Харків, 2014. С. 94-95.

61. Кошман С. А. Методы контроля, диагностики и коррекции ошибок данных, представленных в системе остаточных классов // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління: тези доп. Четвертої міжнародної науково-технічної конференції, Полтава: ПНТУ; Баку: ВА ЗС АР; Бєлгород: НДУ "БєлДУ"; Кіровоград: КЛА НАУ; Харків: ДП "ХНДІ ТМ". Харків, 2014. С. 66.

62. Кошман С. А. Разработка и исследование методов нулевизации в системе остаточных классов // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління: тези доп. П'ятої міжнародної науково-технічної конференції, Полтава: ПНТУ; Баку: ВА ЗС АР; Бєлгород: НДУ "БєлДУ"; Кіровоград: КЛА НАУ; Харків: ДП "ХНДІ ТМ". Харків, 2015. С. 39.

63. Кошман С. А. Методы нулевизации чисел в системе остаточных классов // Проблеми інформатизації: тези доп. Третьої міжнародної науково-технічної конференції, Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН; Полтава: ПНТУ. Харків, 2015. С. 45.

64. Кошман С. А. Контроль, диагностика и коррекция данных, представленных в системе остаточных классов // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління: тези доп. Четвертої міжнародної науково-технічної конференції, Полтава: ПНТУ; Баку: ВА ЗС АР; Бєлгород: НДУ "БєлДУ"; Кіровоград: КЛА НАУ; Харків: ДП "ХНДІ ТМ". Харків, 2017. С. 42.

65. Koshman S., Yanko A., Krasnobayev V. Algorithms of data processing in the residual classes system // Problems of Infocommunications

Science and Technology PIC S&T 2017: abstr. 4th International Scientific-Practical Conference. Kharkiv, 2017. P. 117-121. (*Особистий внесок здобувача: досліджено принципи побудови непозиційних кодових структур*). (Видання входить до міжнародної наукометричної бази Scopus).

66. Krasnobayev V., Kuznetsov A., Koshman S., Moroz S. Improved method of determining the alternative set of numbers in residue number system // Recent Developments in Data Science and Intelligent Analysis of Information. Proceedings of the XVIII International Conference on Data Science and Intelligent Analysis of Information, June 4–7, 2018. Kyiv, 2018. P. 319-328. (*Особистий внесок здобувача: розроблено метод діагностики даних у СЗК*). (Видання входить до міжнародної наукометричної бази Scopus).

***Наукові праці, які додатково відображають наукові результати дисертації*:**

67. Краснобаев В. А., Кошман С. А., Янко А. С. Методы оперативного контроля данных в системе остаточных классов, основанные на принципе параллельной нулевизации // Прикладная радиоэлектроника: научно-технический журнал. 2016. Том 15, № 3. С. 253-265. (*Особистий внесок здобувача: розроблено метод оперативного контролю даних у СЗК на основі принципу паралельної нульовизації*).

68. Krasnobayev V., Yanko A., Koshman S. The method of error detection and correction in the system of residual classes // Computer science and cybersecurity. 2016. Issue 1(1). P. 58–66. URL: http://periodicals.karazin.ua/cscs/issue/viewIssue/453/510 (call date: 26.12.2016). (*Особистий внесок здобувача: вдосконалено метод виправлення помилок даних у СЗК*).

69. Krasnobayev V., Yanko A., Koshman S. Conception of realization of cryptographic RSA transformations with using of the residue number system // Computer science and cybersecurity. 2016. Issue 2(2). P. 5–12. URL: http://periodicals.karazin.ua /cscs/issue/ viewIssue/ 454/517. (call date:

26.12.2016) (*Особистий внесок здобувача: запропоновані шляхи використання СЗК у криптосистемах)*.

70. Krasnobayev V., Koshman S., Yanko A. Method of tabular realization of arithmetic operations in the system of residual classes // Computer science and cybersecurity. 2016. Issue 3(3). P. 28–35. URL: http://periodicals.karazin.ua/cscs/issue/view/533. (call date: 26.12.2016). (*Особистий внесок здобувача: вдосконалення табличного методу реалізації арифметичних операцій)*.

71. Кошман С. А., Краснобаев В. А., Янко А. С. Усовершенствованный метод определения альтернативной совокупности чисел в системе остаточных классов // Радиотехника. Всеукраинский межведомственный научно-технический сборник. Харьков: ХНУРЭ. 2017. Вип. 189. С. 29-37. (*Особистий внесок здобувача: вдосконалено метод визначення альтернативної сукупності чисел у СЗК*).

Додаток Б

АКТИ ВПРОВАДЖЕННЯ НАУКОВИХ РЕЗУЛЬТАТІВ ДОКТОРСЬКОЇ ДИСЕРТАЦІЙНОЇ РОБОТИ

"ЗАТВЕРДЖУЮ"
Ректор
Харківського національного
технічного університету
імені Петра Василенка

_____ О. В. Нанка
"16" червня 2017 р.

"ЗАТВЕРДЖУЮ"
Виконавчий директор
приватного акціонерного
товариства
"Інститут інформаційних
технологій"

_____ В. Ю. Кравченко
"16" червня 2017 р.

АКТ

впровадження наукових результатів докторської дисертаційної роботи

КОШМАНА СЕРГІЯ ОЛЕКСАНДРОВИЧА

Комісія у складі голови – лауреата державної премії України, кандидата технічних наук, старшого наукового співробітника Горбенка Ю. І. і членів комісії кандидата технічних наук Бойка А. О. та кандидата технічних наук, професора Качко О. Г. склала цей акт про впровадження наукових результатів докторської дисертаційної роботи, що отримані доцентом кафедри автоматизації та комп'ютерно-інтегрованих технологій Харківського національного університету сільського господарства імені Петра Василенка кандидата технічних наук, доцента Кошмана С. О. у приватному акціонерному товаристві "Інститут інформаційних технологій". Комісія встановила наступне.

1. Фахівцями приватного акціонерного товариства "Інститут інформаційних технологій" впроваджено такі наукові результати докторської дисертаційної роботи Кошмана Сергія Олексадровича:

- методи контролю даних у системі залишкових класів (СЗК) на основі принципу нулевізації, шляхом застосування процедур послідовної та паралельної нулевізації, що підвищує оперативність контролю даних у СЗК;

- метод контролю даних у СЗК на основі застосуванні позиційної ознаки непозиційного коду, шляхом застосування процедури паралельного віднімання лишків за модулем СЗК, що підвищує оперативність контролю даних у СЗК;

- методи діагностування та корекції помилок даних у СЗК на основі застосування позиційної ознаки непозиційної кодової структури, шляхом підвищення інформативності альтернативної сукупності чисел, що підвищує оперативність діагностування та корекції помилок даних у СЗК.

2. Науково-практичні рекомендації, які сформульовані у дисертації та технічні засоби за патентами України на винахід № 108828, 110901, 110913 і 114063 було використано при створенні спеціалізованих комп'ютерних апаратних засобів швидкої обробки цілочисельних даних.

3. Отримані наукові результати докторської дисертаційної роботи є певним внеском у теорію та практику непозиційного кодування у системі залишкових класів. Впровадження наукових результатів докторської дисертації Кошмана С. О. дозволить фахівцям у галузі комп'ютерних систем і компонентів розробити методи та спеціалізовані апаратні засоби швидкої обробки цілочисельних даних.

Голова комісії:

Лауреат державної премії України,
кандидат технічних наук,
старший науковий співробітник Ю. І. Горбенко

Члени комісії:

кандидат технічних наук А. О. Бойко

кандидат технічних наук, професор О. Г. Качко

ЗАТВЕРДЖУЮ
Проректор з наукової роботи
Харківського національного
університету ім. В.Н. Каразіна

В.О. Катрич

“03” 12 2018 р.

АКТ

реалізації наукових досліджень доцента кафедри безпеки інформаційних систем і технологій Кошмана Сергія Олександровича при проведенні науково-дослідної роботи «Аналіз, дослідження, розробка та стандартизація криптографічних систем для захисту інформації в пост-квантовому середовищі, в умовах інформаційних і гібридних війн»

Комісія у складі: голови комісії – завідувача кафедри безпеки інформаційних систем і технологій доктора технічних наук, доцента Рассомахіна С.Г. та членів комісії – професора кафедри безпеки інформаційних систем і технологій доктора технічних наук, професора Кузнецова О.О., професора кафедри безпеки інформаційних систем і технологій доктора технічних наук, доцента Замули О.А. склала дійсний акт про те, що при обґрунтуванні концептуальних положень з розробки, аналізу та застосування різних сімейств квантово-стійких криптопримітивів для пост-квантового періоду реалізовано запропоновані Кошманом Сергієм Олександровичем такі наукові та практичні результати:

1. Метод контролю даних у системі залишкових класів, який на відміну від відомих, заснований на принципі паралельної нульовизації, шляхом поєднання у часі операцій нульовизації симетричних залишків непозиційної кодової структури, що контролюється і визначення констант нульовизації, що дозволяє підвищити оперативність контролю даних.
2. Метод контролю даних у системі залишкових класів, який на відміну від відомих, заснований на використанні позиційної ознаки непозиційної кодової структури, шляхом паралельного віднімання встановлених констант, що дозволяє підвищити оперативність контролю даних.
3. Метод підвищення достовірності оперативного контролю даних, що представлені у системі залишкових класів, який на відміну від відомих, заснований на використанні позиційної ознаки непозиційної кодової структури, шляхом застосування відповідної основи, що кратна загальному модулю системи залишкових класів, це підвищує достовірність контролю даних.

4. Метод визначення альтернативної сукупності непозиційної кодової структури у системі залишкових класів, який заснований на використанні функції відповідності значень можливих помилок, шляхом зменшення кількості основ, що перевіряються, які входять в альтернативну сукупність чисел, що підвищує оперативність діагностики помилок даних.
5. Метод оперативної діагностики даних, що представлені у системі залишкових класів, який заснований на формуванні числових інтервалів та ознак даних квадрантів знаходження альтернативних сукупностей чисел, шляхом згортки таблиці відповідності значень можливих помилок, це зменшує час вибірки основ, що перевіряються та підвищує оперативність діагностики помилок даних.

Застосування запропонованих методів оперативного контролю даних дозволяють на 25-60% (у порівнянні з існуючими методами) скоротити час, що підвищує оперативність процедури контролю.

Запропоновані методи оперативної діагностики даних дозволяють до 30% (у порівнянні з існуючими методами) скоротити час, що підвищує оперативність процедури діагностики.

Отримані наукові та практичні результати доцільно застосовувати при обґрунтуванні різних сімейств квантово-стійких криптопримітивів з метою оптимізації обчислень у системі залишкових класів для перспективних засобів криптографічного захисту, в тому числі для перехідного та пост-квантового періодів.

Голова комісії
Завідувач кафедри безпеки інформаційних систем і технологій
доктор технічних наук, доцент С. Г. Рассомахін

Члени комісії:
Професор кафедри безпеки інформаційних систем і технологій
доктор технічних наук, професор О. О. Кузнецов

Професор кафедри безпеки інформаційних систем і технологій
доктор технічних наук, доцент О. А. Замула

ЗАТВЕРДЖУЮ
Проректор з наукової роботи
Харківського національного
університету ім. В. Н. Каразіна
_____ В. О. Катрич
"___" _____ 2018 р.

АКТ

реалізації наукових досліджень доцента кафедри безпеки інформаційних систем і технологій Кошмана Сергія Олександровича при проведенні науково-дослідної роботи «Розробка математичних моделей та методів синтезу, формування та обробка сигнально-кодових конструкцій для захищений телекомунікаційних систем подвійного призначення»

Комісія у складі: голови комісії – завідувача кафедри безпеки інформаційних систем і технологій доктора технічних наук, доцента Рассомахіна С. Г. та членів комісії – професора кафедри безпеки інформаційних систем і технологій доктора технічних наук, професора Олійникова Р. В., професора кафедри безпеки інформаційних систем і технологій доктора технічних наук, доцента Замули О. А. склала дійсний акт про те, що при формуванні та обробці сигнально-кодових конструкцій для захищений телекомунікаційних систем подвійного призначення реалізовано запропоновані Кошманом Сергієм Олександровичем такі наукові та практичні результати:

1. Розроблено метод контролю даних у системі залишкових класів, що заснований на принципі паралельної нульовизації. Це підвищує оперативність контролю даних, в залежності від величини розрядної сітки на 25-60 %.
2. Розроблено метод контролю даних у системі залишкових класів, що заснований на використанні позиційної ознаки непозиційної кодової структури. Це дозволяє підвищити оперативність контролю даних до 60 %.
3. Розроблено метод підвищення достовірності оперативного контролю даних, що заснований на використанні позиційної ознаки непозиційної кодової структури. Використання цього методу забезпечує отримання достовірного результату контролю з точністю до одиниці довжини числового інтервалу.
4. Вдосконалено метод визначення альтернативної сукупності непозиційної кодової структури у системі залишкових класів. Це підвищує оперативність діагностики помилок даних до 30 %.
5. Вдосконалено метод оперативної діагностики даних, що представлені у системі залишкових класів. Це зменшує час вибірки основ, що

перевіряються та підвищує оперативність діагностики помилок даних від 6 до 19%.

Зазначені наукові та практичні результати доцільно застосовувати при побудові захищених телекомунікаційних систем подвійного призначення. Використання наукових результатів дозволить забезпечити необхідний рівень завадозахищеності та інформаційної безпеки телекомунікаційних систем.

Голова комісії
Завідувач кафедри безпеки інформаційних систем і технологій
доктор технічних наук, доцент С. Г. Рассомахін

Члени комісії:
Професор кафедри безпеки інформаційних систем і технологій
доктор технічних наук, доцент Р. В. Олійников

Професор кафедри безпеки інформаційних систем і технологій
доктор технічних наук, доцент О. А. Замула

ЗАТВЕРДЖУЮ
Проректор з наукової роботи
Харківського національного
університету ім. В.Н. Каразіна

В. О. Катрич

“22” червня 2018 р.

АКТ
використання результатів докторської дисертаційної роботи Кошмана Сергія Олександровича

Комісія у складі зав. кафедри безпеки інформаційних систем і технологій (БІСТ) Рассомахіна Сергія Генадійовича, професора кафедри БІСТ Замули Олександра Андрійовича та доцента кафедри БІСТ Малахова Сергія Віталійовича склала цей акт про використання наукових результатів докторської дисертації Кошмана С. О. у навчальному процесі.

При викладанні дисципліни "Математичні основи проектування та оптимізації інформаційно-комутаційних систем" використано такі наукові результати дисертаційної роботи:

1. Розроблено метод контролю даних у системі залишкових класів, що заснований на принципі паралельної нульовизації.
2. Розроблено метод контролю даних у системі залишкових класів, що заснований на використанні позиційної ознаки непозиційної кодової структури.
3. Розроблено метод підвищення достовірності оперативного контролю даних, що заснований на використанні позиційної ознаки непозиційної кодової структури.
4. Вдосконалено метод визначення альтернативної сукупності непозиційної кодової структури у системі залишкових класів.
5. Вдосконалено метод оперативної діагностики даних, що представлені у системі залишкових класів.

Зав. кафедри БІСТ, д.т.н., доцент. С. Г. Рассомахін

професор кафедри БІСТ д.т.н., доцент О. А. Замула

доцент кафедри БІСТ к.т.н., доцент С. В. Малахов

ЗАТВЕРДЖУЮ
Перший проректор
Харківського національного технічного
університету сільського господарства
імені Петра Василенка

д.т.н., проф. _____ М. Л. Лисиченко

"21" 02 2017 р.

АКТ

впровадження результатів докторської дисертації Кошмана Сергія Олександровича в навчальний процес і наукову роботу кафедри автоматизації та комп'ютерно-інтегрованих технологій ННІ ЕКТ Харківського національного технічного університету сільського господарства імені Петра Василенка.

Комісія у складі Мороза О. М. – директора ННІ ЕКТ, Піскарьова О. М. – завідувача кафедри автоматизації та комп'ютерно-інтегрованих технологій, Тимчука С. О. – професора кафедри автоматизації та комп'ютерно-інтегрованих технологій, склала цей акт про те, що матеріали дисертації Кошмана С. О. використовуються при викладанні дисципліни "Мікропроцесорні керуючі пристрої" для студентів, що навчаються за спеціальністю: 151 "Автоматизація та комп'ютерно-інтегровані технології".

Комісія встановила, що в навчальний процес впроваджені наступні науково-практичні результати.

1. Метод контролю даних у системі залишкових класів, який заснований на принципі паралельної нулевізації та дозволяє підвищити оперативність контролю даних.

2. Метод контролю даних у системі залишкових класів, який заснований на використанні позиційної ознаки непозиційної кодової структури та дозволяє підвищити оперативність контролю даних.

3. Метод підвищення достовірності оперативного контролю даних, що представлені у системі залишкових класів, який заснований на викори-

станні позиційної ознаки непозиційної кодової структури, та дозволяє підвищити достовірність контролю даних.

4. Метод визначення альтернативної сукупності непозиційної кодової структури у системі залишкових класів, який заснований на використанні функції відповідності значень можливих помилок та дозволяє підвищити оперативність діагностики та корекції помилок даних.

5. Метод оперативної діагностики даних, що представлені у системі залишкових класів, який заснований на використанні альтернативної сукупності непозиційних кодових структур та дозволяє підвищити оперативність діагностики помилок даних.

6. Метод виправлення помилок даних у системі залишкових класів, який заснований на паралельному визначенні помилок у непозиційній кодовій структурі та дозволяє підвищити оперативність виправлення помилок даних.

Голова комісії:

директор ННІ енергетики та
комп'ютерних технологій,
д.т.н., проф. О. М. Мороз

Члени комісії:

завідувач кафедри автоматизації та
комп'ютерно-інтегрованих технологій,
к.т.н. О. М. Піскарьов

професор кафедри автоматизації та
комп'ютерно-інтегрованих технологій,
д.т.н., доц. С. О. Тимчук