УДК 681.31

О.І. Волинський
Карпатський державний центр інформаційних засобів і технологій

МЕТОДИ МІЖБАЗИСНИХ ПЕРЕТВОРЕНЬ НА ОСНОВІ РОЗМЕЖОВАНОЇ СИСТЕМИ ЧИСЛЕННЯ ЗАЛИШКОВИХ КЛАСІВ

Викладено інформаційну технологію реалізації методу міжбазисних перетворень (Радемахера – Крестенсона) на основі розмежованої системи числення залишкових класів. Наведено схемотехнічні рішення базових модульних операцій представлення двійкових чисел у цілочисловій системі залишкових класів.

Information technology of realization of method is expounded between base transformations (Rademakhera – Krestensona) on the basis of the delimited scale of notation of remaining classes. The schematic-technical decisions of base module operations of presentation of binary numbers are resulted in the whole-numeral system of remaining classes.

Вступ. З розвитком сучасних технологій актуальною проблемою стає збільшення швидкодії опрацювання інформації. Для вирішення цієї задачі застосовують різні методи, одним із яких є застосування системи залишкових класів (СЗК).Зокрема, виконання операцій над великорозрядними числами, які використовуються для захисту інформаційних потоків, з використанням СЗК дасть змогу збільшити швидкодію.

Аналіз публікацій і окреслення наукової задачі. За даними наукової літератури, більшість сучасних досягненнь у галузі мікроелектроніки, мікропроцесорної техніки та розвитку фундаментальних досліджень в теорії та розробленні алгоритмів опрацювання інформаційних потоків зосереджені в теоретико-числовому базисі Радемахера [1, 2]. Проектування цифрових пристров у базисі Радемахера має певні недоліки – наявність міжрозрядних зв'язків, велика розрядність адресних шин, масштабність реалізації зовнішніх зв'язків на ПЛІС, значне енергоспоживання [3, 4].

Розглянувши СЗК, видно, що залишки, які утворюються в результаті модульної операції, мають малу кількість розрядів, що відкриває можливість побудови табличної арифметики на основі однотактних операцій, які виконуються простою вибіркою із таблиці [5]. Не менш важливою ознакою цієї системи є незалежність утворення розрядів числа, в результаті чого кожний розряд несе інформацію про вихідне, а не про проміжне число. Ці переваги дають змогу розпаралелити обчислення і спростити виконання арифметичних операцій.

Запропонований у [6] алгоритм перетворення чисел базису Радемахера на СЗК на основі теорії розмежованої СЗК дає змогу поглибити процес розпаралелювання та спрощення арифметичних операцій базису Крестенсона. Водночас виконання процедури розмежування на N розрядів:

$$N = 2^i \cdot n,$$

де N – число розрядів процесора; 2^i – коефіцієнт розмежування,
приводить, як це показано у [6], до спрощення складних дешифраторів, а також передбачає наскрізні перенесення в РСЗК. Реалізація побітного розмежування чисел у базисі Радемахера значно спрощує алгоритм переходу з базису Радемахера в базис Крестенсона. Тому перспективним напрямком підвищення швидкодії алгоритмів міжбазисного перетворення є застосування принципу розмежування.

Мета роботи. Метою роботи є розроблення теоретичних засад та реалізація міжбазисного перетворення Радемахера – Крестенсона, а також аналіз об'єму та швидкодії мікроелектронного обладнання розроблених методів у результаті досліджень.

Теоретичні основи систем числення у базисі Крестенсона.Теоретичні основи перетворення базису Крестенсона, яке реалізовується у вигляді різних форм СЗК, викладено в роботах [2, 3].

У табл. 1 наведено аналітичні вирази прямих та зворотних перетворень таких форм СЗК: цілочислова (1), нормалізована (2), досконала (3), розмежована (4).

Таблиця 1

Аналітичні вирази прямих та зворотних перетворень форм СЗК

№ з/п	Пряме перетворення форми СЗК
1.	$N_k = (b_1 b_2 ... b_i ... b_k)_{(p_1 p_2 ... p_i ... p_k)}$ $N_k = b_i (\mathrm{mod}\, p_i)$, $N_k = a_i p_i + b_i$, $P = \prod_{i=1}^{k} p_i$; $0 \le N_k \le P$.
2.	$\frac{N_k}{P} = res \sum_{i=1}^{k} \frac{b_i \cdot B_i (\mathrm{mod} P)}{P}$, $[N_k]_0 = res \sum_{i=1}^{k} b_i \cdot \frac{B_i}{P} (\mathrm{mod}\, 1)$, $0 \le [N_k]_0 \le P - 1$; $\frac{B_i}{P} = \frac{1}{p_i}$, $d_p \le \frac{1}{P}, \frac{1}{p_i} = 0.ggggggg$, **678 678** ^{d}
3.	$[N_k]_0 = res \sum_{i=1}^{k} [b_i]_0 (\mathrm{mod}\, 1)$.
4.	$N_k = N_{1k} + N_{2k} + ... + N_{ik} + ... + N_{nk}$,
	Зворотнє перетворення форми СЗК
1.	$b_i = res N_k (\mathrm{mod}\, p_i)$ $N_k = res \sum_{i=1}^{k} b_i \cdot B_i (\mathrm{mod}\ P)$, $B_i = \frac{P}{p_i} \cdot m_i \equiv 1 (\mathrm{mod}\ \ P_i)$ ·
2.	$[N_k]_0 = res \sum_{i=1}^{k} b_i \cdot \frac{m_i}{p_i} (\mathrm{mod}\, 1)$ $[N_k]_0 = res \sum_{i=1}^{k} [b_i]_0 \cdot m_i (\mathrm{mod} 1)$, $[b_i]_0 = \frac{b_i}{p_i}$, $0 \le [b_i]_0 \le 1$. $N_k = \mathrm{int}[N_k]_0 \cdot P$,
3.	$b_i = \mathrm{int}\, res [N_k]_0 (\mathrm{mod} 1) \cdot P_i$
4.	N_k → $b_1=(b_{11}+ b_{21}+...+ b_{r1}+...+ b_{n1}) \mathrm{mod} p_1$ $b_2=(b_{12}+ b_{22}+...+ b_{r2}+...+ b_{n2}) \mathrm{mod} p_2$ ... $b_i=(b_{1i}+ b_{2i}+...+ b_{ri}+...+ b_{ni})$ ... b_k $b_2=(b_{1k}+ b_{2k}+...+ b_{rk}+...+ b_{nk})$

Необхідно зауважити, що досконала та розмежована форми СЗК є особливо перспективними для створення високопродуктивних мультибазисних процесорів [6, 8].

Інформаційна база розмежованої СЗК. Теоретичною основою РСЗК є цілочислова форма СЗК, рівняння якої подано у вигляді суми:

$$N_k = N_{1k} + N_{2k} + \ldots + N_{ik} + \ldots + N_{nk},$$

де N_{ik} – m- розрядний (розмежований) фрагмент числа N_k, яке представлене у двійковій системі числення, числового базису Радемахера. Наприклад, 32-розрядний процесор СЗК може бути розмежований на чотири фрагменти по 8 бітів (рис. 1).

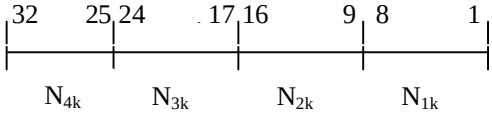

Рис. 1. Процес розмежування 32-розрядного процесора

Отже, пряме перетворення РСЗК матиме вигляд, зображений на рис. 2.

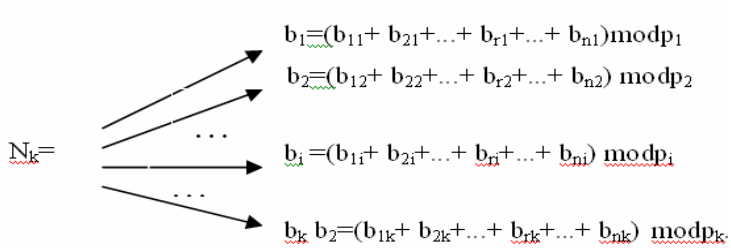

Рис. 2. Пряме перетворення РСЗК

При цьому математичні операції над числами в РСЗК можуть бути розмежовані по кожному із фрагментів процесора, що забезпечує ще глибший рівень розпаралелювання обробки інформації, а відповідно, підвищення швидкодії процесора СЗК.

Отже, у загальному вигляді зворотне перетворення РСЗК аналітично описується виразом:

$$N_k = res \sum_{r=1}^{n} \sum_{i=1}^{k} res(b_{1i} + b_{2i} + \ldots + b_{ri} + \ldots + b_{ni}) \bmod P_i \cdot B_i \bmod P.$$

Застосування міжбазисного перетворення за такого розмежування базису Радемахера дає змогу схемотехнічно реалізувати міжбазисне перетворення на основі дешифратора за відповідним модулем.

Наприклад, на низових рівнях РСЗК широко використовуються 16-бітні та 24-бітні сигнальні процесори. Ці процесори виконують понад 90 % базових операцій додавання, множення та порівняння чисел із використанням процедур цифрової згортки, фільтрації, цифрової томографії та інше.

Тому можливості реалізації швидкодіючого процесора у досліджуваній системі числення доцільно розглядати на основі 16-бітного процесора.

Діапазон кодування чисел РСЗК розраховують за виразом [6]:

$$P = \prod_{i=1}^{k} p_i, \text{ де } 0 \le N_k \le P - 1,$$

де N_k – двійковий код числа, p_i – система взаємопростих модулів, а розрядність процесора

$$n_k = [\log_2 (P - 1)].$$

Із структури розмежованого процесора зрозуміло, що вона потребує обчислення залишків для кожного компонента за виразом:

$$b_{ij} = resN_{ij} (\bmod p_i).$$

При цьому процедуру обчислення загального залишку виконують за виразом:

$$b_i = res(b_{i1} + b_{i2} + \ldots + b_{in}) \bmod p_i.$$

При 4-бітній розрядності компонентів 16-бітного процесора оптимальний набір модулів з максимальним діапазоном кодування задається масивом чисел:

$$p_i=(3\ ,5\ ,7\ ,8\ ,11\ ,13),$$

що відповідає діапазону кодування:

$$P=120.120,$$

що достатньо для реалізації швидкодіючого 16-бітного процесора в РСЗК. Істотною перевагою РСЗК є значне спрощення алгоритму переведення чисел з базису Крестенсона в базис Галуа, що схемотехнічно реалізується за допомогою матричних дешифраторів. На рис. 3 наведено приклад реалізації дешифратора 4-бітних компонентів 16-бітного процесора залишкових класів за модулем 5.

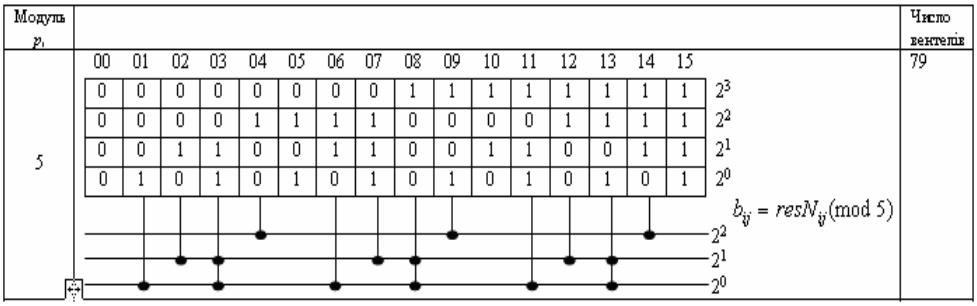

Рис. 3. Приклад схеми обчислення залишку за модулем 5

На рис. 4 зображено принципову схему обчислення залишку за модулем P=5.

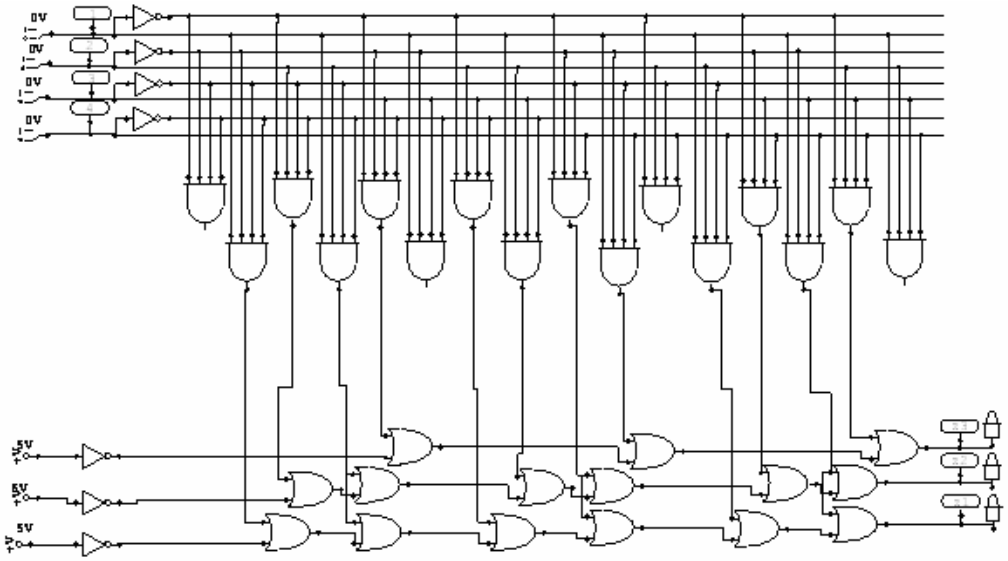

Рис. 4. Дешифратор за модулем P=5

Незважаючи на можливості міжбазисного перетворення Радемахера – Крестонсона на основі дешифратора при ступені розмежування двійкових чисел на N – розрядів ($N=2^k$, k=2, 4,…) таке розмежування характеризується недоліком, оскільки при виконанні арифметичних операцій в РСЗК необхідно реалізувати наскрізні перенесення між N – розрядними групами бітів базису Радемахера.

Бінарно-розмежована СЗК. При бінарному розмежуванні двійкових чисел базису Радемахера, тобто k=0, структура розмежування має такий вигляд:

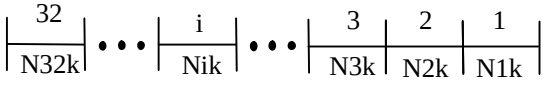

Рис. 5. Процес бінарного розмежування 32-розрядного процесора

У результаті такого розмежування двійкового числа (X_{n-1}, X_{n-2}, …,X_i ,… ,X_1 ,X_0) формується матриця залишків кожного і-го розряду у системі взаємопростих модулів P_1, P_2, ... P_j, ... P_k (табл. 2) [9].

Таблиця 2

Матриця залишків числа X

	X_{n-1}	X_{n-2}	…	X_i	…	X_1	X_0
P_1	$b_{n-1,1}$	$b_{n-2,1}$	…	$b_{i,1}$	…	$b_{1,1}$	$b_{0,1}$
P_2	$b_{n-1,2}$	$b_{n-2,2}$	…	$b_{i,2}$	…	$b_{1,2}$	$b_{0,2}$
P_3	$b_{n-1,3}$	$b_{n-2,3}$	…	$b_{i,3}$	…	$b_{1,3}$	$b_{0,3}$
P_4	$b_{n-1,4}$	$b_{n-2,4}$	…	$b_{i,4}$	…	$b_{1,4}$	$b_{0,4}$
…	…	…	…	…	…	…	…
P_j	$b_{n-1,j}$	$b_{n-2,j}$	…	$b_{i,j}$	…	$b_{1,j}$	$b_{0,j}$
…	…	…	…	…	…	…	…
P_k	$b_{n-1,k}$	$b_{n-2,k}$	…	$b_{i,k}$	…	$b_{1,k}$	$b_{0,k}$

Для переходу в базис Крестенсона над елементами стрічок матриці, поданої у табл. 1, виконується така операція:

$$res(b_{n-1,j} + b_{n-2,j} + ... + b_{i,j} + ... + b_{1,j} + b_{0,j}) \bmod P_i . \quad (1)$$

Для підвищення швидкості модульної операції (1) доцільно застосувати пірамідальний алгоритм сумування згідно з рис. 6.

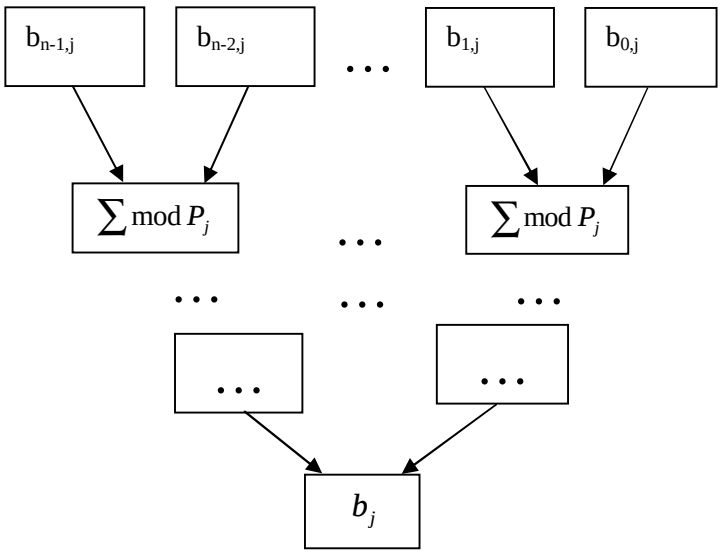

Рис. 6. Пірамідальний алгоритм сумування залишків у РСЗК

Швидкодію такого пірамідально-модульного суматора розраховують за формулою:

$$m = \log_2 n^i ,$$

де n – розрядність процесора базису Радемахера.

Висока швидкодія такого компонента міжбазисного перетворення Радемахера – Крестенсона потребує великої кількості суматорів залежно від розрядності процесора, число яких розраховується за формулою:

$$S = n + n/2 + n/4 + ... + n/n .$$

Отже, загальний об’єм даного міжбазисного перетворення можна оцінити за виразом

$$Q = K \cdot S,$$

де K – число взаємопростих модулів базису Крестенсона.

Об'єм мікроелектронного обладнання, міжбазисного перетворювача (МБП) можна значно зменшити на основі інформаційної технології та структури, показаної на рис. 7.

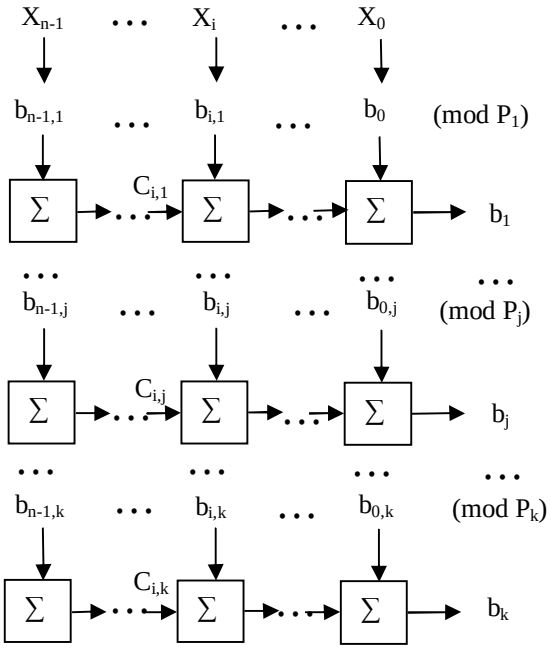

Рис. 7. Структура міжбазисного перетворювача Радемахер–Крестенсон

Характеристика об'єму та швидкодії мікроелектронного обладнання суматора за модулем Pj. За архітектурою пірамідального та лінійного міжбазисних перетворень за модулем P_j, показаних архітектур на рис.7 та 6, порівняння їх характеристик наведено на рис. 8, звідки видно, що лінійна архітектура потребує удвічі менше обладнання відносно пірамідальної.

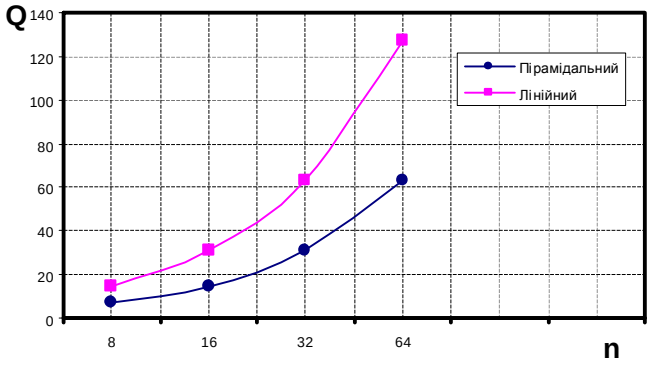

Рис. 8. Об'єм мікроелектронного обладнання міжбазисного перетворення Радемахера – Крестенсона

Результати аналізу швидкодії двох досліджуваних архітектур міжбазисного перетворення при унітарному кодуванні залишків (рис. 9) розраховується за виразами:

$$V_p = \frac{1}{2 + \log_2 n}; \; V_l = \frac{1}{n};$$

де n – число розрядів процесора; V_p – швидкодія пірамідального МБП; V_l – швидкодія лінійного МБП.

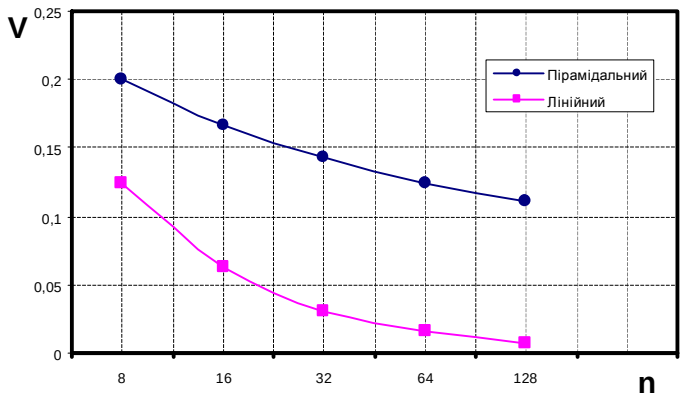

Рис. 9. Швидкодія міжбазисного перетворення Радемахера – Крестенсона

Висновки. Результати досліджень доводять, що у бінарно розмежованій СЗК підвищуються ефективність і реалізація міжбазисного перетворення Радемахера – Крестенсона за схемотехнічними варіантами на основі пірамідально та лінійно з'єднаних суматорів за модулем P, причому об'єм обладнання пірамідальної структури удвічі перевищує об'єм лінійної структури за заданої розрядності процесора. Швидкодія пірамідального МБП зростає із збільшенням розрядності процесора (8 – 128) відповідно у діапазоні (1,6 – 13,8) разів. Розроблений метод міжбазисних перетворень може широко використовуватися для створення спецпроцесорів опрацювання великорозрядних чисел та задач захисту мереж від несанкціонованого доступу, а також інших фундаментальних задач теорії чисел, зокрема задачі знаходження найбільших дільників двох великорозрядних чисел, пошуку простих чисел великої розрядності.

1. Майоров С.А., Новиков Г. И. Принципы организации цифровых машин. – Л.: Машиностроение, 1974. – 432 с. 2. Таненбаум Э. Архитектура комп'ютера, 4-е вид. – Спб.: Пітер, 2003. – 700 с. 2. Богданов А.В., Корхов В.В., Мареев В.В., Станкова Е.Н. Архитектуры и топологии многопроцессорных вычислительных систем. 3. Коуги П.М. Архитектура конвейерных ЭВМ: Пер. с англ. – М.: Радио и связь, 1985. – 360 с. 4. Балашов Е.П. и др. Высокопроизводительные специализированные процессоры для вычисления элементарных функций // Электронное моделирование. – 1983. – № 4. – С. 61–65. 5. Акушський И.Я., Юдицкий Д.И. "Машынная арифметика в остаточных класах". – М.: Сов. радио, 1968. – 440 с. 6. Николайчук Я.М., Волинський О.І., Кулина С.В. Теоретичні основи побудови спецпроцесорів у базисі Крестенсона // Вісник Хмельницького нац. ун-ту. – 2007. – № 3. Т.1(93). – С.85–90. 7. Николайчук Я.М., Федорович Ю.С. Теоретичні основи базисних перетворень СЗК // Матеріали наук. конф. "Автоматика 2000". – Львів, 2000. – 120 с. 8. Николайчук Я.М., Волинський О.І., Кулина С.В. Швидкодіючий алгоритм та процесор порівняння чисел у системі залишкових класів базису Крестенсона // Искусственный интеллект. ІПШІ МОН і НАН України "Наука і освіта". – 2008. – №3. – С. 348–352. 9. Волинський О.І. Методи порівняння та сумування в розмежованій системі числення. Поступ в науку: Збірник праць Бучацького інституту менеджменту і аудиту. – Бучач, 2009. – №4. Т1. – С. 91–94.

УДК 681.325

Н.Я. Возна
Карпатський державний центр інформаційних засобів та технологій

ТЕОРІЯ ТА МЕТОДИ ПОБУДОВИ МОДЕЛЕЙ РУХУ ДАНИХ У РОЗПОДІЛЕНИХ КС

Наведено результати теоретичних та експериментальних досліджень методів формування та організації потоків даних у розподілених комп'ютерних системах.

In this work the results of theoretical and experimental researches of methods of forming and organization of data flows in distributed computing systems.

Вступ. Аналіз світових тенденцій розвитку розподілених комп'ютерних систем показує, що їхні системні функції все більше охоплюють не тільки задачі формування та управління потоками даних, але й задачі штучного інтелекту, прийняття рішень, створення баз знань та ін. Інтенсивний розвиток комп'ютерної техніки, засобів програмування та телекомунікаційних систем дає змогу сьогодні максимально автоматизувати процеси формування, перетворення, передавання, цифрової обробки, архівізації та використання даних у РКС. Зростання об'ємів потоків інформаційних даних на сучасних виробництвах не зменшує актуальності класичних задач оптимізації методів формування інформаційних моделей шляхом ефективного кодування даних, зменшення їх надлишковості, захисту від помилок та несанкціонованого доступу, а також підвищення ефективності методологій і технічних засобів введення, відображення та їх цифрової обробки.

Одним з недоліків сучасних комп'ютеризованих систем є просторова та часова роздільність інформаційних потоків технолого-економічних та собівартісних даних, а також практична відсутність інформаційної технології побудови багаторівневих моделей руху даних комп'ютеризованих систем.

Тому задача підвищення ефективності та оптимізації параметрів методів формування, перетворення та організації руху структуризованих даних є актуальною.

Аналіз публікацій та окреслення проблеми. Сьогодні високорозвинені країни світу перебувають у стадії переходу до постіндустріальної фази свого розвитку – інформаційного суспільства, основою якого стане глобальна інформаційна інфраструктура. При цьому спостерігається стрімкий розвиток та вдосконалення інформаційних технологій збирання, формування, передавання, опрацювання, перетворення, захисту та зберігання інформаційних даних [1].

Успішному вирішенню цієї проблеми сприятиме досвід розроблення та застосування розподілених комп'ютерних систем [2]. Розподілені комп'ютеризовані системи передбачають формування та оброблення інтенсивних потоків інформаційних даних у реальному масштабі часу. До складу таких даних входять техніко-економічні показники (ТЕП), діагностичні, технологічні та технолого-економічні дані, а також моделі джерел інформації, фрейми та моделі руху даних (МРД), які становлять основу розподіленого руху потоків даних, що описуються мережами Петрі та матричними моделями (ММ) [3,4]. Значний внесок у розвиток технології моделювання руху даних в КС зробив Дж. Мартін [5], який ввів одиницю руху даних ke=Ni/Nj , де Ni, Nj – відповідно число читань та запитів даних в активних вузлах КС.

Водночас велика складність процесів проектування та аналізу розподілених КС, а також абстрактність теорії мереж Петрі не дають змоги ефективно використати сучасні потужні комп'ютерні засоби через недостатній рівень формалізації сукупності моделей руху даних в КС, які з необхідною диференціацією векторно відображають характеристики взаємодії та руху інформаційних потоків у розподілених КС.