

## АЛГОРИТМИ ОПРАЦЮВАННЯ ІНФОРМАЦІЙНИХ ПОТОКІВ В КОМП'ЮТЕРНИХ СИСТЕМАХ

І.З. Якименко<sup>1</sup>, М.М. Касянчук<sup>1</sup>, Л.М. Тимошенко<sup>2</sup>, Н.Є. Гребень<sup>2</sup>

<sup>1</sup> Тернопільський національний економічний університет,  
вул. Львівська, 11, Тернопіль, 46029, Україна; e-mail: iyakymenko@mail.ru

<sup>2</sup> Одеський національний політехнічний університет,  
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: nata-sti4@mail.ru

Обґрунтовується використання теоретико-числового базису Крестенсона, що породжує систему числення залишкових класів, для реалізації алгоритмів опрацювання інформаційних потоків. Розроблені нові алгоритми модулярного множення в теоретико-числовому базисі Радемахера-Крестенсона, що дозволили зменшити складність з поліноміально-експоненційної до логарифмічної, що на один-два порядки збільшило швидкодію рішення задач даного класу. Наведені результати чисельних експериментів відповідають теоретично розрахованим параметрам і підтверджують правильність запропонованого наукового підходу.

**Ключові слова:** інформаційні потоки, теоретико-числовий базис Радемахера-Крестенсона, система залишкових класів, матрично-модулярне множення

### Вступ

Способи кодування інформаційних потоків визначаються теоретико-числовими базисами (ТЧБ), які застосовуються для їх представлення [1–3], найбільш поширеними з яких в сучасних комп'ютерних системах (КС) є наступні: унітарний, Хаара, Грея, Радемахера, Крестенсона та Галуа.

Світовий досвід створення процесорів для КС за останні 50 років, поряд з застосуванням ТЧБ Радемахера, який породжує двійкову систему числення, демонструє тенденцію все ширшого застосування інших ТЧБ, в тому числі: унітарного, Хаара, Крестенсона, Галуа, та сумісного використання комбінацій названих ТЧБ, наприклад Радемахера-Хаара, Крестенсона-Галуа тощо [4].

У зв'язку з цим існує проблема глибокого дослідження характеристик «нерадемахівських» ТЧБ та граничних можливостей їх застосування. При цьому перспективним, крім найбільш сьогодні масового одновимірного (векторного) представлення чисел та виконання операцій у ТЧБ Радемахера, є застосування двовимірних систем числення, вертикальної інформаційної технології у базисі Галуа та різних форм багатовимірного представлення чисел у вигляді залишків різних форм системи залишкових класів ТЧБ Крестенсона [5, 6].

Система числення залишкових класів (СЗК) ТЧБ Крестенсона, розроблена Акушським І.Я. та Юдіцьким Д.І., особливо її цілочисельна форма, широко використовувалась, починаючи з 70-х років минулого століття для побудови швидкодіючих спеціалізованих процесорів систем повітряної оборони колишнього СРСР [7]. Нормалізована форма СЗК, запропонована науковою школою професора Николайчука Я.М., активно використовується та застосовується при дослідженні двовимірних (матричних) форм систем числення ТЧБ Радемахера та Галуа [8].

## Мета та задачі дослідження

Досягнення необхідного рівня захисту інформації в КС, які розвиваються, обґрунтовує перспективу удосконалення алгоритмів формування та опрацювання інформаційних потоків. Для досягнення мети удосконалення та підвищення ефективності захисту інформаційних потоків необхідно вирішити ряд задач:

- дослідити теоретичні засади опрацювання інформаційних потоків;
- розробити швидкодіючі алгоритми опрацювання інформаційних потоків на основі різних ТЧБ;
- створити спеціалізовані програмні засоби опрацювання інформаційних потоків.

## Теоретичні засади використання системи залишкових класів

Відомо, що двійкова система числення, яка використовується в сучасних комп'ютерних системах, має певні недоліки – наявність міжрозрядних зв'язків та велику розрядність [9]. Тому актуальним є розвиток і застосування непозиційних систем числення, в яких відсутні вказані недоліки. Прикладом може бути СЗК, або, як її ще називають, представлення чисел у базисі Крестенсона [10], [11], причому найбільш фундаментально досліджено цілочисельну форму в системі залишкових класів. Хоча вона не набула значного поширення у зв'язку з необхідністю визначення умов переповнення, складністю та громіздкістю зворотнього перетворення чисел у десяткову систему числення, а також складнощами реалізації операцій ділення та порівняння, але СЗК можна ефективно використовувати у мультибазисних процесорах, спеціалізованих обчислювальних машинах для виконання операцій додавання, віднімання та множення, наприклад, у задачах лінійної алгебри (матрично-векторні операції) тощо. Необхідно відмітити, що ця система особливо ефективна при обчисленнях з великими числами [12], [13].

Фундаментальною основою СЗК є теорія чисел [14], зокрема, властивості китайської теореми про залишки. Будь-яке ціле додатне число  $N$  у десятковій системі числення представляється в СЗК у вигляді набору найменших додатніх залишків від ділення цього числа на фіксовані цілі додатні попарно взаємно прості числа  $p_1, p_2, \dots, p_n$  ( $N_{10} = (b_1, b_2, \dots, b_n)_{p_1, p_2, \dots, p_n}$ , де  $b_i = N \bmod p_i$ ), які називаються модулями ( $n$  — кількість модулів). При цьому повинна виконуватись умова  $0 \leq N \leq P-1$ , де

$$P = \prod_{i=1}^n p_i.$$

На відміну від позиційних систем числення, де величина визначеного розряду суми, різниці або множення залежить не тільки від значень відповідних, але і від попередніх розрядів доданків або множників, в СЗК додавання, віднімання та множення цілих чисел виконується окремо по кожному модулю і переноси між розрядами відсутні. Отже, такі операції в СЗК є модульними [15].

Нехай два десяткові числа  $A$  і  $B$ , записані в СЗК за вибраними модулями:

$$A_{10} = (a_1, a_2, \dots, a_i, \dots, a_n)_{p_1, p_2, \dots, p_i, \dots, p_n},$$

$$B_{10} = (b_1, b_2, \dots, b_i, \dots, b_n)_{p_1, p_2, \dots, p_i, \dots, p_n}.$$

Тоді:

$$A_{10} \pm B_{10} = C_{10} = (c_1, c_2, \dots, c_i, \dots, c_n)_{p_1, p_2, \dots, p_i, \dots, p_n},$$

$$A_{10} \times B_{10} = D_{10} = (d_1, d_2, \dots, d_i, \dots, d_n)_{p_1, p_2, \dots, p_i, \dots, p_n}$$

де

$$c_i = a_i \pm b_i,$$

$$d_i = a_i \times b_i.$$

Останні рівності справедливі лише в тому випадку, коли результат операції не виходить за межі інтервалу  $\prod_{i=1}^n p_i - 1$ .

Зворотне перетворення із ТЧБ Крестенсона у десяткову систему числення є досить громіздким і ґрунтується на використанні китайської теореми про залишки [14]:

$$N = \left( \sum_{i=1}^n b_i B_i \right) \bmod P, \quad (1)$$

де  $B_i = M_i m_i$ ,  $M_i = \frac{P}{p_i}$ ,  $m_i$  шукається з виразу  $(M_i m_i) \bmod p_i = 1$ , при цьому повинна

виконуватись умова  $\left( \sum_{i=1}^n B_i \right) \bmod P = 1$ .

Слід зазначити, що при переведенні чисел із СЗК у десяткову систему числення значну обчислювальну складність становить пошук коефіцієнтів  $m_i = M_i^{-1} \bmod p_i$ . У роботі [8] розглянуто досконалу форму СЗК (ДФ СЗК), у якій підбір модулів такий, що  $m_i = 1$ , тобто

$$M_i \bmod p_i = 1. \quad (2)$$

Подальший розвиток ДФ СЗК отримала у роботах [16, 17], у яких було встановлено правила побудови наборів з будь-якої кількості модулів ДФ СЗК для будь-якого діапазону десяткових чисел. Шукані модулі повинні отримуватися з такої умови:

$$\begin{cases} p_1 = 2 \\ p_i = p_1 p_2 \dots p_{i-1} + 1, 1 < i < n. \\ p_n = p_1 p_2 \dots p_{n-1} - 1. \end{cases} \quad (3)$$

Слід зазначити, що запропонована система не вичерпує всіх можливих наборів для ТЧБ Крестенсона при заданих  $n$ . Набір модулів, отриманий за допомогою системи (3), найоптимальніший, оскільки в цьому випадку величина  $P$  є максимальна, що дозволяє розглядати найбільший діапазон десяткових чисел. При цьому досягається зменшення розрядності вдвічі.

Крім того, у цих роботах запропонована напівдосконала форма СЗК ( $m_i = \pm 1$ ), яку зручно використовувати у випадку обмеженої кількості модулів та необхідності розгляду великих чисел. Перспективними модифікаціями СЗК, які на даний час досліджуються, є нормалізована та розмежована форми СЗК.

Отже, переваги представлення чисел у базисі Крестенсона для опрацювання інформаційних потоків в КС очевидні – виконання операцій над великорозрядними числами, які представляються залишками, а не над великими числами базису Радемахера.

## Алгоритм модулярного множення у ТЧБ Радемахера–Крестенсона

У роботі [18] викладені теоретичні основи виконання операцій модулярного множення та експоненціювання при застосуванні теоретико-числових базисів Радемахера та Крестенсона та отримано аналітичні вирази обчислювальної складності запропонованих високопродуктивних алгоритмів.

Запропоновано алгоритм матрично-модулярного множення  $n$ -розрядних чисел  $a = a_{n-1}2^{n-1} + \dots + a_i2^i + \dots + a_12 + a_0$  та  $b = b_{n-1}2^{n-1} + \dots + b_j2^j + \dots + b_12 + b_0$ , де  $a_i, b_j = 0, 1$ ,  $n$  — розрядність модуля  $p$ . Після побудови матриці  $\|c_{ij}\| = 2^{i+j} \bmod p$  добуток чисел  $a$  та  $b$  отримується згідно формули:

$$a \cdot b = \left( \sum_{i=1}^{n-1} \sum_{j=1}^{n-1} a_i b_j 2^{i+j} \right) \bmod p, \quad (4)$$

де  $a_i, b_j = 1$ , тобто  $c_{ij}$  знаходиться на перетині стовпця та рядка, для яких відповідні  $a_i$  та  $b_j$  дорівнюють 1.

Модулярне множення в ТЧБ Радемахера–Крестенсона здійснюється згідно наступного алгоритму.

**Вхід:**  $a = a_{n-1}2^{n-1} + \dots + a_i2^i + \dots + a_12 + a_0$ ,  $b = b_{n-1}2^{n-1} + \dots + b_j2^j + \dots + b_12 + b_0$ ,  $a_i, b_j = 0, 1$ ,  $n$  — розрядність модуля  $p$ .

1) Знаходимо залишки кожного біта  $a$  і  $b$  по заданому модулю  $p$ .

2) Сумуємо залишки останньої стрічки матриці розкладу чисел  $a$  і  $b$  по модулю  $p$ .

Отримуємо  $c_n$ .

3) Помножуючи  $c_n \cdot 2$  за модулем  $p$  і пропускаючи нульові стрічки, записуємо вектор стовпчик  $c_i$ . Отримуємо вектор залишків  $a \cdot b \pmod{p}$ .

**Вихід:**  $c_i$ .

Блок-схема алгоритму представлена на рис. 1. Отриманий алгоритм заміни операції множення, яка має квадратичну обчислювальну складність  $O_1(n) = n^2$ , матрично-модульною операцією сумування в ТЧБ Радемахера–Крестенсона з логарифмічною складністю

$$O_2(n) = \begin{cases} (\log_2 n)^2, & \text{якщо } n < 256 \\ n \cdot (\log_2 n), & \text{в інших випадках} \end{cases}$$

Основна перевага розробленого алгоритму по відношенню до існуючих – заміна багатотактної операції множення на однокітну сумування залишків. Алгоритм дозволяє реалізувати матриці розрядності 1024 біти за 2-4 мс, що при тактовій частоті процесора  $10^9$  прискорює реалізацію алгоритму в 20-40 разів.

## Удосконалений алгоритм модулярного множення на основі використання ТЧБ Радемахера–Крестенсона

Для виконання операції модулярного множення  $a \cdot b \pmod{p}$  двох  $n$ -розрядних чисел, представимо числа  $a$  та  $b$  в двійковій системі числення базису Радемахера, тобто:

$$a = \sum_{i=1}^{n-1} a_i 2^i = a_0 2^0 + a_1 2^1 + a_2 2^2 + \dots + a_{n-1} 2^{n-1},$$

$$b = \sum_{j=1}^{n-1} b_j 2^j = b_0 2^0 + b_1 2^1 + b_2 2^2 + \dots + b_{n-1} 2^{n-1},$$

де

$$a_i = 0.1;$$

$$b_j = 0.1;$$

$n$  — розрядність модуля  $p$ .

Для знаходження результату їх множення за модулем  $p$  побудуємо матрицю, представлену в табл. 1, де  $k_j = 2^j \bmod p$ .

**Таблиця 1.**

Матриця множення в ТЧБ Радемахера–Крестенсона

|           |           |       |           |       |           |           |       |       |       |
|-----------|-----------|-------|-----------|-------|-----------|-----------|-------|-------|-------|
|           | $k_{n-1}$ |       | $k_1$     | $k_0$ | .....     | $k_{n-1}$ |       | $k_1$ | $k_0$ |
| $a_{n-1}$ | $b_{n-1}$ |       | $b_1$     | $b_0$ | 0         | 0         | 0     | 0     | 0     |
| ...       | 0         | ..... | .....     | ..... | .....     | 0         | 0     | 0     | 0     |
| $a_i$     | 0         | 0     | $b_{n-1}$ |       | $b_1$     | $b_0$     | 0     | 0     | 0     |
| ...       | 0         | 0     | 0         | ..... | .....     | .....     | ..... | 0     | 0     |
| $a_1$     | 0         | 0     | 0         | 0     | $b_{n-1}$ |           | $b_1$ | $b_0$ | 0     |
| $a_0$     | 0         | 0     | 0         | 0     | 0         | $b_{n-1}$ |       | $b_1$ | $b_0$ |

$$a \cdot b(\bmod p) = a_0 b_0 k_0 + (a_0 b_1 + a_1 b_0) k_1 + (a_0 b_2 + a_1 b_1 + a_2 b_0) k_2 + \dots + (a_0 b_{n-1} + a_1 b_{n-2} + \dots + a_{n-1} b_0) k_i \tag{6}$$

Позначимо через:

$$A_l = (a_0 b_{n-1} + a_1 b_{n-2} + \dots + a_{n-1} b_0) k_l, \tag{7}$$

$$a \cdot b(\bmod p) = \sum_{l=1}^{2n} A_l \bmod p. \tag{8}$$

З врахуванням (7) співвідношення (8) набуде вигляду:

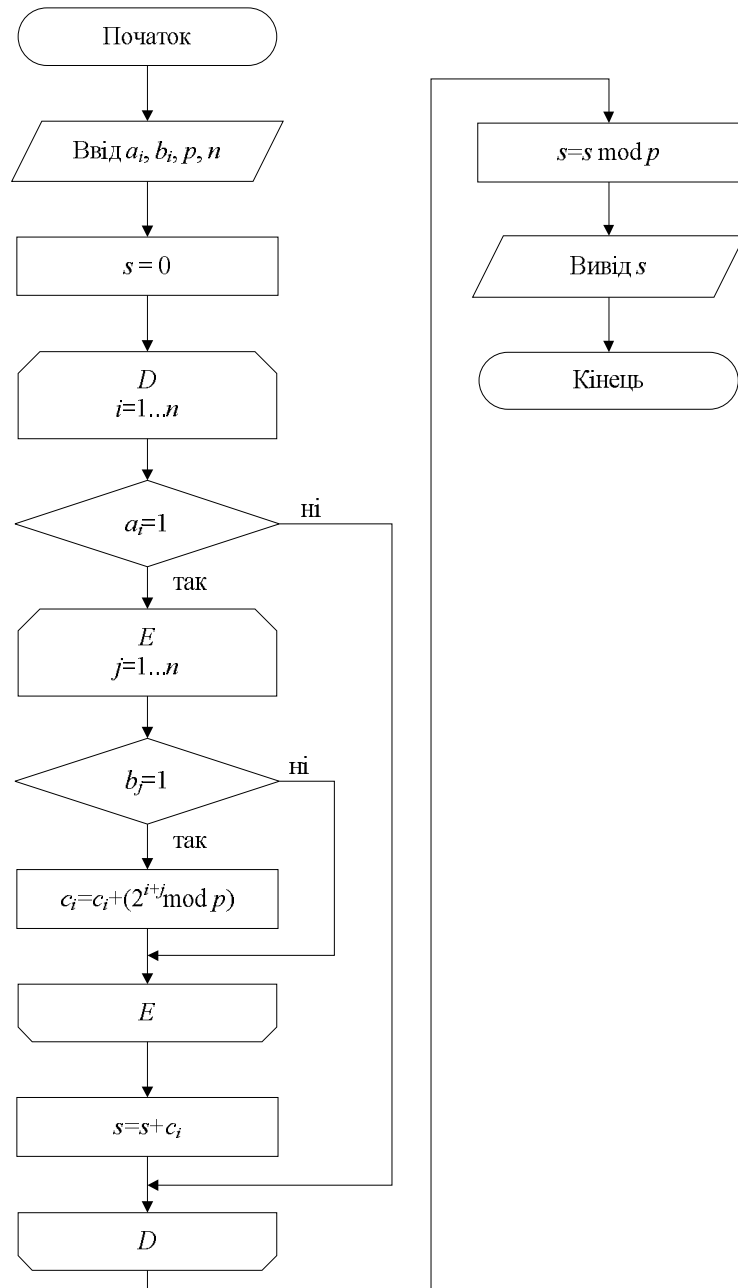
$$a \cdot b(\bmod p) = \left( \sum_{l=1}^{2n} \left( \sum_{\substack{i=0 \\ j=0}}^{n-1} a_i b_j \right) k_l \right) \bmod p, \tag{9}$$

$$i + j = n - 1.$$

Причому, якщо  $a_i = 1, b_s, b_q = 1$ , тоді отримуємо спрощення при розрахунку операції модулярного множення з використанням наступного співвідношення:

$$(b_s + b_q)k_i = k_{i+1} \quad (10)$$

Отже, при використанні співвідношення (10) суттєво зменшується обчислювальна складність виконання операції модулярного множення, що дозволяє ефективно використовувати запропонований метод в алгоритмах захисту інформаційних потоків, побудованих на асиметричних криптосистемах.



**Рис. 1.** Блок схема алгоритму модулярного множення в ТЧБ Радемахера-Крестенсона

Розглянемо приклад: знайти значення виразу  $21 \cdot 25 \bmod 29$ .

Для початку представляємо числа 21 і 25 в двійковій системі числення, тобто  $21=10101$ ,  $25=11001$ , тоді на основі використання табл. 1 отримуємо:

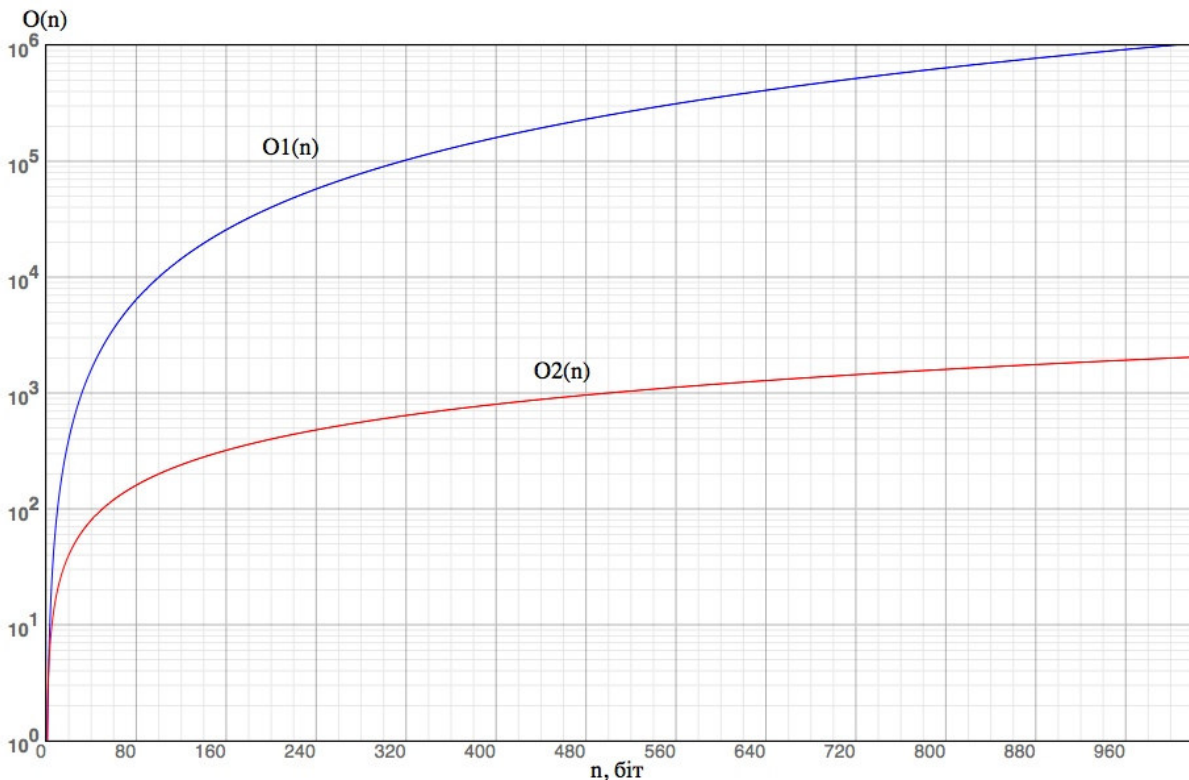
|   |    |    |    |   |   |    |   |   |   |   |
|---|----|----|----|---|---|----|---|---|---|---|
|   | 19 | 24 | 12 | 6 | 3 | 16 | 8 | 4 | 2 | 1 |
| 1 |    | 1  | 0  | 1 | 0 | 1  |   |   |   |   |
| 1 |    |    | 1  | 0 | 1 | 0  | 1 |   |   |   |
| 0 |    |    |    |   |   |    |   |   |   |   |
| 0 |    |    |    |   |   |    |   |   |   |   |
| 1 |    |    |    |   |   | 1  | 0 | 1 | 0 | 1 |

З врахуванням співвідношення (10) одержимо

$$(24+12+6+16+16+8+4+1)\text{mod}29=(19+8+4+1)\text{mod}29=3.$$

Таким чином, отримано удосконалений новий алгоритм заміни операції множення, яка має квадратичну обчислювальну складність  $O1(n) = n^2$ , матрично-модульною операцією сумування в ТЧБ Радемахера–Крестенсона з лінійною складністю  $O2(n) = 2n$ .

Результати дослідження обчислювальної складності запропонованого алгоритму наведені на рисунку 2.



**Рис. 2.** Обчислювальна складність операції модулярного множення удосконаленого алгоритму на основі використання ТЧБ Радемахера–Крестенсона

Результати чисельного експерименту показують, що розроблений метод характеризується на 1 порядок меншою обчислювальною складністю по відношенню до відомих і дозволяє ефективно застосовувати його в різного роду задачах, наприклад в асиметричних системах захисту на етапах як генерування ключів, так і шифрування/дешифрування даних.

## Висновки

Розроблені нові алгоритми опрацювання інформаційних потоків – модулярного множення в ТЧБ Радемахера-Крестенсона дозволили зменшити складність з поліноміально-експоненційної до логарифмічної та лінійної, що на 1-2 порядки збільшило швидкодію рішення задач даного класу. Розроблені інструментальні програмні засоби реалізації алгоритмів модулярного множення дали можливість дослідити вплив часової складності на характеристики запропонованих алгоритмів. Результати відповідають теоретично розрахованим параметрам і підтверджують правильність та результативність запропонованого наукового підходу по вдосконаленню алгоритмів опрацювання інформаційних потоків в комп'ютерних системах.

Оскільки операція модулярного множення є базовою в найбільш поширених системах захисту інформаційних потоків з відкритими ключами, то доцільно використовувати розроблений метод в задачах захисту інформаційних потоків на практиці для вдосконалення систем захисту інформаційних потоків.

## Список літератури

1. Блейхут, Р. Быстрые алгоритмы цифровой обработки сигналов [Текст] = Fast algorithms for digital signal processing : таблицы / Р.Э. Блейхут ; пер. И.И. Грушко ; ред.: В.И. Арнольд, А.С. Попов ; худож. А. Рейнце, пер. с англ. — Москва : Мир, 1989. — 448 с.
2. Николайчук, Я.М. Теорія джерел інформації [Текст] : монографія / Я.М. Николайчук. — Т. : ТНЕУ, 2008. — 536 с.
3. Литвин, А.И. Организация векторных вычислений спектральных коэффициентов преобразования Хаара / А.И. Литвин, А.И. Май, Л.А. Писаренко // Тезисы докладов международной конференции по вычислительной математике (МКВМ-2002), 24–28 июня 2002 г., Новосибирск, Академгородок. — Новосибирск, 2002. — С. 46–58.
4. Николайчук, Я.М. Теоретичні основи побудови та структура спецпроцесорів в базисі Крестенсона / Я.М. Николайчук, О.І. Волинський, С.В. Кулина // Вісник Хмельницького національного університету. — Хмельницький, 2007. — № 3, Т. 1. — С. 85–90.
5. Алексеев, В.Е. Графы и алгоритмы. Структуры данных. Модели вычислений [Текст] : учеб. для студ., обуч. по спец. 010200 – «Прикладная математика и информатика» и по напр. 510200 – «Прикладная математика и информатика» / В.Е. Алексеев, В.А. Таланов. — М. : ИНТУИТ : БИНОМ. ЛЗ, 2006. — 320 с.
6. Столлингс, В. Структурная организация и архитектура компьютерных систем: Проектирование и производительность [Текст] = Computer organization and architecture: Designing and Performance : монографія / В. Столлингс; [Пер. с англ. и ред. В.Т. Тертышного]. — 5-е изд. — М. : Вильямс, 2002. — 892 с.
7. Николайчук Я.М. Основи побудови часових систем на базі вертикальної інформаційної технології / Я.М. Николайчук // Тези науково-практичної конференції професорсько-викладацького складу. — Івано-Франківськ, 1999. — С. 90–92.
8. Николайчук, Я.М. Матричні системи числення / Я.М. Николайчук, О.Д. Круцкевич // Вісник Хмельницького національного університету. — Хмельницький, 2007. — № 3, Т. 1. — С. 62–64.
9. Акушский, И.Я. Машинная арифметика в остаточных классах [Текст] : монографія / И.Я. Акушский, Д.И. Юдицкий. — М. : Советское радио, 1968. — 439 с.
10. Касянчук, М.М. Теорія та оптимізація алгоритмів опрацювання великорозрядних чисел у базисі Крестенсона / М.М. Касянчук, І.З. Якименко, С.В. Івасьєв // Вісник Хмельницького національного університету. — Хмельницький, 2011. — № 3. — С. 265–273.
11. Корнилов, А.И. Принципы построения модулярных индексных умножителей // А.И. Корнилов, М.Ю. Семенов, О.В. Ласточкин // Известия высших учебных заведений. Электроника. — 2004. — № 2. — С. 48–55.
12. Задірака, В.К. Комп'ютерна арифметика багаторозрядних чисел: наукове видання / В.К. Задірака, О.С. Олексюк. — Київ, 2003. — 264 с.
13. Локазюк, В.М. Контроль і діагностування часових пристроїв та систем : Навчальний посібник для ВУЗів. — Хмельницький : ТУП, 2001. — 242 с.