

УДК 004.021

МЕТОДЫ РАСШИРЕНИЯ БАЗИСА В СИСТЕМЕ ОСТАТОЧНЫХ КЛАССОВ: ОБЗОР И АНАЛИЗ ВЫЧИСЛИТЕЛЬНОЙ СЛОЖНОСТИ**Коржавина А.С., Князьков В.С.***ФГБОУ ВО «Вятский государственный университет», Киров, e-mail: as_korzhavina@vyatsu.ru*

Расширение базиса системы остаточных классов – одна из наиболее важных немодульных операций, которая используется, когда необходимо выполнить расширение диапазона представления чисел дополнительными модулями или полную смену базиса, а также при выполнении операции деления и масштабирования, сравнения, контроля четности, определения знака или абсолютной позиционной величины числа. В работе проводится обзор методов расширения базиса, основанных на вычислении коэффициентов системы счисления со смешанными основаниями, и анализ их вычислительной сложности с целью выбора направления для разработки метода расширения базиса, имеющего оптимальное соотношение времени выполнения и аппаратных затрат. Методы расширения базиса, основанные на вычислении коэффициентов системы счисления со смешанными основаниями, наиболее целесообразно использовать для массового выполнения операций расширения базиса, полной или частичной смены базиса.

Ключевые слова: система остаточных классов, расширение базиса системы остаточных классов, система счисления со смешанными основаниями

**BASE EXTENSION IN RESIDUE NUMBER SYSTEMS:
A REVIEW AND COST ANALYSIS****Korzhavina A.S., Knyazkov V.S.***Federal State Budgetary Educational Institution of Higher Education «Vyatka State University», Kirov,
e-mail: as_korzhavina@vyatsu.ru*

Base extension is the most important intermodular operation in residue number system. It is used when the residue range has to be expanded to include additional moduli, or when a conversion to a different RNS has to be done. In addition, it can be exploited for performing division and scaling, comparison, parity checking, sign or magnitude determination. In this paper we present a review of base extension methods and schemes using mixed-radix system coefficients and their cost analysis for developing a new effective base extension method that has an optimal balance of execution time and hardware cost. Base extension methods and schemes using mixed-radix system coefficients are the most effective in massive base extension and base conversion.

Keywords: residue number system, base extension in residue number system, mixed-radix number system

Система остаточных классов (СОК) – это непозиционная система счисления, которая позволяет заменить последовательные методы выполнения арифметических операций над «длинными» целыми числами в позиционных системах счисления на параллельные методы выполнения арифметических операций над наборами «коротких» целых чисел [1–3]. Преимуществом СОК является простота выполнения операций сложения, вычитания, умножения (так называемых модульных операций) по сравнению с арифметикой в позиционных системах счисления, а существенным недостатком – сложность выполнения немодульных операций, таких как операции масштабирования, деления, определения знака, сравнения и определения переполнения диапазона представления чисел и т.д. Другим существенным преимуществом вычислений с применением СОК является более простая аппаратно-техническая реализация вычислительных устройств и, как следствие, их более низкое энергопотребление по сравнению с устройства-

ми на основе вычислений в позиционных системах счисления. Учитывая особенности организации вычислений в СОК, их применение наиболее эффективно для решения задач, алгоритмизация которых реализована с существенным преобладанием модульных операций, например, задач цифровой обработки сигналов [4, 5], криптографии [6, 7].

Одной из важных и сложно реализуемых операций является операция расширения базиса СОК, которая необходима для выполнения операций расширения диапазона представления чисел, например, при реализации алгоритма Монтгомери в приложениях криптографии [6, 7], деления и масштабирования [4, 8], контроля ошибок вычислений [9, 10].

Задача расширения базиса

Система остаточных классов является непозиционной системой счисления, в которой значения позиционного числа A число представлено набором n остатков $(x_1, x_2, \dots, x_n)$ от деления числа A на каждый из n модулей $p_i \in \{p_1, p_2, \dots, p_n\}$ [1–3]:

$$x_i = |A|_{p_i} = A - \left\lfloor \frac{A}{p_i} \right\rfloor \cdot p_i, i=1, 2, \dots, n,$$

где $\left\lfloor \frac{A}{p_i} \right\rfloor$ – целая часть частного $\frac{A}{p_i}$,

$\{p_1, p_2, \dots, p_n\}$ – набор оснований или базис СОК.

Произведение $P = p_1 \cdot p_2 \cdot \dots \cdot p_n$ определяет диапазон представления чисел $A \in [0; P)$ в СОК, причем, если все числа $p_i \in \{p_1, p_2, \dots, p_n\}$ являются попарно взаимно простыми, то между любым положительным целым числом A из диапазона $[0; P)$ и числом, представленным в СОК, имеется взаимно однозначное соответствие.

Расширение базиса, или смена базиса – это процедура, в которой осуществляется поиск значения $(x_{n+1}, x_{n+2}, \dots, x_{n+m})$ числа в СОК с новыми основаниями $\{p_{n+1}, p_{n+2}, \dots, p_{n+m}\}$, представленного изначально в виде $(x_1, x_2, \dots, x_n)$ в СОК с основаниями $\{p_1, p_2, \dots, p_n\}$. Частным случаем является вычисление остатка от деления числа, представленного в СОК, по новому основанию p_{n+1} . Для вычисления остатка от

деления x_{n+1} числа, представленного в СОК, по новому основанию p_{n+1} , используются два подхода: вычисление x_{n+1} с помощью Китайской теоремы об остатках (КТО) [11] и вычисление коэффициентов системы счисления со смешанными основаниями [2, 8, 12–15].

Система счисления со смешанными основаниями

Пусть $\langle p_1, p_2, \dots, p_n \rangle$ – упорядоченный набор оснований СОК. Тогда любое число, представленное в СОК упорядоченным набором остатков от деления $\langle x_1, x_2, \dots, x_n \rangle$ по соответствующим основаниям $\langle p_1, p_2, \dots, p_n \rangle$, может быть также представлено в системе счисления (СС) со смешанными основаниями, с базисом из n элементов $\langle 1, p_1, p_1 \cdot p_2, \dots, p_1 \cdot p_2 \cdot \dots \cdot p_{n-1} \rangle$ с коэффициентами $\langle \tilde{x}_1, \tilde{x}_2, \dots, \tilde{x}_n \rangle$, такими, что для целого числа $A \in [0; P)$ выполняется равенство

$$A = \tilde{x}_1 + \tilde{x}_2 \cdot p_1 + \dots + \tilde{x}_n \cdot p_1 \cdot p_2 \cdot \dots \cdot p_{n-1}. \quad (1)$$

Точный метод определения остатка от деления по новому модулю, основанный на преобразовании числа в СССР, был предложен Сабо и Танакой [2]:

$$|A|_{p_{n+1}} = \left| \tilde{x}_1 + \tilde{x}_2 \cdot p_1 + \dots + \tilde{x}_n \cdot p_1 \cdot p_2 \cdot \dots \cdot p_{n-1} \right|_{p_{n+1}} = \left| \sum_{i=1}^n \tilde{x}_i \cdot \tilde{p}_i \right|_{p_{n+1}}, \quad (2)$$

где $\left| \tilde{p}_i \right|_{p_{n+1}} = \left| \prod_{j=1}^i p_j \right|_{p_{n+1}}$, $\left| \tilde{p}_i \right|_{p_{n+1}}$ вычислены заранее и занесены в таблицу.

Таким образом, для вычисления остатка от деления по новому модулю p_{n+1} необходимо сначала вычислить коэффициенты СС со смешанными основаниями $\langle \tilde{x}_1, \tilde{x}_2, \dots, \tilde{x}_n \rangle$, затем вычислить остаток от деления по формуле (2).

Вычислительная сложность методов расширения базиса на основе вычисления коэффициентов системы счисления со смешанными основаниями

Коэффициенты $\langle \tilde{x}_1, \tilde{x}_2, \dots, \tilde{x}_n \rangle$ представления $A = \tilde{x}_1 + \tilde{x}_2 \cdot p_1 + \dots + \tilde{x}_n \cdot p_1 \cdot p_2 \cdot \dots \cdot p_{n-1}$ вычисляются следующим образом [2]:

$$\begin{aligned} \tilde{x}_1 &= x_1, \\ \tilde{x}_2 &= \left| (x_2 - \tilde{x}_1) \cdot |p_1^{-1}|_{p_2} \right|_{p_2}, \\ \tilde{x}_3 &= \left| \left((x_3 - \tilde{x}_1) \cdot |p_1^{-1}|_{p_3} - \tilde{x}_2 \right) \cdot |p_2^{-1}|_{p_3} \right|_{p_3}, \\ &\dots \\ \tilde{x}_n &= \left| \left(\dots \left((x_n - \tilde{x}_1) \cdot |p_1^{-1}|_{p_n} - \tilde{x}_2 \right) \cdot |p_2^{-1}|_{p_n} - \dots - \tilde{x}_{n-1} \right) \cdot |p_{n-1}^{-1}|_{p_n} \right|_{p_n}. \end{aligned} \quad (3)$$

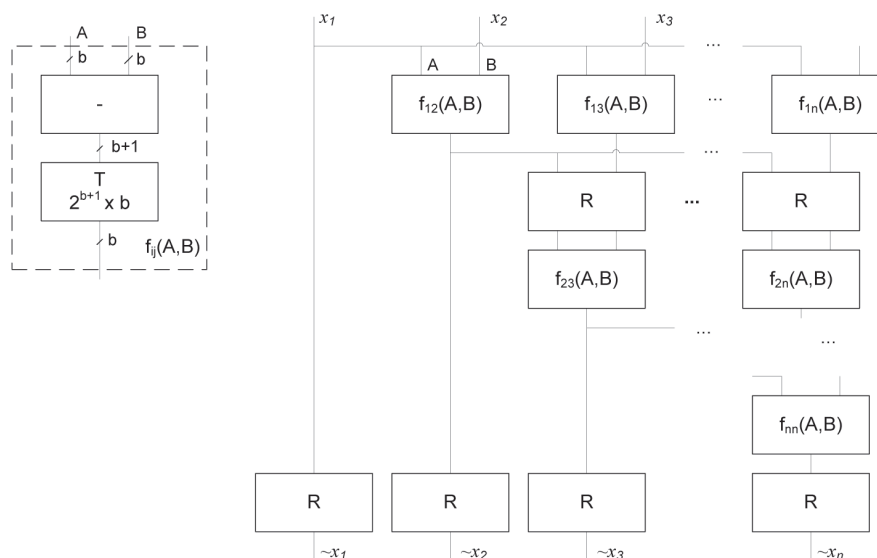


Рис. 1. Схема конвейеризованного метода Сабо и Танаки [14]

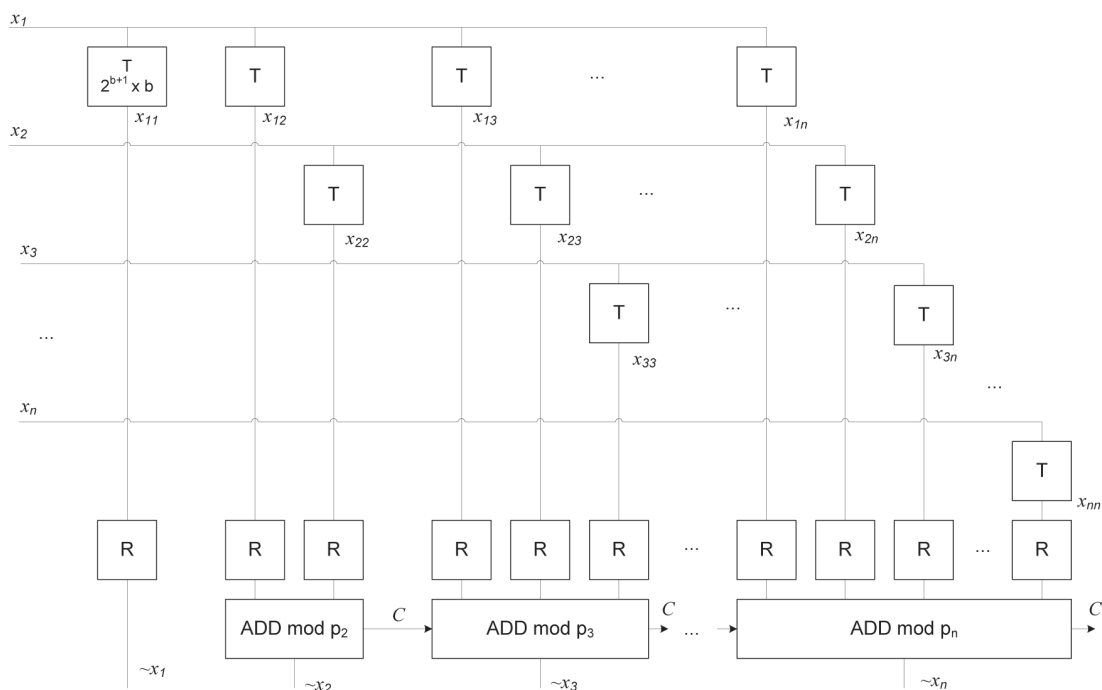


Рис. 2. Схема параллельного метода Хуанга [14]

Для вычисления коэффициентов по формулам (3) требуется выполнение $\frac{n \cdot (n-1)}{2}$

операций модулярного вычитания и столько же операций модулярного умножения [2].

Методы, представленные в работах [12, 13], основаны на классических методах [2], имеющих сложность $O(n^2)$, и ориентированы на оптимизацию числа арифметических операций.

Параллельные методы [8, 14, 15] также основаны на классических методах [2] и позволяют сократить время вычисления коэффициентов $\langle \tilde{x}_1, \tilde{x}_2, \dots, \tilde{x}_n \rangle$ за счет введения дополнительных вычислительных устройств. Например, Хуангом [14] предложен конвейеризованный метод Сабо и Танаки [2] (рис. 1), а также параллельный алгоритм преобразования в систему счисления со смешанными основаниями,

использующий дополнительные подстановочные таблицы (рис. 2). На рисунках использованы следующие обозначения: R – регистр для хранения промежуточных результатов, f_{ij} – функциональный блок, состоящий из вычитателя («–») и таблицы (T), T – подстановочная таблица, C – каналы передачи единиц переноса, $ADD \bmod p_i$ – каскадные сумматоры по модулю p_i .

В [14] время выполнения представлено как $t_T + (\log_2 n + 1) \cdot t_A$ (где t_T – время выборки из таблицы, t_A – время выполнения операции сложения), что, как было показано в [8], не достигается в связи с формированием переносов. Данный метод был улучшен в [8] за счет введения дополнительных $\frac{n \cdot (n-1)}{2}$ умножителей, сложность

алгоритма при этом показана как $O(\log n)$. Схема формирования коэффициентов СС со смешанными основаниями [8] представлена на рис. 3. Используются следующие обозначения: m_{ij} – значения коэффициентов СС со смешанными основаниями для чисел $P_i = \frac{p_1 \cdot p_2 \cdot \dots \cdot p_n}{p_i}$, вычислены заранее

и хранятся в таблицах, $*$ – умножители по модулю p_i , $ADD \bmod p_i$ – каскадные сумматоры по модулю p_i , C – каналы передачи единиц переноса, ADD – позиционный двоичный каскадный сумматор для формирования старшей единицы переноса.

Алгоритм Чакраборти и др. [15] использует каскадную схему подстановочных таблиц и сумматоров, при этом таблицы имеют два входа и два выхода, таким образом, таблиц в общей сложности требуется меньше. При конвейерной обработке время преобразования равно времени выборки из таблицы плюс время одного модулярного сложения. Метод хорошо работает для разрядности модулей 4–6 бит, поскольку при большей разрядности значительно увеличивается объем подстановочных таблиц. Параллельный алгоритм Миллера и Мак-Кормика [15] использует только подстановочные таблицы и основан на решении линейных диофантовых уравнений. Алгоритм медленнее, чем [14], однако он не требует дополнительных арифметических устройств, и в случае конвейерной обработки время одного преобразования равно времени выборки из таблицы.

В таблице представлены следующие характеристики наиболее быстрых методов вычисления коэффициентов СС со смешанными основаниями [2, 8, 14, 15]: количество и объем требуемых подстановочных таблиц, сумматоров/вычитателей (ADD/SUB) и модулярных умножителей (MUL), а также время выполнения; при этом использованы следующие обозначения: n – количество модулей, t_T – время выборки из таблицы, t_A – время выполнения операции сложения/вычитания, t_M – время выполнения операции умножения.

Характеристики методов вычисления коэффициентов СССО

Метод	Количество и объем таблиц	ADD/SUB	MUL	Время вычисления $\langle \check{x}_1, \check{x}_2, \dots, \check{x}_n \rangle$
Сабо, Танака [2], классические	–	$(n-1)$	$(n-1)$	$\frac{n \cdot (n-1)}{2} \cdot (t_M + t_A)$
Сабо, Танака [2], конвейеризированный	$\frac{n \cdot (n-1)}{2}, 2^{b+1} \times b$	$\frac{n \cdot (n-1)}{2}$	–	$(n-1) \cdot (t_T + t_A)$
Хуанг [14]	$\frac{n \cdot (n+1)}{2}, 2^b \times b$	$\frac{n \cdot (n+1)}{2}$	–	$t_T + (n-1) \cdot t_A$
Хитц, Калтофен [8]	$\frac{n \cdot (n+1)}{2}, 2^b \times b$	$\frac{n \cdot (n+1)}{2}$	$\frac{n \cdot (n+1)}{2}$	$t_T + t_M + (2 \cdot \log_2 n + 1) \cdot t_A$
Чакраборти и др. [15], последовательный	$\frac{n \cdot (n-2)}{4}, 2^{2b} \times 2 \cdot b$	$\frac{n \cdot (n-2)}{4}$	–	$\frac{n}{2} \cdot (t_T + t_A)$
Чакраборти и др. [15], параллельный	$\frac{n \cdot (n-2)}{4} + (n-1), 2^{2b} \times 2 \cdot b$	$\frac{n \cdot (n+2)}{4} - 3$	–	$t_T + \frac{n}{2} \cdot t_A$
Миллер [15]	$\frac{n \cdot (n-1)}{2}, 2^{2b} \times b$	–	–	$(n-1) \cdot t_T$

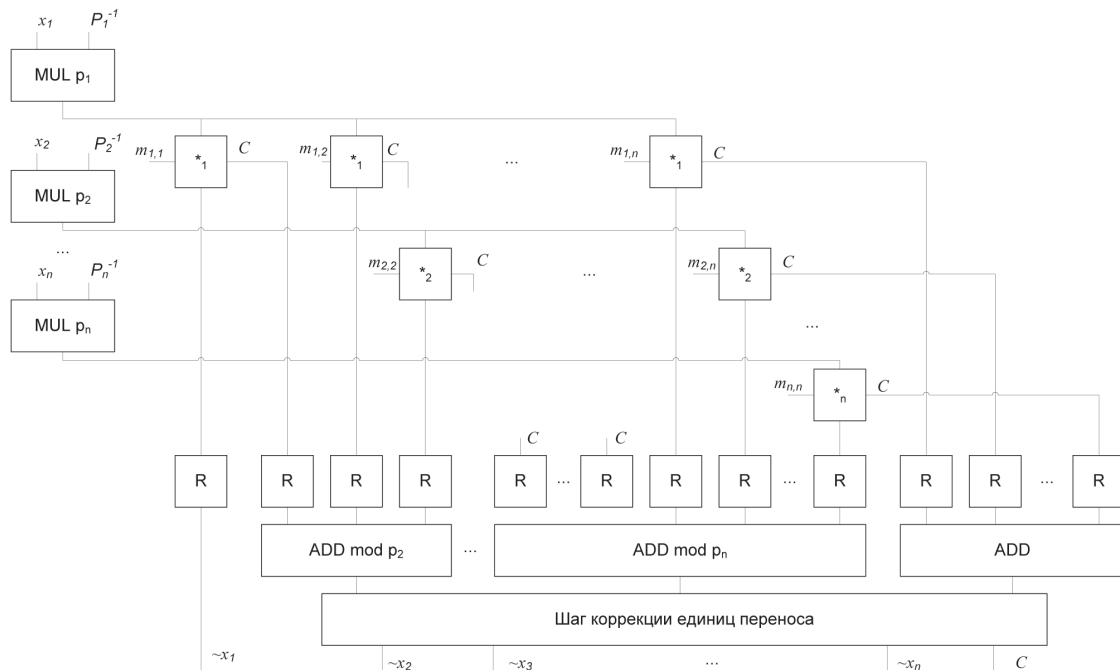


Рис. 3. Схема работы алгоритма Хитц, Калтофен [8]

Как видно из таблицы, самые быстрые методы вычисления коэффициентов СС со смешанными основаниями требуют $O(n^2)$ арифметических устройств и подстановочных таблиц, время же вычисления коэффициентов ограничивается $O(\log n)$.

Вычисление остатка от деления по формуле (2) требует n модулярных умножителей, работающих параллельно и $(n - 1)$ модулярных сумматоров, включенных по каскадной схеме, при этом время вычисления составляет $t_M + \log_2 n \cdot t_A$ [8] или один модулярный умножитель с накоплением (состоящий из одного умножителя по модулю, одного сумматора по модулю и регистра для хранения промежуточного результата), время при этом составляет $n \cdot t_M + (n - 1) \cdot t_A$. Общее время выполнения операции расширения базиса методом [8] составляет $t_T + 2 \cdot t_M + (3 \cdot \log_2 n + 1) \cdot t_A$, при этом для его реализации потребуется $\frac{n \cdot (n + 1)}{2}$ под-

становочных таблиц, $\frac{n \cdot (n + 1)}{2} + m \cdot (n - 1)$

модулярных сумматоров/вычитателей, $\frac{n \cdot (n + 1)}{2} + m \cdot n$ модулярных умножителей, m — количество дополнительных модулей, на которые необходимо расширить базис.

Заключение

Для преобразования числа $x_1, x_2, \dots, x_n$, представленного в СОК с основаниями

$\{p_1, p_2, \dots, p_n\}$ к $x_{n+1}, x_{n+2}, \dots, x_{n+m}$ в СОК с основаниями $p_{n+1}, p_{n+2}, \dots, p_{n+m}$, необходимо вычислить коэффициенты СС со смешанными основаниями $\langle \tilde{x}_1, \tilde{x}_2, \dots, \tilde{x}_n \rangle$, затем m раз вычислить остатки от деления по модулям $p_{n+1}, p_{n+2}, \dots, p_{n+m}$ по формуле (2). Вычисления остатка от деления по каждому модулю независимы и могут быть выполнены параллельно.

В качестве дальнейшего направления исследований планируется разработка метода расширения базиса, имеющего оптимальное соотношение времени выполнения и аппаратных затрат, основанного на том, что при вычислении коэффициентов СС со смешанными основаниями на каждом шаге последовательно вычисляется очередной разряд $\langle \tilde{x}_1, \tilde{x}_2, \dots, \tilde{x}_n \rangle$, который может сразу же использоваться для вычисления остатка по формуле (2). Таким образом, можно совместить во времени процесс получения коэффициентов $\langle \tilde{x}_1, \tilde{x}_2, \dots, \tilde{x}_n \rangle$ и вычисления остатков от деления.

Методы расширения базиса, основанные на вычислении коэффициентов системы счисления со смешанными основаниями, наиболее целесообразно использовать для массового выполнения операций расширения базиса, полной или частичной смены базиса. Для вычисления единичного остатка от деления по новому основанию лучше выбирать способы, позволяющие максимально быстро вычислить остаток,

например, [8], или методы, основанные на Китайской теореме об остатках [11]. В случае использования метода [8] необходим дополнительный анализ целесообразности его использования, поскольку аппаратные затраты для его реализации достаточно велики.

Список литературы

1. Gerard B., Kammerer J.-G., Merkiche N. Contributions to the Design of Residue Number System Architectures // Proceedings of the 22nd IEEE International Symposium on Computer Arithmetic. – France, 2015. – P. 105–112.
2. Szabo N., Tanaka R. Residue Arithmetic and Its Applications to Computer Technology. – NY: McGraw Hill, 1967. – 236 p.
3. Omondi A., Premkumar B. Residue Number Systems: Theory and Implementation. – London: Imperial College Press, 2007. – 296 p.
4. Czyzak M., Smyk R., Ulman Z. Pipelined scaling of signed residue numbers with the mixed-radix conversion in the programmable gate array // Poznan University of Technology Academic Journals. Electrical Engineering. – 2013. – no. 8. – P. 89–99.
5. Cardarilli G.C., Nannarelli A., Re M. Residue number system for low-power DSP applications // Proc. of 41st Asilomar Conference on Signals, Systems, and Computers, IEEE. – 2007. – P. 1412–1416.
6. Bigou K., Tisserand A. RNS modular multiplication through reduced base extensions // In Proc. 25th International Conference on Application-specific Systems, Architectures and Processors (ASAP), IEEE. – 2014. – P. 57–62.
7. Bajard J.C., Eynard J., Merkiche N. Montgomery reduction within the context of residue number system arithmetic // Journal of Cryptographic Engineering. – 2017. – P. 1–12.
8. Hitz M., Kaltofen E. Integer division in Residue Number Systems // IEEE Trans. on Computers. – 1995. – vol. 44(8). – P. 983–989.
9. Sachenko A., Zhengbing H., Yatskiv V. Increasing the data transmission robustness in WSN using the modified error correction codes on residue number system // Elektronika i Elektrotehnika. – 2015. – vol. 21(1). – P. 76–81.
10. Xiao H., Garg H. K., Hu J., Xiao G. New Error Control Algorithms for Residue Number System Codes // ETRI Journal. – 2016. – vol. 38(2). – P. 326–336.
11. Kawamura S. I., Yonemura T., Komano Y., Shimizu H. Exact Error Bound of Cox-Rower Architecture for RNS Arithmetic // IACR Cryptology ePrint Archive. – 2016. – P. 266.
12. Akkal M., Siy P. A new mixed radix conversion algorithm MRC-II // Journal of Systems Architecture. – 2007. – vol. 53(9). – P. 577–586.
13. Gbolagade K.A., Cotofana S.D. An O(n) residue number system to mixed radix conversion technique // IEEE International Symposium on Circuits and Systems (24–27 May, 2009), IEEE. – 2009. – P. 521–524.
14. Huang C.H. Fully parallel mixed-radix conversion algorithm for residue number applications // IEEE Trans. Comput. – 1983. – vol. 32(4). – P. 398–402.
15. Mohan P.V. Residue Number Systems // Theory and Applications. Springer. – 2016. – 351 p.