

УДК 004.62

DOI: 10.25140/2411-5363-2020-4(22)-109-117

Андрій Роговенко

## ДОСЛІДЖЕННЯ ОБЧИСЛЮВАЧІВ ПРИСКОРЕНОГО ОБЧИСЛЕННЯ ДАНИХ ЗБІЛЬШЕНОЇ РОЗРЯДНОСТІ НА ОСНОВІ ОДНОВИМІРНОГО КАСКАДУ КОНСТРУКТИВНИХ МОДУЛІВ

*Актуальність теми дослідження.* Дослідження обчислювачів обчислення даних збільшеної розрядності та врахування впливу методів їх опису, при реалізації в базисі ПЛІС, дозволить збільшити швидкість обробки даних та ефективніше використати ресурси ПЛІС.

*Постановка проблеми.* Прискорення процесу обчислення даних збільшеної розрядності висуває додаткові вимоги до реалізації елементів обчислювальних систем та обчислювальних систем загалом.

*Аналіз останніх досліджень і публікацій.* Швидкість обчислень даних збільшеної розрядності, які використовуються в базисі ПЛІС, залежать від методів їх опису, але ці методи також впливають на апаратні витрати.

*Виділення недосліджених частин загальної проблеми.* Відсутні теоретичні й експериментальні дослідження обчислювачів збільшеної розрядності для обчислень операцій за модулем на основі одновимірних каскадів конструктивних модулів у базисі ПЛІС.

*Постановка завдання.* Метою роботи є опис та дослідження обчислювачів складних операцій за модулем над даними збільшеної розрядності в базисі ПЛІС.

*Виклад основного матеріалу.* Обчислювачі складних операцій за модулем збільшеної розрядності описані методом функціонального опису за допомогою стандартних операторів VHDL, та методом структурного опису у вигляді одновимірних каскадів конструктивних модулів. Залежності швидкодії та апаратних витрат від розрядності визначені експериментальним шляхом, з урахуванням внутрішньої будови конкретного сімейства ПЛІС для кожного з методів опису.

*Висновки відповідно до статті.* Використання методу функціонального опису типовими інструментальними засобами в базисі ПЛІС не дає змогу врахувати особливості алгоритмів обробки даних великої розрядності, що приводить до надлишковості у апаратних витратах. Запропонований метод структурного опису з використанням одновимірних каскадів конструктивних модулів мовою опису апаратури, демонструє кращі результати та дає змогу більш гнучко підходити до використання апаратних ресурсів ПЛІС.

Зменшення апаратних витрат на реалізацію засобів обчислення даних збільшеної розрядності в межах конкретної ПЛІС, за рахунок вивільнення додаткових ресурсів дає змогу збільшити розрядність даних, що обробляються, без додаткових витрат на заміну апаратного забезпечення при загальному збільшенні продуктивності обчислювального елемента або системи.

*Ключові слова:* одновимірний каскад конструктивних модулів; ПЛІС; арифметичні операції за модулем; VHDL; функціональний опис; багаторозрядні дані; комбінаційна логіка.

*Рис.: 10. Табл.: 2. Бібл.: 6.*

*Актуальність теми дослідження.* Операції за змінним модулем є одними із найбільш поширених арифметичних операцій, які вимагають проведення обчислень над даними з великою розрядністю, оскільки основними галузями їх використання є системи цифрової обробки сигналів, криптографічні системи, відмовостійкі системи, спеціалізовані обчислювачі, що побудовані на основі апарату модулярних обчислень.

*Постановка проблеми.* Основною з головних вимог, що висуваються до таких пристроїв, є збільшення швидкодії при помірних апаратних витратах. Одним із напрямів підвищення швидкодії багаторозрядного обчислювального пристрою є використання прискорених методів та алгоритмів обчислення. А при реалізації цих обчислювальних пристроїв у базисі ПЛІС швидкодія буде залежати також і від методу опису.

Метод опису обчислювального пристрою в базисі ПЛІС, крім швидкодії, суттєво впливає і на апаратні витрати. Навіть при дуже гарних результатах роботи пристрою за критерієм швидкодії, витрати на апаратну реалізацію можуть виявитись недопустимими.

*Аналіз останніх досліджень і публікацій.* У попередніх роботах детально розглядається метод опису обчислювальних елементів операцій додавання за модулем на основі одновимірних каскадів конструктивних модулів [1; 2], який побудований на основі конструктивного модуля [3]. На основі операції додавання за модулем були запропоновані реалізації інших складніших арифметичних операцій за модулем, таких як множення та піднесення до степеня [4].

Раніше проведені дослідження суматорів за модулем демонструють достатню швидкість при невеликих апаратних витратах у обчислювальних пристроях, побудованих на основі одновимірних каскадів конструктивних модулів [5]. Для оцінки ефективності пристроїв, які обчислюють більш складні операції за модулем, необхідно провести дослідження впливу збільшення розрядності пристрою на швидкість з урахуванням апаратних витрат.

**Виділення недосліджених частин загальної проблеми.** Відсутні теоретичні й експериментальні дослідження обчислювачів збільшеної розрядності для обчислень операцій за модулем на основі одновимірних каскадів конструктивних модулів у базисі ПЛІС.

**Мета роботи.** Метою роботи є дослідження апаратних витрат та швидкості обчислювальних пристроїв, які складаються із суматорів на основі одновимірних каскадів конструктивних модулів при збільшенні розрядності даних що обробляються. А також порівняння отриманих результатів із результатами дослідження пристроїв описаних методом функціонального опису на мові VHDL.

**Виклад основного матеріалу.** У якості обчислювальних пристроїв для дослідження обрані пристрій множення за модулем, та пристрій підведення до степеню за модулем, які будуються на основі суматорів.

Типова реалізація обчислювачів передбачає використання методу функціонального опису на мові VHDL та базується на основі стандартних операторів цієї мови [6].

Наприклад, пристрій множення за модулем описується за допомогою бінарного оператора множення та оператору mod:

```
AmB <= std_logic_vector(unsigned(A) * unsigned(B));
```

```
R <= std_logic_vector(unsigned(AmB) mod unsigned(P));
```

Тут AmB – це проміжний сигнал множення двох операндів, розрядність яких дорівнює подвоєній розрядності операнду.

Опис сигналів має такий вигляд:

```
signal A,P,B,R : std_logic_vector(N - 1 downto 0);
```

```
signal AmB : std_logic_vector(N*2 - 1 downto 0);
```

Для завантаження вхідних даних, та реєстрації результату була запропонована структура обчислювача, що наведена на рис 1.

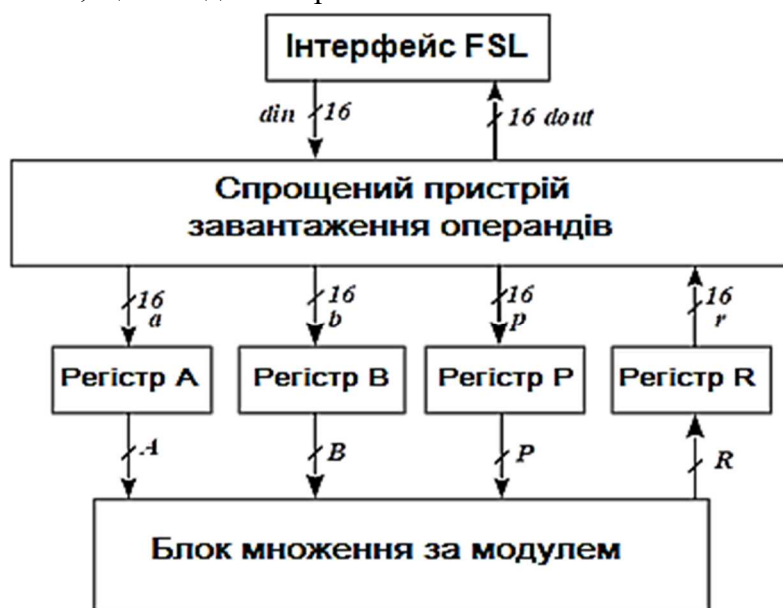


Рис. 1. Структура пристрою множення за модулем, яка описана методом функціонального опису мовою VHDL

Крім блока множення дослідний пристрій складається зі спрощеного пристрою завантаження, який забезпечує узгодження з інтерфейсом FSL, та регістрів вводу/виводу. Алгоритм роботи спрощеного пристрою завантаження операндів представлений на рис. 2.

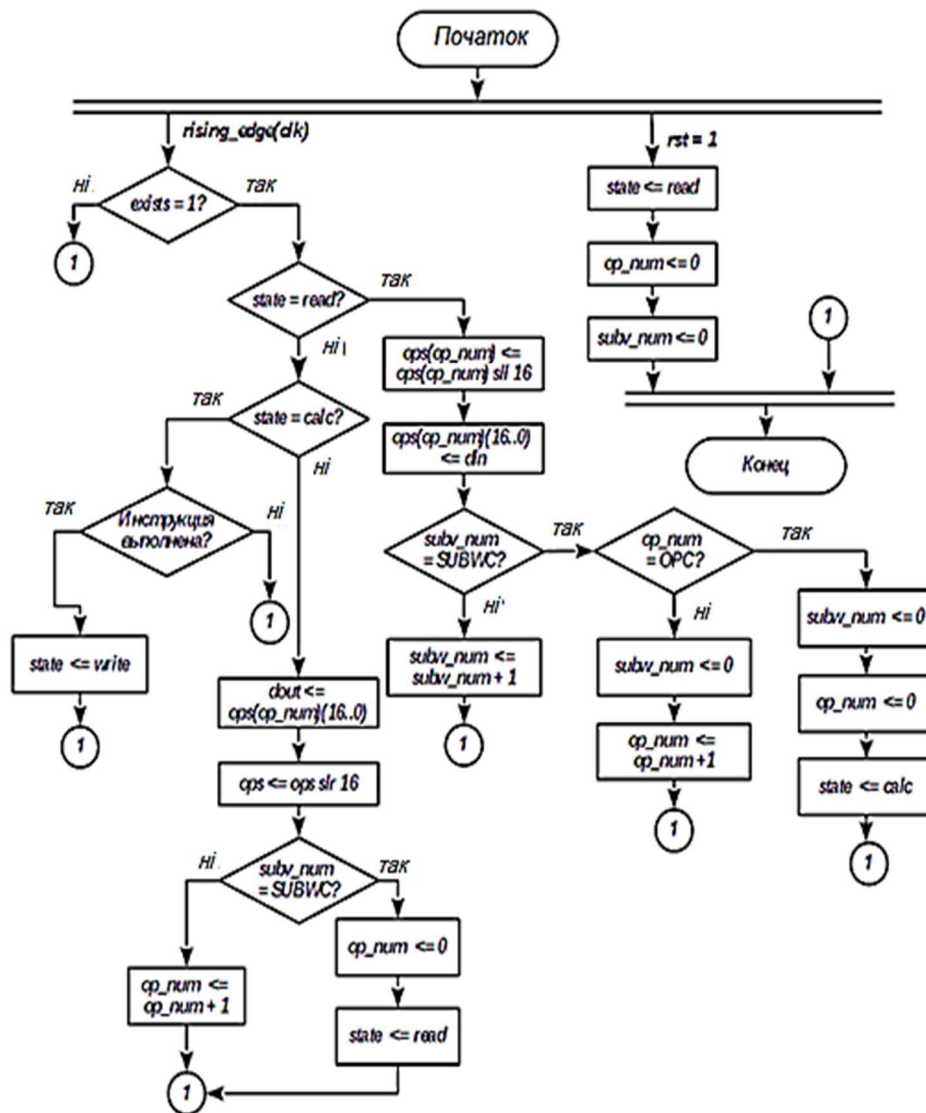


Рис. 2. Схема алгоритму роботи спрощеного пристрою завантаження операндів

Для дослідження множення на основі одновимірного каскаду конструктивних модулів побудована аналогічна схема, але операція додавання за модулем буде виконуватись окремим багаторозрядним суматором за модулем. Це дозволяє реалізувати алгоритм множення, що запропонований на рис. 3.

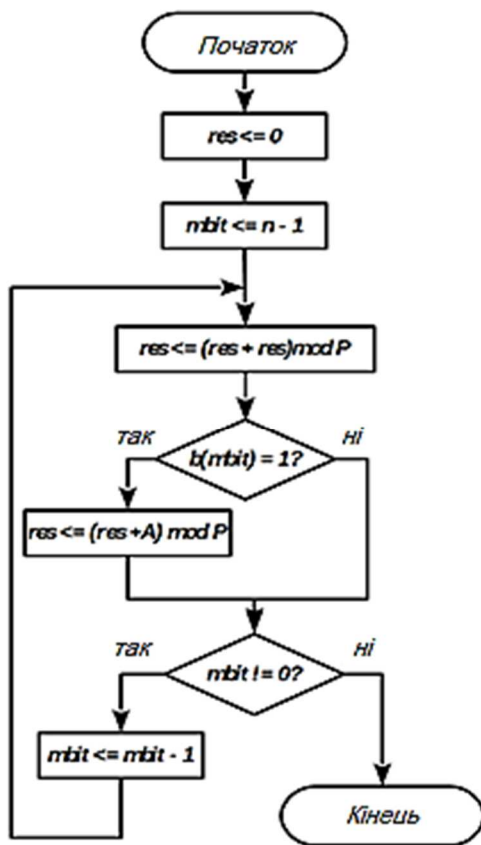


Рис. 3. Схема алгоритму роботи блоку множення на основі одновимірного каскаду конструктивних модулів

З урахуванням особливостей алгоритму та інтерфейсу суматора запропонована структура пристрою множення за модулем, яка представлена на рис. 4, з якого видно, що інтерфейсна частина пристрою відповідає інтерфейсній частині з першого дослідження (рис. 1). Таким чином, її впливом на загальну кількість ресурсів можна в подальшому знехтувати.

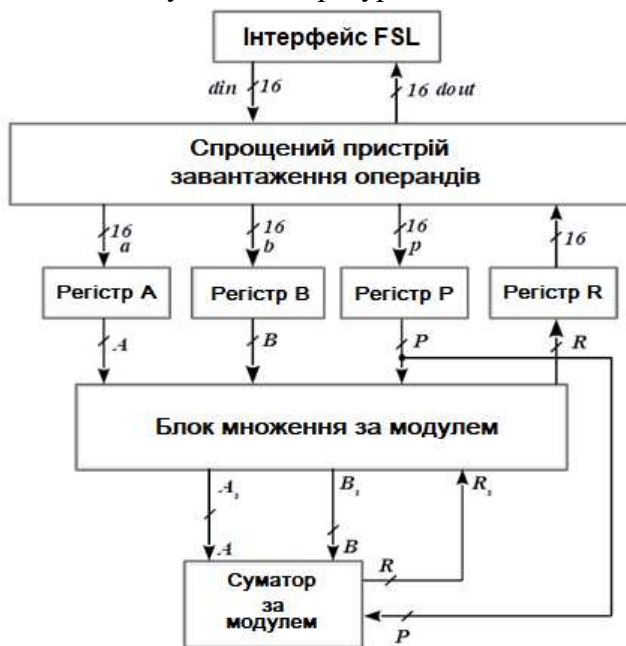


Рис. 4. Структура пристрою множення на основі одновимірного каскаду конструктивних модулів

Досліди проводились із вхідними даними з розрядністю від 16 до 1024. Результати експериментальних обчислень наведені в таблицях 1 та 2, а також проілюстровані у вигляді функцій, зображені на рисунках 5 та 6.

Таблиця 1

*Результати експериментів із пристроєм множення за модулем, який описаний методом функціонального опису на мові VHDL*

Розрядність	Кількість LUT	Кількість Slice	Затримка, нс
16	1611	549	106,385
32	6325	1796	243,701
48	14273	3826	387,603
64	25164	6619	540,669
80	38890	10090	704,07
96	56152	15075	876,24

Таблиця 2

*Результати експериментів із пристроєм множення за модулем, який описаний методом на основі одновимірного каскаду конструктивних модулів*

Розрядність	Кількість LUT	Кількість Slice	Затримка, нс
128	1755	592	11177,216
256	3480	1276	32699,392
384	5252	1881	64521,984
512	6491	2317	107351,04
640	8078	2854	159002,88
768	9272	3630	222587,904
896	10968	4305	295778,56
1024	14056	5438	379039,744

Табличні дані для першого опису з використанням операторів VHDL наведені лише для розрядів до 96. Подальше збільшення розрядності вхідних даних обмежувалось ресурсами ПЛІС, що використовувалась у дослідях, і неспроможністю інструментів синтезу виконати імплементацію проекту.

Для порівняння результатів при розрядності понад 96 з результатами методу функціонального опису на мові VHDL була побудована аналітична функція, що отримана за допомогою методу найменших квадратів, тому що отримання практичних значень обмежилось можливістю апаратури.

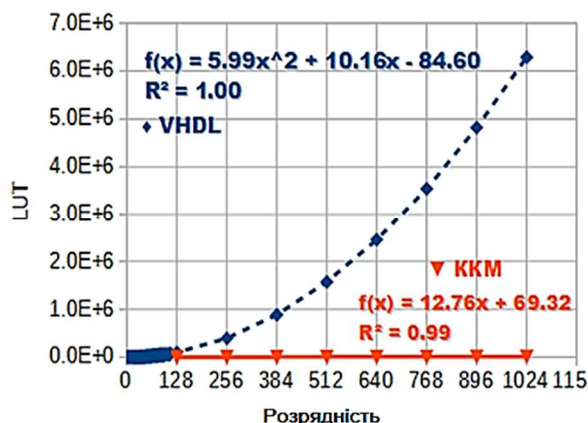


Рис. 5. Залежність кількості LUT від розрядності

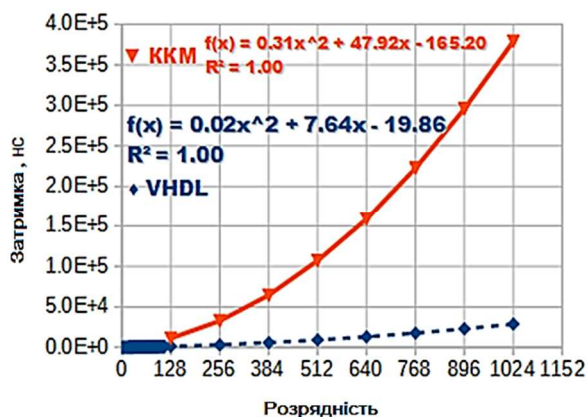


Рис. 6. Залежність затримки від розрядності

Оскільки стандартний оператор піднесення до степеню мовою VHDL не підтримує роботу із сигналами, реалізація цієї операції виконана на основі операції множення за алгоритмом наведеним на рис. 7.

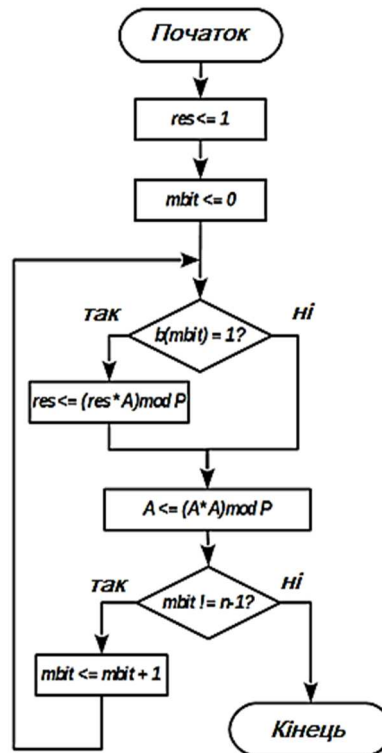


Рис. 7. Схема алгоритму піднесення до степеню за змінним модулем

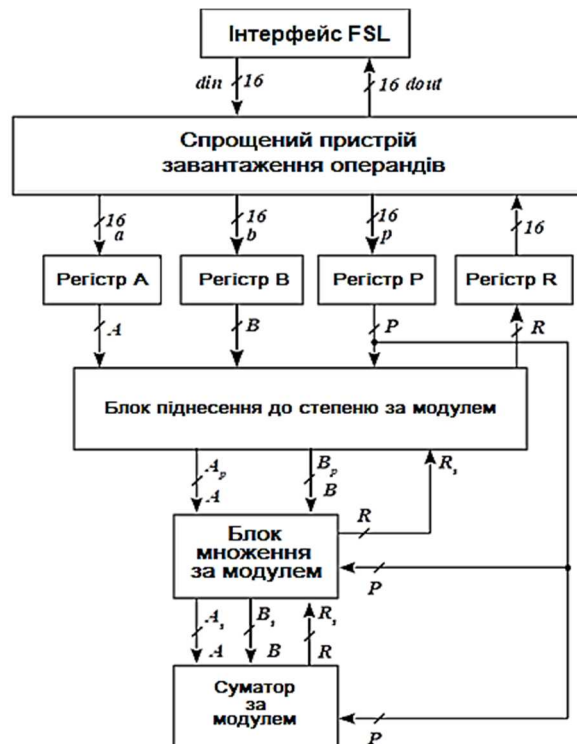


Рис. 8. Структура пристрою піднесення до степеню на основі одновимірного каскаду конструктивних модулів

З урахуванням особливостей алгоритму запропонована структура пристрою піднесення до степеню за модулем, яка представлена на рис. 8. Досліди проводились із вхідними даними з розрядністю від 16 до 1024. Результати експериментальних обчислень проілюстровані у вигляді функцій на рисунках 9 та 10.

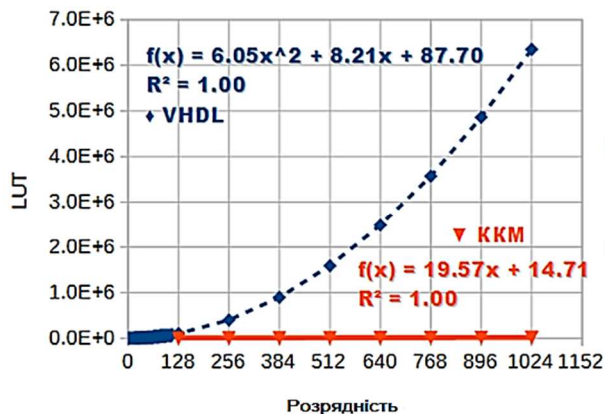


Рис. 9. Залежність кількості LUT від розрядності

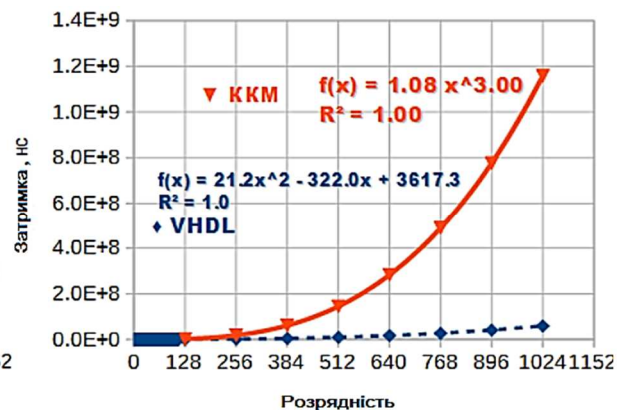


Рис. 10. Залежність затримки від розрядності

**Висновки відповідно до статті.** Відповідно до отриманих результатів у реалізаціях обох операцій методом функціонального опису мовою VHDL, затримка на обчислення результату має менші значення в діапазоні від 8 до 96 розрядів, ніж при використанні методу структурного опису на основі одновимірного каскаду конструктивних модулів, це пояснюється використанням у переважній більшості комбінаційної логіки на відміну від одновимірного каскаду конструктивних модулів, у якому переважає послідовна логіка.

Згідно з результатами експерименту можна констатувати, що реалізація обчислювачів великої розрядності стандартними засобами є неефективною у зв'язку з надлишковістю апаратних витрат. Водночас великою перевагою використання суматора на основі одновимірного каскаду конструктивних модулів як основи для блока піднесення до степеню за модулем є те, що для реалізації блоків великої розрядності витрачається суттєво менше ресурсів. Наприклад, реалізація методом функціонального опису мовою VHDL на розрядності понад 96 займає кількість ресурсів, яку не можуть надати навіть найбільші екземпляри сімейству ПЛІС Spartan6. При цьому реалізація з використанням суматора за модулем на основі КKM дає змогу реалізувати блоки розрядністю більше ніж 1024.

#### Список використаних джерел

1. Роговенко А. І., Тарасенко В. П., Тесленко О. К. Використання схем групового перенесення у суматорах в залишках на основі одновимірних каскадів конструктивних модулів. *Системний аналіз та інформаційні технології: матеріали 15-ї Міжнародної науково-технічної конференції SAIT 2013* (Київ, 27-31 травня 2013 р.). Київ : "ІПСА" НТУУ "КПІ", 2013. С. 484-486.
2. Rogovenko A., Tarasenko V., Teslenko O. The performance defining for adders with variable module based on one-dimensional cascade of constructional modules. *Advanced Computer System and Networks: Design and Application. Proceedings Of the 4st International Conference ACSN-2009*. Lviv, 2009. Pp. 11–13.
3. Роговенко А. І., Тарасенко В. П., Тесленко О. К. Створення параметричних ядер (softcores) для виконання операцій в кінцевих полях. *Науково-технічний журнал "Радіоелектронні і комп'ютерні системи"*. 2008. № 6. С. 261–263.

4. Роговенко А. І. Структура операційного пристрою виконання операцій за модулем на основі одномірного каскаду конструктивних модулів. *Актуальные научные исследования в современном мире : XXIV Междунар. научн. конф.* (26-27 апреля 2017 г., Переяслав-Хмельницкий). Переяслав-Хмельницкий, 2017. Вип. 4(24), ч. 4. С. 60–63.

5. Роговенко А. І., Тарасенко В. П., Тесленко О. К. Оптимізація апаратних витрат на реалізацію параметричних ядер (soft-cores) для виконання операцій в скінченних полях. *Науково-технічний журнал "Радіоелектронні і комп'ютерні системи"*. 2009. № 5. С. 184–189.

6. IEEE Std 1076-2008: IEEE standard VHDL language reference manual. Institute of Electrical and Electronics Engineers. IEEE computer society (2009).

### References

1. Rohovenko, A. I., Tarasenko, V. P., Teslenko, O. K. (2013). Vykorystannia skhem hrupovoho perenesennia u sumatorakh v zalyshkakh na osnovi odnovymirnykh kaskadiv konstruktyvnykh moduliv [Use of group transfer schemes in adders in residues on the basis of one-dimensional cascade of constructional modules]. *Systemnyi analiz ta informatsiini tekhnolohii: materialy 15-i Mizhnarodnoi naukovo-tekhnichnoi konferentsii SAIT 2013 – Systems analysis and information technologies: materials of the 15th International Scientific and Technical Conference SAIT 2013* (pp. 484-486), NNK "IPSA" NTUU "KPI".

2. Rogovenko, A., Tarasenko, V., Teslenko, O. (2009). The performance defining for adders with variable module based on one-dimensional cascade of constructional modules. *Advanced Computer System and Networks: Design and Application. Proceedings Of the 4st International Conference ACSN-2009* (pp. 11–13).

3. Rohovenko, A. I., Tarasenko, V. P., Teslenko, O. K. (2008). Stvorennia parametrychnykh yader (softcores) dlia vykonannia operatsii v kintsevykh poliakh [Creating parametric cores (softcores) to perform operations in finite fields]. *Radioelektronni i kompiuterni systemy – Electronic and computer systems*, (6), pp. 261–263.

4. Rohovenko, A. I. (2017). Struktura operatsiinoho prystroiu vykonannia operatsii za modulem na osnovi odnomirnoho kaskadu konstruktyvnykh moduliv [The structure of the operating device for performing operations on the module based on a one-dimensional cascade of constructional modules]. *Aktualnie nauchnie yssledovanyia v sovremennom myre: XXIV Mezhdunar. nauchn. konf. – Actual scientific research in the modern world: XXIV Intern. scientific. conf.* (Vol. 4(24)(4), pp. 60–63).

5. Rohovenko, A. I., Tarasenko, V. P., Teslenko, O. K. (2009). Optyimizatsiia aparatnykh vytrat na realizatsiiu parametrychnykh yader (soft-cores) dlia vykonannia operatsii v skinchenykh poliakh [Optimization of hardware costs for the implementation of parametric cores (soft-cores) to perform operations in finite fields]. *Radioelektronni i komp'iuterni systemy – Electronic and computer systems*, (5), pp. 184–189.

6. IEEE Std 1076-2008: IEEE standard VHDL language reference manual. Institute of Electrical and Electronics Engineers. IEEE computer society (2009).

UDC 004.62

*Andrii Rohovenko*

## RESEARCH OF COMPUTERS FOR ACCELERATED CALCULATION OF HIGH BIT DEPTH DATA BASED ON A ONE-DIMENSIONAL CASCADE OF CONSTRUCTIVE MODULES

**Urgency of the research.** *The study of computers to calculate data of increased bit size and take into account the impact of methods of their description on the implementation of FPGA will increase the speed of data processing, and more efficient use of FPGA resources is certainly an urgent task.*

**Target setting.** *Accelerating the process of calculating data of increased bit size places additional demands on the implementation of elements of computer systems and computer systems in general.*

**Actual scientific researches and issues analysis.** *The speed of computing high-bit data used in an FPGA depends on the methods used to describe it, but these methods also affect hardware costs.*

**Uninvestigated parts of general matters defining.** *There are no theoretical and experimental studies of high-bit computers to calculate the operations of modules based on one-dimensional cascades of structural modules based on FPGA.*



**The research objective.** The aim of the work is to describe and study computers of complex operations on the module on the data of the increased bit size in the basis of FPGA.

**The statement of basic materials.** Computers of complex operations on the increased bit module are described by the method of functional description using standard VHDL operators and the method of structural description in the form of a one-dimensional cascade of structural modules. The dependences of speed and hardware costs on the bit are determined experimentally taking into account the internal structure of a certain family of FPGAs for each of the methods of description.

**Conclusions.** The use of the method of functional description by typical tools based on FPGA does not allow to take into account the peculiarities of large data processing algorithms, which leads to excessive hardware costs. The proposed method of structural description using a one-dimensional cascade of structural modules in the language of hardware description demonstrates better results and allows a more flexible approach to the use of FPGA hardware resources.

Reducing the hardware cost of implementing high-bit computing tools within a particular FPGA, by freeing up additional resources, increases the bit size of the data being processed at no additional cost to replace the hardware with an overall increase in the performance of the computing element or system.

**Keywords:** one-dimensional cascade of structural modules; FPGA; arithmetic operations modulo; VHDL; functional description; multi-bit data; combinational logic.

Fig.: 10. Table: 2. References: 6.

**Роговенко Андрій Іванович** – старший викладач кафедри інформаційних та комп'ютерних систем, Національний університет «Чернігівська політехніка» (вул. Шевченка, 95, м. Чернігів, 14035, Україна).

**Rohovenko Andrii** – senior lecturer of Department of Information and Computer Systems, Chernihiv Polytechnic National University (95 Shevchenko Str., 14035 Chernihiv, Ukraine).

**E-mail:** arogoenko@gmail.com

**ORCID:** <https://orcid.org/0000-0003-4594-5692>

**ResearcherID:** G-3926-2014