УДК 004.274:004.383:621.391.7

ЗАСТОСУВАННЯ СИСТЕМНОГО ПІДХОДУ ДЛЯ СИНТЕЗУ МОДЕЛЕЙ БАЗОВИХ ЕЛЕМЕНТІВ РЕКОНФІГУРОВНИХ СТРУКТУР В СИСТЕМАХ ПЕРЕДАЧІ ІНФОРМАЦІЇ

Г. І. Воробець, О. І. Воробець, В. Е. Гордіца

Чернівецький національний університет імені Юрія Федьковича

Анотація. *Для модуль-орієнтованої технології синтезу цифрових систем удосконалено методику системного підходу до розробки і моделювання спеціалізованих кодерів та потокових шифраторів у комп'ютерних засобах з реконфігуровною архітектурою. Обґрунтовано математичну модель відображення набору станів кіберфізичної системи множиною виконуваних комп'ютерною компонентою процедур, функцій, процесів. Запропоновано алгоритм пошуку оптимізованого програмованого логічного середовища для реалізації проекту.*

Ключові слова: *реконфігуровні комп'ютерні засоби, сигнально кодові конструкції, потокове шифрування, програмовані логічні середовища, VHDL моделі, системний аналіз.*

Вступ

Сучасні технічні системи (ТС), наприклад системи телеметрії та автоматики [1], робототехнічні комплекси промислового та індивідуального застосування, кіберфізичні системи (КФС) [2] та засоби інтернету речей (IoT) все частіше проектують і використовують для розв'язку багатоплановых задач, що потребують комплексного підходу до вирішення питань отримання, обробки і захисту інформації. Кіберскладовою компонентою (КСК) [3] вказаних ТС і комплексів, тобто складовою, що відповідає за «інтелектуалізацію» опрацювання інформації та прийняття рішень про функціонування ТС, є вбудовані (ВКСЗ) чи розподілені комп'ютерні системи і засоби (РКСЗ), здатні реалізувати складні алгоритми аналізу і опрацювання даних.

До ВКСЗ в ТС, зокрема портативного і мобільного призначення для технологій IoT і КФС, поряд з мультизадачністю часто виставляються вимоги мініатюризації їх конструктивного виконання та мінімізації енергоспоживання.

Одним із сучасних підходів для вирішування вказаних задач є застосування КСК з реконфігуровною архітектурою на основі програмованих логічних інтегральних структур і середовищ (ПЛІС, FPGA – Field Programmable Gate Array, CPLD – Complex Programmable Logic Device) [4, 5] для реалізації високопродуктивних обчислювачів ВКСЗ, спеціалізованих систем з паралельною обробкою даних, тощо. Проте наразі залишаються недостатньо обґрунтованими низка питань щодо ефективного аналізу і синтезу систем з реконфігуровною архітектурою: оцінки доцільності застосування такої архітектури порівняно з традиційною, раціонального використання ресурсів ПЛІС для реалізовуваних проектів, коректного вибору структурних рішень проектів, та інші. Метою даного дослідження є обґрунтування застосування методів системного аналізу та модуль-орієнтованої технології для вирішення задач аналізу і синтезу реконфігуровних цифрових пристроїв ВКСЗ в роботизованих ТС і комплексах, системах телеметрії та керування, тощо, де реалізуються складні алгоритми завадозахисного кодування і шифрування даних при передачі інформації у відкритих каналах зв'язку [6, 7].

1. Особливості обробки інформації в мультизадачних телеметричних системах

ТС телеметрії і телекерування можна розглядати як один з прикладів систем, де яскраво виражена мультизадачність їх функціонування. Такі системи застосовуються в комп'ютерній томографії у медичній галузі, космічних дослідженнях, атомній енергетиці, нафтовій і газовій промисловості, в тому числі на об'єктах критичного застосування [1, 8, 9]. В залежності від функціонального призначення та множини й особливостей вирішуваних задач, КСК таких ТС забезпечують вимірювання і контроль сотень і тисяч різних типів параметрів. Це, наприклад, потребує опрацювання різних за фізичною природою інформаційних сигналів, лінеаризації характеристик вимірювальних перетворювачів [2], нормалізації та масштабування сигналів для коректного аналізу даних, математичної й функціональної обробки векторних чи матричних величин, баз даних, тощо. Змінюється обсяг даних, які опрацьовуються безпосередньо окремими модулями КСК ВКСЗ чи транспортуються між модулями.

Розширення функціональних можливостей і переліку технічних, зокрема високоенергетич-

них, об'єктів, для яких впроваджуються технології IoT і КФС [2], застосування при цьому мобільних і портативних пристроїв (аджетів) для передачі інформації потребують підвищення надійності і захисту даних в комунікаційних каналах.

Прикладом портативної мобільної ТС може бути багатофункціональний модуль обробки сигналів розподіленої мережі інтелектуальних сенсорів для вирішення задач технологічного чи біомедичного профілю та моніторингу екологічного стану довкілля [10]. Сенсорна мережа в даному випадку може реалізуватись за принципами функціонування Mesh Wi-Fi мереж [11, 12], в тому числі з використанням ZigBee протоколів [12, 13]. В таких ТС критично зростає загальний обсяг інформації, що підлягає контролю з боку її КСК і потребує додаткової обробки та аналізу ресурсами ВКСЗ, чи застосування ресурсів РКСЗ, наприклад, для моделювання й аналізу процесів [6] із застосуванням технічних можливостей високопродуктивних кластерів, «хмарних» чи «туманних» обчислень, тощо [14].

Таким чином, раціональний розподіл і балансування обчислювального навантаження між кінцевими пристроями КСК ТС, серверами, модулями ВКСЗ і РКСЗ, упорядкування маршалінгу даних в ТС та Internet/Ethernet трафіку при використанні «хмарних» технологій чи технологій IoT, захисту потоків даних від несанкціонованого доступу є складними задачами, що потребують системного підходу і комплексних апаратно-програмних рішень [6, 7, 10]. Одним з ключових завдань з вказаного переліку є оцінка ресурсів ПЛІС, необхідних для апаратного відображення множини всіх алгоритмів мультизадачної ТС засобами синтезованої КСК з урахуванням часового розподілу їх реалізації.

2. Опис КСК ТС як об'єкта узагальненої задачі системного аналізу

Суть ієрархічно-модульного підходу до проектування ВКСЗ/РКСЗ полягає в декомпозиції задачі, а, відповідно, загального алгоритму її розв'язку та структурного рішення ТС, на окремі сегменти з ієрархічним підпорядкуванням від найпростішого до найскладнішого. Запропонована в [15] ієрархія: Структура – Пристрій – Модуль – Процес – Функція – Процедура/Дія (Structure - Device - Module - Process - Function - Procedure/Action, S-D-M-P-F-A), дозволяє достатньо деталізувати довільний алгоритм для його реалізації апаратними засобами. Основою даної ієрархії виступає об'єкт "Модуль" як функціонально завершений вузол для реалізації певного нескладного процесу. Реалізовуваний "Процес" описується деякою логічною/арифметичною "Функцією", що складається з послідовності елементарних "Процедур/Дій". Певний набір модулів реалізує певну підпрограму із узагальненого функціонального алгоритму і розглядається як окремий "Пристрій" у загальній "Структурі" КСК ТС. Таким чином, модуль-орієнтована технологія може розглядатись як підхід до уніфікації структурних (апаратних) рішень, що є відображенням наборів алгоритмів, реалізовуваних мультизадачною ТС.

Узагальнена структура КСК ТС (рис.1) як правило містить: центральний мікропроцесорний пристрій (CPU); та/чи модуль логічного аналізу (MA) вхідних умов $X(t)=\{x_i(t) \mid i=\overline{1,I}\}$, та вихідних результатів $Y(t)=\{y_m(t) \mid m=\overline{1,M}\}$ отриманих при виконанні команд $U(t)=\{u_h(t) \mid i=\overline{1,H}\}$; програмовне середовище (FPGA) із засобами програмування/реконфігурування (PR) і вбудовані засоби зберігання (LB) у вигляді певної бібліотеки, чи засоби зовнішнього/мережевого доступу (I/O Ext) до реконфігураційних файлів виконуваних задач $Z=\{z_j \mid j=\overline{1,J}\}$. Для коректного інтелектуального управління процесами ТС множина її фізичних станів має бути відображена відповідними станами КСК у мультизадачному просторі станів (рис. 2) $S(t)=\{s_k \mid k=\overline{1,q}\}$, що визначається його розмірністю S=<LNZ>.

Можливі три основні класичні варіанти реалізації структури КСК ТС: 1) у вигляді лінійної системи з послідовним виконанням задач Z, і, відповідно, послідовними переходами між станами S системи; 2) розпаралеленої структури, в якій певні задачі Z^* з множини Z реалізуються одночасно, що відповідає синхронізації певних

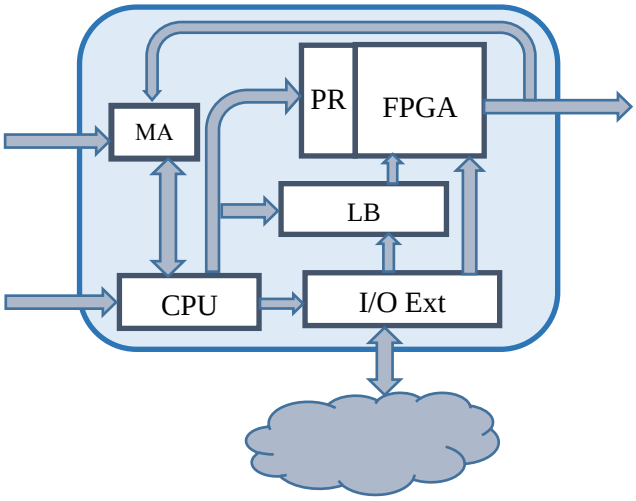

Рис. 1. Узагальнена структура кіберскладової компоненти технічної системи

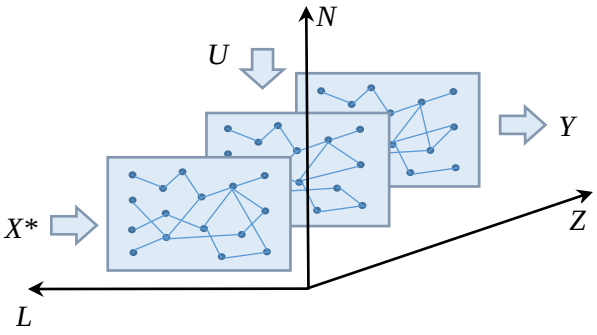

Рис. 2. Модельне відображення кіберскладовою компонентою простору станів технічної системи

станів системи; 3) комбінована структура з паралельно-послідовним виконання множини задач Z. Задача синтезу КСК ТС в залежності від умов реалізовуваних процесів може формулюватись як задача системного аналізу, що визначається цільовою функцією мінімізації використовуваних апаратних ресурсів при задовільній швидкодії системи, чи функцією максимальної швидкодії синтезованої ТС при задовільних значеннях використовуваних ресурсів. У першому випадку необхідно забезпечити максимальне суміщення модулів, а, відповідно, елементів, що виконують певні процедури у загальному просторі станів S. Тоді задача синтезу зводиться до пошуку оптимального за розмірністю програмованого середовища FPGA за значенням відповідної цільової функції з урахуванням обмежень мінімально необхідної кількості елементів FPGA для реалізації конкретних процедур виконуваних алгоритмів.

Другий випадок є складнішим, оскільки оптимізація цільової функції потребує врахування як розмірностей виконуваних алгоритмів за реалізовуваними станами, так і синхронізації цих алгоритмів.

3. Постановка та опис узагальненої задачі системного аналізу КСК ТС

Розглянемо модельне представлення КСК ТС (рис. 2) для простішого випадку, коли набір задач виконуваних ТС можна відобразити окремими площинами Z тривимірного простору S. Набір станів для окремої задачі з множини $Z=\{z_j \mid j=\overline{1,J}\}$ зображено вузлами на площинах z_j, переходи між ними відповідними ребрами. Отриманий граф у простішому випадку відтворює алгоритм виконуваної задачі z_j для деякого процесу, що описується відповідною множиною функцій $F(t)=\{f_n(t) \mid n=\overline{1,N}\}$, кожна з яких використовує стандартизовані набори процедур / дій / актів $A=\{a_l(t) \mid \ell=\overline{1,L}\}$, тобто $f_n(t)=g(A)$. Якщо елементарна процедура виконується певним типом елементів FPGA, то реалізовуваний деяким модулем M процес $p_q \in P$, де $P(t)=\{p_q(t) \mid q=\overline{1,Q}\}$ для окремої задачі потребує апаратних ресурсів:

$$R_{p_q}(t)=\sum_{n=1}^{N} f_n(t)=\sum_{n=1}^{N}\sum_{l=1}^{L} a_{nl}(t), \qquad (1)$$

де $a_{nl}(t)$ є коефіцієнтами матриці P розмірністю P=<LN>, які приймають вагові значення відповідно до кількості використовуваних типів елементів FPGA. У випадку виконання умови «один модуль M – один процес q» структурна складність η синтезованого модуля M визначається записаним в (1) параметром R_{p_q}: $\eta(M(P_q))=R_{p_q}$. При паралельному виконанні кількох процесів в одному модулі потрібно записати суму:

$$\eta(M(P))=\sum_{q=1}^{Q} P_q(t). \qquad (2)$$

Для випадку, коли задачі мультизадачної ТС розв'язуються однопроцесними модулями реконфігуровне середовище FPGA має забезпечувати можливість відображення Z файлів реконфігурації, що потребує визначення загальних мінімально необхідних ресурсів Ф для різних функціональних типів алгоритмів ТС:

1) для послідовного алгоритму функціонування ТС –

$$\Phi_{ser}=\min_{\delta}(\max_{1\le z\le Z}\eta(M(P)))=\min_{\delta}(\max_{1\le z\le Z}(\sum_{q=1}^{Q}P_q(t))), \qquad (3)$$

що з мінімальним коефіцієнтом запасу $\delta_{ser}=R_0-R_{P_{\max}}$, де R_0 – сумарний ресурс вибраного середовища FPGA, забезпечує завантаження файлу конфігурації задачі z_j, яка потребує максимальної кількості ресурсів $R_{P_{\max}}$ у реконфігуровній матриці;

2) для паралельного алгоритму функціонування ТС –

$$\Phi_{par}=\min_{\delta}\eta(M(P))=\min_{\delta}\sum_{j=1}^{J}\sum_{q=1}^{Q}P_{jq}(t), \qquad (4)$$

що з мінімальним коефіцієнтом запасу $\delta_{par}=R_0-R_{P_\Sigma}$ забезпечує одночасне завантаження в реконфігуровну матрицю деякого набору Z^* з усіх файлів конфігурації задач з повного набору Z, які повинні виконуватись паралельно і потребують сумарних ресурсів R_{P_Σ};

3) для комбінованого алгоритму $\Phi_{complex}$ описується виразом подібним до (4) для кожного нового етапу переконфігурації структури новим на-

бором Z^* і може приймати проміжне значення між Φ_{ser} та Φ_{par}, однак коефіцієнт запасу $\delta_{complex} = R_0 - R_{P_{opt}}$ визначається для структури оптимально упакованої за використовуваними ресурсами $R_{P_{opt}}$ для наборів Z^*. Критерієм оптимального упакування є мінімізація кількості невикористаних базових елементів вибраної FPGA. При цьому потрібно враховувати, що для другого і третього типів алгоритмів можливі додаткові витрати ресурсів для синхронізації паралельних процесів і вводу/виводу певних проміжних результатів обробки інформації.

Для другого і третього типів алгоритмів матриця процесів використовуваних ресурсів для ТС структурної складності $\eta(M(P))$ трансформується у тривимірний тензор з коефіцієнтами $a_{jnl}(t)$: $V = \left\{ a_{jnl}(t) \mid j = \overline{1,J};\ n = \overline{1,N};\ \ell = \overline{1,L} \right\}$. Кількість ресурсів для реалізації паралельного і комбінованого типів алгоритму функціонування ТС описується виразом:

$$R_P = \sum_{j=1}^{J} R_{p_q}(t) = \sum_{j=1}^{J} \sum_{n=1}^{N} \sum_{l=1}^{L} a_{jnl}(t). \qquad (5)$$

Обмежуючими факторами щодо прийняття рішення про вибір типу FPGA для синтезу реконфігуровного середовища є особливості і доступні ресурси $B = \{b_k \mid k = \overline{1,K}\}$ елементної бази, яка розроблена для конкретної серії ПЛІС і дозволяє реалізувати елементарні процедури/дії $a_{jnl}(t)$ для виконання алгоритмів вирішуваних задач: кількість базових універсальних логічних блоків (LUT), перемикальних і тригерних елементів (Flip Flops), буферних елементів та мультиплексорних фрагментів (Number of BUFGMUXs), ліній/шин вводу/виводу сигналів (IOBus), а також можливостей їх конфігурації для міжелементної компоновки. Особливості реалізації міжелементних/міжмодульних з'єднань, а також вибір способу синхронізації сигналів різних модулів можуть значно впливати на загальні витрати ресурсів для реалізації проекту. Останній фактор може значно відрізнятися для різних серій FPGA.

Таким чином, узагальнена задача системного аналізу для синтезу КСК мультизадачної ТС полягає у визначенні мінімально необхідних, але достатніх ресурсів ПЛІС для забезпечення повної функціональності системи, і формулюється як задача пошуку мінімуму цільової функції $F^* = f(\delta)$ для відповідних типів функціональних алгоритмів, яка обмежена базисом $B = \{b_k\}$ у *K*-вимірному просторі.

Дискретними станами *K*-вимірного $B = \{b_k\}$ простору є точки, що відповідають конфігурації конкретних типів FPGA. Тому алгоритм пошуку розв'язків сформульованої задачі в геометричній інтерпретації зводиться до знаходження точок найближче розташованих до опуклого многогранника необхідних ресурсів Ф для різних функціональних типів алгоритмів ТС побудованого у цьому ж *K*-вимірному просторі.

Остаточне рішення щодо реалізації цілісного проекту КСК ТС залежить від супутніх компонент, синтезованих виробником в одному корпусі з програмованим середовищем, зокрема процесорного ядра (CPU), додаткових модулів пам'яті (RAM), інтерфейсів комутації з периферією, тощо. Наявність таких компонент в FPGA, що пропонують фірми Xilinx, Altera спрощує синтез ТС і забезпечує їй більшу гнучкість включаючи можливість динамічного реконфігурування програмованого середовища.

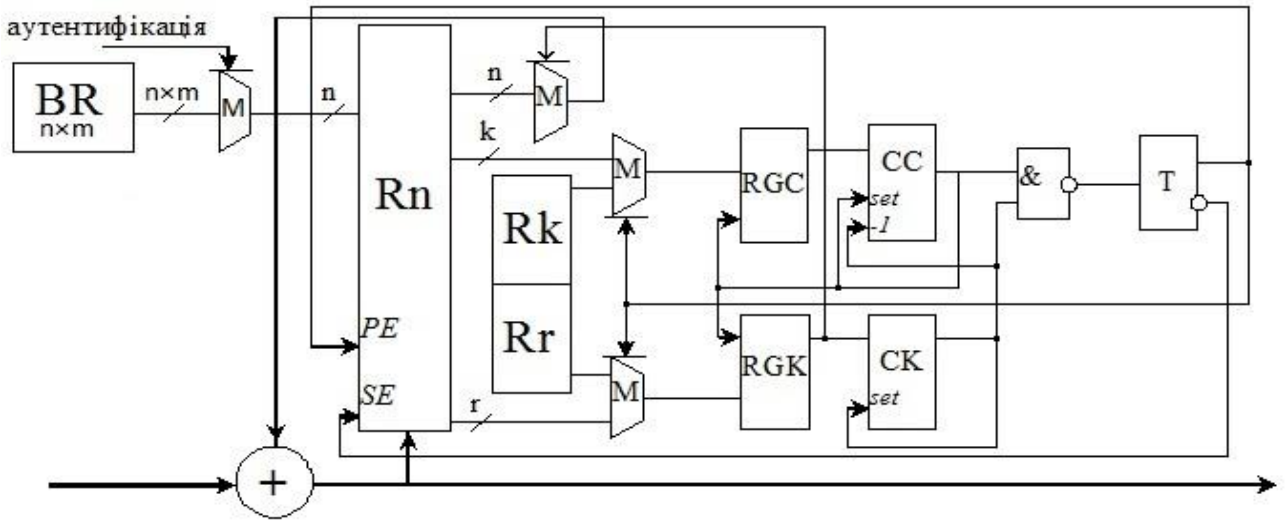

Рис. 3. Варіант схеми потокового шифратора для телеметричної системи

4. Особливості синтезу моделей файлів реконфігурації КСК ТС на основі системного підходу

Розглянемо приклад синтезу моделі потокового шифратора [7] для телеметричної системи (рис. 3) на основі системного підходу. Результати досліджень удосконалених рішень потокових шифраторів з динамічною зміною автоключа [7] підтверджують їх високі статистичні показники за тестами NIST STS 2.1.2. Однак, в залежності від типів шифрованих файлів для покращення їх криптостійкості доцільно динамічно модифікувати вектор ініціалізації та принципи формування автоключа. Це досягається за рахунок реконфігурування базового модуля шифрування за результатами аутентифікації учасників транзакції перед кожним наступним сеансом передачі даних.

Алгоритм синтезу моделей реконфігуровних файлів для набору задач шифрування / дешифрування наступний: 1) синтезують схемотехнічні рішення подібні до рис. 3 для всього набору задач; 2) синтезують VHDL моделі для схемотехнічних рішень; 3) проводять симуляцію VHDL моделей програмними засобами рекомендованими виробником ПЛІС; 4) синтезують комплексну системну модель; 5) визначають коефіцієнти використання ресурсів для задач проекту; 6) розраховують мінімально необхідні ресурси для заданого алгоритму функціонування системи та оцінюють цільову функцію; 7) вибирають потрібний для проекту кристал FPGA за критерієм мінімуму невикористаних надлишкових ресурсів і реалізують синтезований модуль.

Особливістю середовища ISE WebPack, створеного фірмою Xilinx для роботи з кристалами FPGA їхнього виробництва є наявність модуля симуляції проекту, який після завантаження VHDL моделі і її компіляції дозволяє згенерувати звіт у вигляді таблиці з розрахунками використаних для проекту базових елементів кристалу. Як видно з таблиці 1, у заголовному рядку приведено крім назви всіх типів базових елементів також інформацію про їх загальну кількість у кристалі, а у стовпцях – кількість використаних елементів для синтезу елементарного вузла (регістра reg_spispo_16, лічильника count_down_4, мультиплексора mux_16_1, тощо), що виконує певну процедуру чи функцію. Таким чином, приведені в таблиці значення і є коефіцієнтами $a_{jnl}(t)$ для записаних вище співвідношень, а значеннями $B=\{b_k \mid k=\overline{1,K}\}$, які визначають обмеження за ресурсами для реалізації проекту виступають величини максимального числа базових елементів, приведені у верхньому рядку під їх назвами.

Отримати оцінку використаних ресурсів для синтезу базового вузла можна як використовуючи його окрему VHDL модель (рис. 4, 5), так і модель повної конфігурації реконфігуровного файлу (рис. 6).

Таблиця 1

Фрагмент таблиці використаних ресурсів FPGA Spartan 3NE для реалізації однієї конфігурації

Module Name	Logic Utilization											
	Number of Slice Flip Flops		Number of 4 input LUTs		Number of occupied Slices		Number of Slices containing only related logic		Total Number of 4 input LUTs		Number of bonded IOBus	
	11,776		11,776		5,888				11,776		372	
reg_spispo_16	31	1%	18	1%	18	1%	18(18)	100%	18	1%	37	9%
reg_pipo_16											34	9%
reg_pipo_8									18	4%		
reg_pipo_4											10	2%
ad_m2											1	1%
CC	4	1%	9	1%	5	1%	5(5)	100%	9	1%	7	1%
count_down_4	4	1%	9	1%	5	1%	5(5)	100%	9	1%	7	1%
mux_4_1			4	1%	2	1%	2(2)	100%	4	1%	13	3%
mux_8_n_8_1			32	1%	16	1%	16(16)	100%	32	1%	82	22%
mux_16_1			8	1%	4	1%	4(4)	100%	8	1%	21	5%
n_and (n_or)			1	1%	1	1%	1(1)	100%	1	1%	3	1%
trig	2	1%			2	1%	2(2)	100%			4	1%

```
entity reg_sispo is
    Port ( sin : in  STD_LOGIC;
           R : in  STD_LOGIC;
           L : in  STD_LOGIC;
           clk : in  STD_LOGIC;
           pout : out  STD_LOGIC_VECTOR (7 downto 0);
           sout : out  STD_LOGIC);
end reg_sispo;

architecture Behavioral of reg_sispo is

begin
 process (clk,R,L)
     variable temp : STD_LOGIC_VECTOR (7 downto 0):="00000000";
     begin
                 if (R='1') then pout<="00000000";
                                                 sout<='0';
                 else if (rising_edge (clk) and L='1') then
                                                          temp(7 downto 1)
:= temp(6 downto 0);
                                                       temp(0) := sin;
                      end if;
                 sout <= temp(7);
                 pout <= temp;
               end if;
 end process;
end Behavioral
```

Рис. 4. Текст фрагмента VHDL коду для моделювання регістра з послідовним введенням та послідовним і паралельним виведенням даних

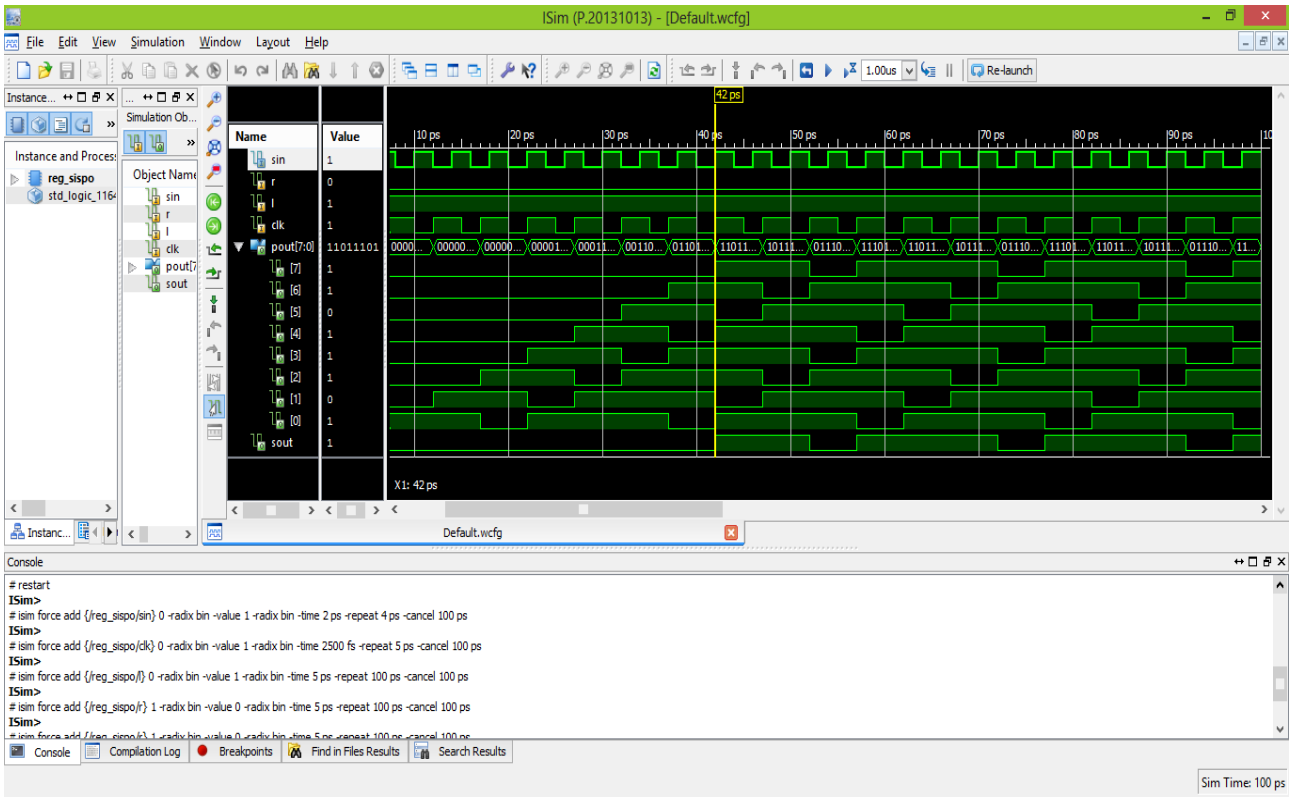

Рис. 5. Результати тестування VHDL моделі 8-розрядного регістра

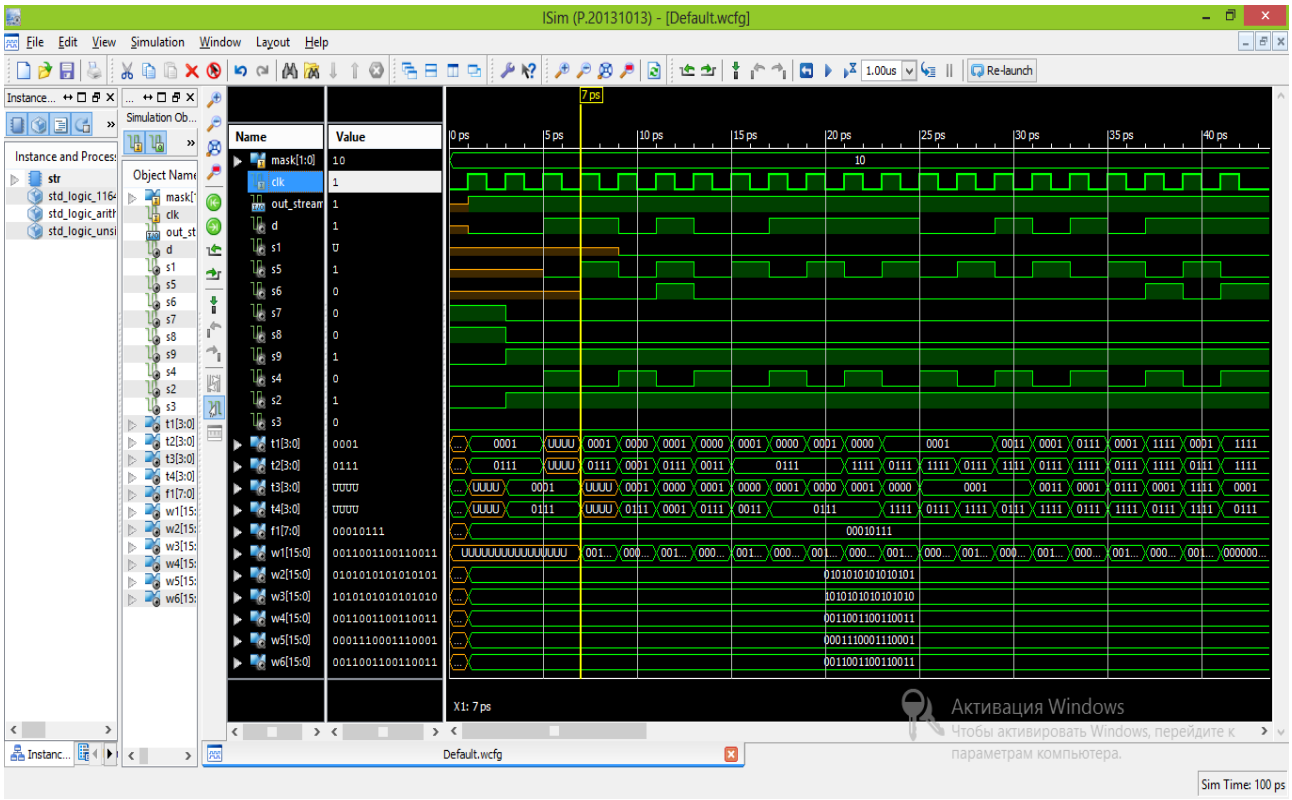

Рис. 6. Налагоджування синхронізації сигналів між окремими елементами шифратора

Використовуючи VHDL моделі окремих компонент середовище програмування ISE Xilinx WebPack дає можливість протестувати побітову трансформацію інформаційних сигналів у кожному вузлі (рис. 5). У вікні користувача "Console" відображено інформацію про коректність чи наявність колізій при трансформації даних у досліджуваній компоненті.

При досліджуванні VHDL моделей файлів конфігурації завершених модулів можна прослідкувати зміну станів сигналів на входах/виходах окремих компонент загальної схеми, що відображено у двох лівих колонках консолі користувача на рисунку 6.

Слід зауважити, що коефіцієнти $a_{jnl}(t)$ отримані цими двома способами можуть дещо відрізнятися, як зазначено вище, оскільки в повній конфігурації проводиться валідація всіх комутованих з'єднань та синхросигналів, на відміну від моделей окремих вузлів. Модель функціонально завершеного модуля (рис. 6) також дозволяє провести оцінку можливості його реалізації ресурсами всіх доступних типів структур FPGA кристалів відповідних серій, що є в наявності у підключених бібліотеках використовуваного пакету ISE WebPack. Таким чином, синтезувавши всі файли реконфігурації для множини задач Z ТС та отримавши шукані коефіцієнти $a_{jnl}(t)$ достатньо скласти зведені таблиці використаних та доступних ресурсів, і з допомогою нескладних аналітичних розрахунків вибрати кристал FPGA з оптимальною конфігурацією як за мінімумом надлишковості використовуваних ресурсів, так і за загальною вартістю проекту.

Приведені в таблиці 1 та рисунках 5 і 6 результати моделювання реалізовано засобами Spartan-3A-3AN FPGA Starter Kit Board [16].

Відмітимо, що паралельні і комбіновані функціональні алгоритми ТС доцільно реалізовувати на кристалах з можливим динамічним реконфігуруванням, оскільки для реалізації на простіших структурах їх потрібно фрагментувати для синхронного послідовно завантаження паралельно виконуваних фрагментів в кристал. Математичні моделі задачі системного аналізу для таких алгоритмів потребують подальших досліджень.

5. Висновки

В результаті проведених досліджень запропоновано удосконалений системний підхід до аналізу і синтезу вбудованої кіберскладової компоненти для складних мультизадачних комп'ютеризованих систем, та апробовано його для послідовних функціональних алгоритмів обробки інформації в технічних системах з реконфігуровною архітектурою комп'ютерних засобів.

Обґрунтовано математичну модель комп'ютерної компоненти технічної систем, яка дозволяє відобразити множину станів системи на множину виконуваних комп'ютерною складовою процедур, функцій, процесів. Вперше сформульовано узагальнену постановку задачі системного аналізу для пошуку мінімаксного рішення цільової функції синтезу комп'ютерної кібер компоненти мультизадачної технічної системи, особливістю якої є використання 3D розмірної матриці для опису кількісних параметрів необхідних базових логічних структур FPGA, чи CPLD типу, які дозволяють синтезувати схемні рішення для виконання вказаних процесів, функцій, процедур.

Запропоновано алгоритм пошуку оптимізованого рішення щодо вибору програмованого логічного середовища для реалізації проекту. Показано, що такий підхід спрощує прийняття рішень щодо вибору елементної бази для реалізації проектів, та підвищує їх техніко-економічну ефективність за рахунок обґрунтованої мінімізації надлишковості використовуваних ресурсів програмованих логічних структур.

Описані особливості застосування запропонованої методики для синтезу і моделювання багато режимного потокового шифратора в системах захисту при передачі даних, що реалізуються в технологіях інтернету речей і кіберфізичних систем, дозволяють легко адаптувати запропоновану методику, наприклад використовуючи засоби програмного пакету ISE WebPack фірми Xilinx, для синтезу двовимірних матриць і тривимірних тензорів розрахункових коефіцієнтів цільової функції і обмежуючих факторів та визначення необхідних ресурсів програмованого логічного середовища для реалізації файлів реконфігурації синтезованого мультизадачного проекту практично довільної складності.

Результати даних досліджень було використано для створення теоретичного курсу та лабораторних робіт з навчальної дисципліни "IoT technologies for cyber physical systems" освітньо-професійної програми підготовки магістрів зі спеціальності «Комп'ютерна інженерія», яка впроваджена у навчальні плани Чернівецького національного університету за підтримки Erasmus + проекту "Internet of Things: Emerging Curriculum for Industry and Human Applications" (AL-IoT) No. 573818-EPP-1-2016-1-UK-EPPKA2-CBHE-JP, відповідно грантової угоди 2016-2967 / 001-001 з Європейським Союзом.

Список використаної літератури

1. Козырев, Г. И. Современная телеметрия в теории и на практике. Учебный курс. [Текст] / Г. И. Козырев, А. В. Назаров, И. В. Шитов, и др. – М.: Наука и техника, 2007. – 672 с.

2. Lee, E. A. Introduction to Embedded Systems. A Cyber-Physical Systems Approach. [Electronic resours] / Lee E. A., Seshia S. A. // http://LeeSeshia.org, ISBN 978-0-557-70857-4, 2011. [Electronic Resource]. – Access Mode: https://ptolemy.berkeley.edu/books/ leeseshia/.

3. Воробець, Г. І. Самореконфігуровні комп'ютерні засоби як модельна основа інтелектуальної самоорганізації кіберфізичних систем. / Воробець Г. І., Тарасенко, В. П. – Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua / [Електронний ресурс]. – Режим доступу : http://ena.lp.edu.ua:8080/bitstream/ntb/39386/1/20-114-120.pdf

4. Mazurenko, M. I. WEB-system dynamical reconfiguration based on metric analysis of vulnerability databases OTS-components. [Text] / M. I. Mazurenko, V. S. Kharchenko, A. V. Gorbenko // Radio electronic and computer systems. – 2014. – № 5 (69). – P. 135–139.

5. Palagin, A. V. Design and Application of the PLD-Based Reconfigurable Devices. [Text] / A. V. Palagin, V. M. Opanasenko // Design of Digital Systems and Devices. Series: Lecture Note in Electrical Engineering. – 2011. – Vol. 79. – P. 59–91.

6. Vorobets, G. I. Application of the self-adaptive and self-reconfigurable computer devices for micro- and nanoelectronics. [Text] / G. I. Vorobets, V. P. Tarasenko // Radio electronic and computer systems. – 2015. – № 1 (71). – P.143–148.

7. Vorobets, H. Self - reconfigurable cryptographical coprocessor for data streaming encryption in tasks of telemetry and the Internet of Things. [Electronic resours] / H. Vorobets, O. Vorobets, V. Horditsa, at al., // Proceedings of the 2017 IEEE 9th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2017. – Vol. 2. – 3 November, 2017. – Bucharest; Romania; 21-23 September 2017. – pp. 1117–1120. – DOI: 10.1109/IDAACS.2017.8095259. – Режим доступа: https://ieeexplore.ieee.org/document/ 8095259/.

8. Аппаратно-программный комплекс сбора, передачи и обработки данных системы телеметрии. [Электронный ресурс]. – Режим доступа: http://radmirtech.com.ua/processing-data-system-telemetry/

9. Мурашов, В. А. Применение современных технологий передачи данных при модернизации системы телеметрии. / В. А. Мурашов, А. В. Зотов [Электронный ресурс]. – Режим доступу: https://gaselectro.ru/stati/primenenie-sovremennyh-tehnologij-peredachi-dannyh-pri-modernizacii-sistemy-telemetrii.html

10. Воробець, Г. І. Комп'ютеризована система з реконфігуровною архітектурою для моніторингу параметрів довкілля. [Текст] / Г. І. Воробець, Р. Д. Гуржуй, М. А. Кузь // Восточно-Европейский журнал передовых технологий ISSN 1729-3774-2015-№2, С. 55–59.

11. Pawan, C. Study of Wireless Networks and WMN Architecture [Electronic resours] / C. Pawan, Bangar, at all.. // International Journal of Engineering Innovation & Research. – Vol. 1, Is. 2. – 2012. – pp. 61–65. – Access Mode: https://ijeir.org/administrator/components/ com_jresearch/files/publications/IJEIR_45_Final.pdf

12. Raniwala, K. Centralized Channel Assignment and Routing Algorithms for Multi-Channel Wireless Mesh Networks. [Text] / K. Raniwala, T. Gopalan, C. Chiueh // Mobile Computing and Communication Review. Vol. 8, no. 2. – 2004. – pp. 50–65.

13. Abu Ali, N.A. IEEE 802.16 Mesh Schedulers: Issues and Design Challenges. [Text] / N. A. Abu Ali, A. E. M. Taha, H. S. Hassanein, H. T. Mouftah // IEEE Network. – 2008. –.Vol. 22, No. 1. – pp. 58–65.

14. Воробець, Г.І. Застосування моделей розсіювання Гауса та "хмарних" технологій для прогнозування розповсюдження домішок в атмосфері. [Текст] / Г. І. Воробець, М. І. Скрипський // Східно-Європейський журнал наукових досліджень. – 2013. – №6. – С.18–21.

15. Воробець, Г.І. Методика синтезу архітектури самореконфігуровних вбудованих комп'ютерних засобів технологічних кіберфізичних систем. [Текст] // Матеріали міжнародної наукової конференції «Проблеми інформатики і комп'ютерної техніки», ПІКТ'2015. – Чернівці, 26-29 травня 2015 р. – С.20–23.

16. Spartan-3A-3AN FPGA Starter Kit Board User Guide. UG334 (v1.1) June 19, 2008 [Electronic resours] – Access Mode: https://www.xilinx.com/support/documentation/boards_and_kits/ug334.pdf

References

1. Kozyrev, G., Nazarov, A. and Shitov, I. (2007). Modern telemetry in theory and practice. Training course. [Sovremennaya telemetriya v teorii i na praktike. Uchebnyiy kurs.] Moscow: Science and Technology, p.672.

2. Lee, E. and Seshia, S. (2011). Introduction to Embedded Systems. A Cyber-Physical Systems Ap-proach.. [ebook] Available at: https://ptolemy.berkeley.edu/books/ leeseshia/.

3. Vorobets, G. and Tarasenko, V. (2016). Self-configurable computer tools as the basis model of the telecommunicational self-organization of cyber-physics systems. [Camorekonfihurovni kompiuterni zasoby yak modelna osnova intelektualnoi samoorhanizatsii kiberfizychnykh system][online] Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua/. Available at: http://ena.lp.edu.ua:8080/bitstream/ ntb/39386/1/20-114-120.pdf [Accessed 25 Jun. 2018].

4. Mazurenko, M., Kharchenko, V. and Gorbenko, A. (2014). WEB-system dynamical reconfiguration based on metric analysis of vulnerability databases OTS-components. Radio electronic and computer systems, (5 (69).), pp. 135–139.

5. Palagin, A. V. and Opanasenko, V. M. (2011) Design and Application of the PLD-Based Reconfigurable Devic-es. Design of Digital Systems and Devices. Series: Lecture Note in Electrical Engineering, Vol. 79, pp. 59–91.

6. Vorobets, G. I. and Tarasenko, V. P. (2015) Application of the self-adaptive and self-reconfigurable computer devices for micro- and nanoelectronics. Radio electronic and computer systems, (1 (71)), pp. 143–148.

7. Vorobets, H., Vorobets, O., at al. (November, 2017). Self–reconfigurable cryptographical coprocessor for data streaming encryption in tasks of telemetry and the Internet of Things. Proceedings of the 2017 IEEE 9th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2017, (2), Bucharest; Romania; 21-23 September 2017. [online] 2, pp.1117–1120. Available at: https://ieeexplore.ieee.org/document/ 8095259/.

8. Hardware and software complex for collecting, transmitting and processing data of the telemetry system. [Apparatno-programmnyiy kompleks sbora, peredachi i obrabotki dannyih sistemyi telemetrii] Available at: http://radmirtech.com.ua/ processing-data-system-telemetry/

9. Murashov, V. A. and Zotov, A. V. Application of modern technology of data transmission during modernization of telemetry system [Primenenie sovremennyih tehnologiy peredachi dannyih pri modernizatsii sistemyi telemetrii]. [ebook] Available at: https://gaselectro.ru/stati/primenenie-sovremennyh-tehnologij-peredachi-dannyh-pri-modernizacii-sistemy-telemetrii.html

10. Vorobets, G. I., Gurzhu, R. D. and Kuz, M. A. Computerized system with reconfigurable architecture for environmental parameters monitoring. [Kompiuteryzovana systema z rekonfihurovanoiu arkhitekturoiu dlia monitorynhu parametriv dovkillia] The East European Journal of Advanced Technologies (2), pp. 55–59. ISSN 1729-3774-2015.

11. Pawan, C., Bangar, at all. (2012). Study of Wireless Networks and WMN Architec-

ture. International Journal of Engineering Innovation & Research, [online] 1(2), pp.61-65. Available at: https://ijeir.org/administrator/components/com_jresearch/files/publications/IJEIR_45_Final.pdf.

12. Raniwala, K., Gopalan, T. and Chiueh, C. Centralized Channel Assignment and Routing Algorithms for Multi-Channel Wireless Mesh Networks. Mobile Computing and Communication Review, 8(2), pp. 50–65.

13. Abu Ali, N. A., Taha, A. E. M., Hassanein, H. S., Mouftah, H. T. (2008) IEEE 802.16 Mesh Schedulers: Issues and Design Challenges. IEEE Network, 22(1), pp. 58–65.

14. Vorobets, G. I., Skrypsky, M. I. (2013) Application of Gaussian dispersion models and "cloud" technologies to predict the propagation of impurities in the atmosphere. [Zastosuvannia modelei rozsiiuvannia Hausa ta "khmarnykh" tekhnolohii dlia prohnozuvannia rozpovsiudzhennia domishok v atmosferi] East European Journal of Scientific Research, (6), pp. 18–21.

15. Vorobets, G. I. (2015) Methods of synthesizing the architecture of self-reconfigurable embedded computer tools of technological cyberphysical systems. [Metodyka syntezu arkhitektury samorekonfihurovnykh vbudovanykh kompiuternykh zasobiv tekhnolohichnykh kiberfizychnykh system] Materials of the international scientific conference "Problems of computer science and computer technology", PIKT'2015, Chernivtsi, May 26-29, pp. 20–23.

16. Spartan-3A-3AN FPGA Starter Kit Board User Guide. UG334 (v1.1) June 19, 2008 [Electronic resours] – Available at: https://www.xilinx.com/support/documentation/boards_and_kits/ug334.pdf

APPLICATION OF THE SYSTEM APPROACH FOR SYNTHESIS OF MODELS OF BASIC ELEMENTS OF RECONFIGURABLE STRUCTURES AT THE INFORMATION TRANSMISSION SYSTEMS

G. I. Vorobets, O. I. Vorobets, V. E. Gorditsa

Yuri Fedkovych Chernivtsi National University

Abstract. *For module-oriented technology of digital systems synthesis, the method of a system approach to the development and modeling of specialized encoders and stream encoders in computers with reconfigurable architecture has been improved. The mathematical model of the mapping of a set of states of a cyberphysical system by a set of performed computer components of procedures, functions, processes is substantiated. The generalized statement of the problem of system analysis for the search of the mini-max solution of the target function of synthesis of computer cyber components of the multitasking technical system is formulated. The peculiarity of the reasoned model is the use of 3D dimensional matrix for describing the quantitative parameters of the necessary basic logical structures of FPGA, or CPLD type, which allow to synthesize circuit solutions for the implementation of these processes, functions and procedures. The algorithm of search of the optimized programmable logical environment for the project realization is offered.*

The features of application of the proposed method for synthesis and simulation of a multi-mode streaming encoder, which can be used for data protection in systems that implement technologies of the Internet of things and cyberphysical systems, are described. An example of the use of the tools of the software package ISE WebPack of the company Xilinx for the construction of two-dimensional matrices and three-dimensional tensors to determine the coefficients of calculating the necessary resources of the programmable logical environment for the implementation of reconfiguration files of the synthesized multi task project.

It is shown that such an approach simplifies the choice of components, improves the technical and economic efficiency of the project by minimizing the resources used for its implementation, in particular the basic logical structures of programmable logical environments.

Keywords: *reconfigurable computer tools, signal code designs, flow-ve encryption, programmable logical environments, VHDL models, system analysis.*

ПРИМЕНЕНИЕ СИСТЕМНОГО ПОДХОДА ДЛЯ СИНТЕЗА МОДЕЛЕЙ БАЗОВЫХ ЭЛЕМЕНТОВ РЕКОНФИГУРИРУЕМЫХ СТРУКТУР В СИСТЕМАХ ПЕРЕДАЧИ ИНФОРМАЦИИ

Г. И. Воробец, А. И. Воробец, В. Е. Гордица

Черновицкий национальный университет имени Юрия Федьковича

Аннотация. *Для модуль-ориентированной технологии синтеза цифровых систем усовершенствована методика системного подхода к разработке и моделированию специализированных кодеров и потоковых шифраторов в компьютерных средствах с реконфигурируемой архитектурой. Обоснована математическая модель отображения набора состояний киберфизической системы множеством выполняемых компьютерной компонентой процедур, функций, процессов. Предложен алгоритм поиска оптимизированной программируемой логической среды для реализации проекта.*

Ключевые слова: *реконфигурируемые компьютерные средства, сигнально кодовые конструкции, потоковое шифрование, программируемые логические среды, VHDL модели, системный анализ.*

Отримано 29.06.2018

Воробець Георгій Іванович, кандидат фізико-математичних наук, доцент, завідувач кафедри комп'ютерних систем та мереж Чернівецького національного університету імені Юрія Федьковича. Вул. Коцюбинського, 2, Чернівці, Україна, 58012. E-mail: g.vorobets@chnu.edu.ua, тел. +38-0372-50-91-73

George Vorobets, PhD, Associate Professor, Head of the Department of Computer Systems and Networks, Yuriy Fedkovych Chernivtsi National University. 2, Kotsyubynskogo Str., Chernivtsi, Ukraine, 58012. E-mail: g.vorobets@chnu.edu.ua, phone: +38-0372-50-91-73

ORCID ID: 0000-0001-8125-2047

Воробець Олександр Іванович, кандидат фізико-математичних наук, доцент кафедри комп'ютерних систем та мереж Чернівецького національного університету імені Юрія Федьковича. Вул. Коцюбинського, 2, Чернівці, Україна, 58012. E-mail: o.vorobets@chnu.edu.ua, тел. +38-0372-50-91-73

Olexandr Vorobets, PhD, Associate Professor of the Department of Computer Systems and Networks, Yuriy Fedkovych Chernivtsi National University. 2, Kotsyubynskogo Str., Chernivtsi, 58012. Ukraine, E-mail: g.vorobets@chnu.edu.ua, phone: +38-0372-50-91-73

ORCID ID: 0000-0003-3195-8214

Гордіца Валентина Емануїлівна, асистент кафедри комп'ютерних систем та мереж Чернівецького національного університету імені Юрія Федьковича. Вул. Коцюбинського, 2, Чернівці, Україна, 58012. E-mail: v.horditsa@chnu.edu.ua, тел. +38-0372-50-91-73

Valentyna Horditsa, Assistant of Professor, Department of Computer Systems and Networks, Yuriy Fedkovych Chernivtsi National University. 2, Kotsyubynskogo Str., Chernivtsi, Ukraine, 58012. E-mail: g.vorobets@chnu.edu.ua, phone: +38-0372-50-91-73

ORCID ID: 0000-0003-4548-2536