УДК 004.75

Л.О. ДУБЧАК
Тернопільський національний економічний університет

ЗАСІБ РОЗПОДІЛУ ДОСТУПУ ДО ІНФОРМАЦІЙНИХ РЕСУРСІВ КОМП'ЮТЕРНОЇ СИСТЕМИ

В статті представлено реалізацію засобу розподілу доступу до інформації комп'ютерної системи за допомогою "Spartan-3 Starter Kit", що містить ПЛМ Spartan-3 обсягом 200 тисяч логічних елементів. Даний засіб побудований на основі запропонованого автором методу на основі нечіткої логіки. Дослідження синтезованої структурної схеми запропонованого засобу підтвердили його працездатність та можливість застосування у сучасних комп'ютерних системах з метою розподілу доступу до інформаційних ресурсів.

Ключові слова: захист інформації, нечітка система, HDL-модель, ПЛМ Spartan-3.

L.O. DUBCHAK
Ternopil National Economic University

MEANS OF ACCESS DISTRIBUTION TO COMPUTER SYSTEMS' INFORMATION RESOURCES

Abstract – the aim of this article is the development and researching of means of access distribution to the information resources of the computer system.

For the construction of means of access distribution the fuzzy system based on the classic mechanism of fuzzy conclusion of Мамдані is offered. However, this method is quicker due to dividing of all process of working of fuzzy data into the stages of studies and exploitation. The means of access distribution that works on the offered method are realized by means of "Spartan - 3 Starter Kit", that contains 200 thousand logical elements. Realization is carried out in language of VHDL by facilities of environment of ISO of a 10.3 planning of firm Xilinx.

Undertaken researching confirmed a capacity and acceptable fast-acting of the worked out means of access distribution to the informative resources in computer system.

Keywords: information security, fuzzy system, HDL-model, Spartan-3.

Вступ

Основними критеріями працездатності комп'ютерної системи є висока продуктивність, оптимальні затрати пам'яті та стійкість до атак зловмисника.

Будь-яка комп'ютерна система може бути захищена від активних атак зловмисників, які можна виявити в процесі експлуатації завдяки відомим заходам політики безпеки [1]. Проте, існує також можливість виникнення пасивних атак (атака часового аналізу чи аналізу енергоспоживання), які можуть здійснюватись віддалено і тому їх важко виявити [2, 3].

Комп'ютерна система при передачі інформації використовує мережу для здійснення доступу клієнтів. Таку мережу передачі даних можна умовно розділити на захищену та незахищену частини.

У незахищеній частині мережі клієнти можуть бути випадковими, тому вони не є надійними для сервера з точки зору безпеки, тобто є велика ймовірність існування зловмисника. Крім того, ця частина мережі, як правило, не захищена від збоїв внаслідок впливів зовнішнього середовища і є відкритою для проведення всіх видів сучасних атак на реалізацію.

У захищеній частині мережі клієнти вважаються надійними і, завдяки політиці безпеки, виключається існування внутрішнього зловмисника. Проте в цій частині мережі все-таки залишається можливість проведення пасивної атаки часового аналізу [2].

Сервер комп'ютерної системи можна умовно поділити на підсистему ідентифікації клієнта, командну підсистему та блок оброблення інформації.

Підсистема ідентифікації клієнта подає на блок оброблення інформації дані про необхідний рівень стійкості до часового аналізу, враховуючи усі дані про користувача.

Клієнти мережі відомі серверу по IP-адресі і, враховуючи «стаж» користування мережею, мають свій рівень довіри, що можна задати ймовірністю збоїв при передачі пакетів інформації.

Отже, якщо клієнт є новим для даної системи або має рівень довіри дуже низький, то необхідний рівень стійкості до часового аналізу повинен бути максимальним, тобто, наприклад, рівним 1. І навпаки, для клієнта з дуже високим рівнем довіри значення стійкості може прямувати до 0, що забезпечить підвищення швидкодії системи.

Щодо незахищеної частини мережі, то можна застосувати відомі рекомендації стосовно підвищення стійкості до часового аналізу [2].

Командна підсистема сервера подає на блок оброблення інформацію про саму комп'ютерну систему, тобто допустимі затрати пам'яті та необхідний рівень продуктивності.

Для захисту інформації у мережі необхідно оптимально вибрати метод піднесення до степеня за модулем для здійснення шифрування інформації чи проведення аутентифікації клієнта за допомогою криптоалгоритму RSA. Це завдання вирішує блок оброблення інформації, побудований на основі нечіткої логіки, а саме, на механізмі нечіткого висновку Мамдані, описаному у [4]. Він опрацьовує вхідні значення продуктивності, затрат пам'яті та стійкості до часового аналізу і подає оптимальний у кожному випадку метод модулярного експоненціювання на командну підсистему, яка в свою чергу, застосовує його для шифрування інформації. Основною перевагою цього блоку є те, що він працює в режимі реального часу, що забезпечує вищу

стійкість системи від атак зловмисника, оскільки він не буде достовірно знати алгоритму шифрування [5-7].

Блок оброблення інформації на основі нечіткої логіки є основою системи захисту комп'ютерної системи. На його вхід поступають критерії вибору методу модулярного експоненціювання, серед яких необхідний рівень стійкості до часового аналізу, продуктивності криптосистеми та допустимі затрати пам'яті сервера. Вхідні нечіткі дані опрацьовуються підсистемою оптимального вибору методу піднесення до степеня за модулем на основі механізму нечіткого висновку за механізмом Мамдані. Виходом блоку оброблення інформації є метод модулярного експоненціювання, що забезпечує оптимальну конфігурацію системи захисту відносно значень вхідних критеріїв вибору.

Метод оптимального вибору алгоритму модулярного експоненціювання

На блок оброблення інформації сервера системи захисту КС поступає нечітка інформація про необхідний рівень продуктивності та стійкості до часового аналізу, а також про допустимі затрати пам'яті. Система в режимі реального часу опрацьовує ці дані за допомогою відомого алгоритму нечіткого висновку Мамдані, як це описано вище.

Детальний опис та реалізація запропонованого методу оптимального вибору алгоритму медулярного експоненціювання засобами Fuzzy Logic Toolbox середовища MATLAB подані в [8].

Основний недолік нечіткого висновку, побудованого на класичному механізмі Мамдані, полягає в тому, що для будь-яких вхідних даних необхідно опрацьовувати усю базу правил. Такий шлях оброблення нечітких даних знижує швидкодію системи та вимагає великих затрат пам'яті, тому варто вдосконалити метод вибору методу модулярного експоненціювання [9], що базується на класичному методі Мамдані, який би задовольняв вимоги до швидкодії.

Суть пропонованого методу вибору методу піднесення до степеня за модулем полягає в тому, що процес оброблення вхідної нечіткої інформації розділено на етапи навчання та експлуатації.

Під час навчання засобу оброблення нечіткої інформації визначено області функцій належності виходу для кожного з правил.

Під час експлуатації спочатку відбувається порівняння вхідних даних зі значеннями функцій належності виходу у визначених базою правил областях пам'яті, де зберігаються значення згаданих функцій належності виходу, відповідних до кожного правила нечіткого висновку. Далі відсікаються значення функцій належності виходу, які перевищують вхідні дані. Потім вибираються мінімальні значення функцій належності виходу, отриманих після відсікання, і будується з цих мінімальних значень відповідна фігура. Останньою операцією методу оброблення нечітких даних є пошук центра ваги фігури, отриманої в результаті додавання відсічених функцій належності виходу [10].

Порівняння операцій пропонованого методу оброблення нечіткої інформації та класичного механізму Мамдані під час експлуатації наведені в таблиці 1.

Таблиця 1

Операції з оброблення нечіткої інформації

№ п/п	Операції нечіткого висновку за класичним механізмом Мамдані	Операції нечіткого висновку пропонованого методу	
		Співпадаючі операції пропонованого методу	Нові операції пропонованого методу
1	Порівняння вхідних даних зі значеннями функцій належності входів	–	Порівняння вхідних даних зі значеннями функцій належності виходів у відповідних областях ПЗП
2	Знаходження найменшого значення функцій належності входів щодо кожного з входів, які відповідають базі правил	–	–
3	Відсікання на осі ординат функцій належності виходу значень, які перевищують значення, знайдені в п. 2	–	Відсікання на осі ординат функцій належності виходу в усіх відповідних областях багатоканального блоку пам'яті значень, які перевищують значення, знайдені в п. 1
4	Знаходження серед відсічених функцій належності виходу тих, що мають максимальну амплітуду	–	Знаходження серед відсічених функцій належності виходу у всіх відповідних областях багатоканального блоку пам'яті тих, що мають мінімальну амплітуду
5	Знаходження суми знайдених в п. 4 значень відсічених функції належності виходу, що утворює кінцеву фігуру	Знаходження суми знайдених в п. 4 значень відсічених функції належності виходу, що утворює кінцеву фігуру	–
6	Знаходження центра ваги отриманої в п. 5 фігури	Знаходження центра ваги отриманої в п. 5 фігури	–

Як видно з таблиці 1, всі операції пропонованого методу близькі до операцій класичного механізму Мамдані і за складністю не перевищують їх. Однак кількість операцій у пропонованому методі менша, що спричиняє зростання його швидкодії. Зменшення кількості операцій зумовлено тим, що на етапі навчання (який передує етапу експлуатації) визначено області функцій належності виходу для кожного з правил. Результати записано у відповідні області багатоканального блоку пам'яті, звідки вони вибираються при виконанні операцій пп. 3, 4 таблиці 1. Така попередня підготовка власне й дозволяє уникнути операції, передбаченої в п. 2 методу Мамдані.

Реалізація даного методу опрацювання нечітких даних дозволяє здійснити розподіл доступу до інформаційних ресурсів комп'ютерної системи.

На етапі навчання засобу реалізації пропонованого методу оброблення нечітких даних, відповідно до областей функцій належностей входів та вхідних даних, однозначно визначаються області функцій належності виходу (тобто відповідних до цих функцій належності виходу методів модулярного експоненціювання) згідно бази правил нечіткого висновку Мамдані. Отримані значення, які відповідають ординатам визначених функцій належності виходу, записуються у відповідних областях багатоканального блоку пам'яті.

На етапі експлуатації засобу, коли задані значення вхідних даних, опрацьовуються лише ті області функцій належності виходу, які відповідають записаним областям функцій належностей входів згідно бази правил нечіткого висновку.

Реалізація запропонованого засобу розподілу доступу

Дослідження ефективності роботи пропонованого засобу розподілу доступу за описаним вище методом здійснено за допомогою "Spartan-3 Starter Kit", що містить ПЛМ Spartan-3 обсягом 200 тисяч логічних елементів [11]. Реалізацію здійснено на мові VHDL засобами середовища ISO 10.3 проектування фірми Xilinx. З цією метою проект засобу розподілу доступу на основі нечіткої логіки розділено на 3 основні модулі – модуль реалізації блоку керування (Control Unit), блоку обробки нечіткої інформації (Processing Unit) та блоку знаходження центра ваги, тобто здійснення нечіткого висновку (ROM). Структурна схема спроектованого засобу подана на рисунку 1.

За цією схемою входи data_in_0, data_in_1 та data_in_2 відповідають вхідним значенням продуктивності, стійкості до часового аналізу та допустимих затрат пам'яті, відповідно. Ці значення поступають безпосередньо з сервера, де вони попередньо обробляються. Вхід start_processing та вихід end_processing здійснюють дозвіл на обробку нечітких даних та завершення роботи засобу, відповідно. Виходи блоку Control Unit address_mem, K2 і K3 позначають адресу та керуючі сигнали, що є виходами блоку керування сервера. Сигнал wr_en здійснює дозвіл на запис значень у регістри пам'яті сервера.

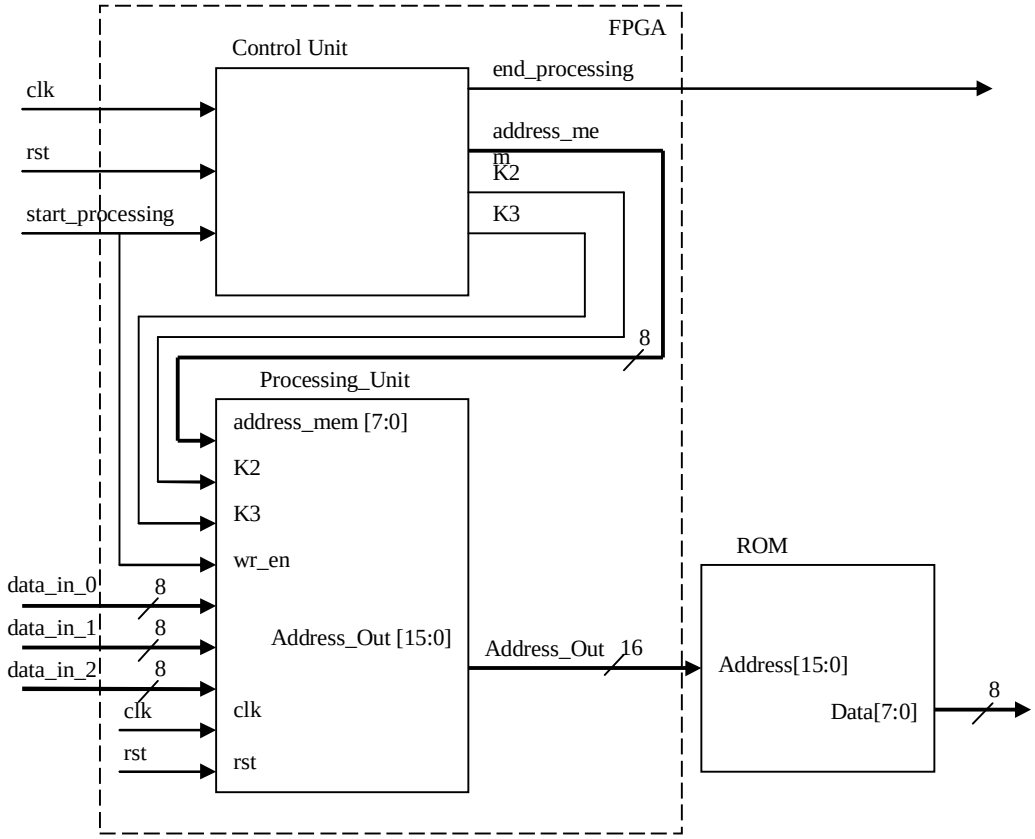

Рис. 1. Структурна схема засобу розподілу доступу на основі нечіткої логіки

Структурна схема блоку керування Control Unit подана на рисунку 2. У цій схемі RS_FF відповідає тригеру, Counter_1 та Counter_2 – лічильникам, відповідно. Logical circuits виконує роль дешифратора, виходами якого є керуючі сигнали. Виходом блоку Parraller_Reg є код адреси набору значень функцій належності входу.

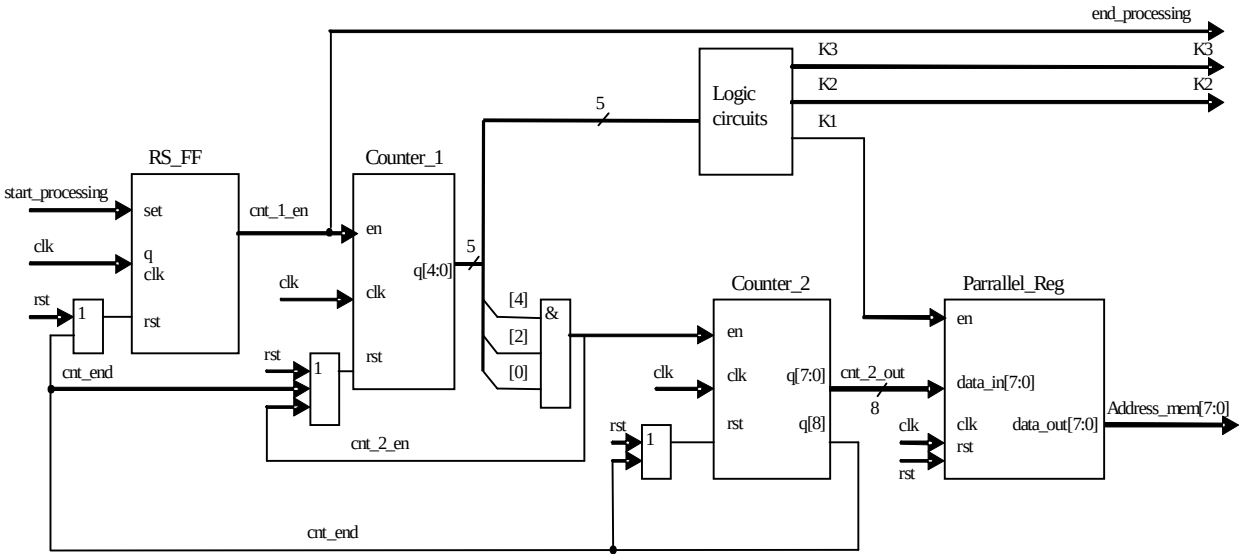

Рис. 2. Структурна схема блоку керування

В загальному HDL-проект засобу розподілу доступу шляхом вибору методу модулярного експоненціювання складається з наступних модулів:

- control unit – блок керування (див. рис. 1);
- memory unit – модуль виводу коду адреси запису даних у постійний запам'ятовуючий пристрій (ПЗП);
- compare cor – модуль порівняння вхідних даних із даними, що зберігаються в ПЗП;
- adder – модуль роботи суматора;
- min–operand – знаходження мінімального значення;
- multiplier – модуль виконання множення;
- parallel_reg – модуль виводу коду адреси набору значень функцій належності входу (див. рис. 2);
- modular_exponentiation – модуль знаходження методу модулярного експоненціювання;
- processing unit – блок опрацювання даних.

Результати симуляції роботи засобу розподілу доступу в комп'ютерних системах на основі нечіткої логіки на базі налагоджувальної плати Spartan-3 Starter Kit (xc3s200-4-ft256) подані в таблиці 2.

Таблиця 2

Витрати на реалізацію засобу

Параметр	Значення
Апаратні затрати	
Кількість слайдів	121 з 1920 (6%)
Кількість тригерів	103 з 3840 (2%)
Кількість 4-входових LUT, з них в якості ПЗП	549 з 3840 (14%), 384
Кількість ліній вводу-виводу	44
Часовий аналіз	
Мінімальний період виконання	32.053ns
Максимальна частота	31.198MHz
Час затримки у логічних схемах засобу	20.023ns (62,5 %)
Час проходження (затримки) у лініях зв'язку та вхідних і вихідних шинних формувачах	12.030ns (37,5 %)

Аналіз таблиці 2 показує, що в загальному апаратні затрати прийнятні для застосування пропонованого засобу в комп'ютерних системах. При цьому доцільно апаратно реалізувати в цій же ПЛМ інші вузли, що відносяться до системи захисту.

Висновки

У даній статті запропонована структура сервера комп'ютерної мережі, що дає можливість

забезпечити оптимальну його роботу шляхом розподілу доступу до інформаційних ресурсів.

Автором також описано метод оброблення нечітких даних для налаштування сервера комп'ютерної системи, який забезпечує його вищу швидкодію, ніж класичний механізм нечіткого висновку Мамдані.

Крім того, синтезовано структурну схему засобу визначення методу модулярного експоненціювання та проведено дослідження його роботи, що підтвердили його працездатність та можливість застосування у комп'ютерних системах з метою розподілу доступу до інформаційних ресурсів.

Література

1. Васильцов І.В.Атаки спеціального виду на криптопристрої та методи боротьби з ними / І.В.Васильцов ; за ред. В.П.Широчина. – Кременець: Видавничий центр КОГПІ, 2009. – 264 с.

2. Васильцов І.В. Методи захисту проти атак спеціального виду / І.В.Васильцов, Л.О.Дубчак // Вісник Хмельницького національного університету. Технічні науки. – 2007. – №5. – С.174-182.

3. Quisquater J.-J. Side Channel Attacks [Електронний ресурс] / J.-J.Quisquater, F.Koeune.// State-of-the-art regarding side channel attacks: report, October, 2010. – 2010. – 47 p. - Режим доступу до звіту: http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/1047_Side_Channel_report.pdf

4. Штовба С.Д. Обеспечение точности и прозрачности нечеткой модели Мамдани при обучении по экспериментальным данным / С.Д.Штовба // Проблемы управления и информатики. – 2007. – №4. – С. 102–114.

5. Петров А.О. Принципи проектування та оцінки систем захисту інформації в мережах загального користування / А.О.Петров // Інформаційна безпека. – 2011. – №1(5). – С.49-56.

6. Patent US 2010/0177887A1, Int.Cl. H04L9/28. Montgomery-based modular exponentiation secured against hidden channel attacks / M.Ciet, B.Feix; Gemalto SA (FR). – № 12/666,892; заявл. 02.05.2008; опубл. 15.07.2010.

7. Patent US 7,020,281B2, Int.Cl. H04L9/00. Timing attack resistant cryptographic system / A.Vadekar, R.J.Lambert; Certicom Corp. (CA). – № 09/761,700; заявл. 25.10.2001; опубл. 28.03.2006.

8. Дубчак Л.О. Модель апаратного засобу вибору методу модулярного експоненціювання / Л.О.Дубчак // Науковий вісник Чернівецького національного університету імені Юрія Федьковича. Серія: Комп'ютерні системи та компоненти. – 2011. – Т. 2, вип. 4. – С.44-48.

9. Дубчак Л.О. Спосіб вибору методу модулярного експоненціювання для побудови оптимальної системи захисту конфіденційної інформації / Л.О.Дубчак, Л.М.Тимошенко, Т.О.Яремчук // Інформаційна безпека. – 2011. - №1(5). – С.112-116.

10. Дубчак Л.О. Метод обробки нечітких даних на основі механізму Мамдані /Л.О.Дубчак // Системи обробки інформації. – 2012. – №7(105). – С.131-134.

11. Spartan-3 Generation FPGA User Guide. Extended Spartan-3A, Spartan-3E, and Spartan-3 FPGA Families. UG331 [Електронний ресурс] // Xilinx Inc. – 2011. – Rev.1.8. - Режим доступу до інструкції користувача- http://www.xilinx.com/support/documentation/user_guides/ug331.pdf.

References

1. Vasyltsov I.V. Ataky spetsialnogo vydu na kryptoprystroi ta metody borotby z nymy / za red. V.P.Shyrochyna – Kremenets: Vydavnychyi tsentr KOGPI, 2009. – P. 264

2. Vasyltsov I.V., Dubchak L.O. Metody zakhystu proty atak spetsialnogo vydu // Visnyk Khmelnytskogo natsionalnogo universytetu. Technical sciences. Khmelnitsky. 2007. Volume 5. Pp. 174-182.

3. Quisquater J.-J. Side Channel Attacks [Electronic resource] / J.-J.Quisquater, F.Koeune.// State-of-the-art regarding side channel attacks: report, October, 2010. – 2010. – 47 p. Web resource: http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/1047_Side_Channel_report.pdf

4. Shtovba S.D. Obespechenie tochnosti I prozrachnosti nechetkoi modeli Mamdani pri obuchenii po eksperimentalnym danym // Problemy upravleniya I informatiki. 2007. Volume 4. Pp. 102–114.

5. Petrov A.O. Printsypy proektuvannya ta otsinky system zahystu informatsii v meregakh zagalnogo korystuvannya // Informatsiyna bezpeka. 2011. Volume 1(5). Pp.49-56.

6. Patent US 2010/0177887A1, Int.Cl. H04L9/28. Montgomery-based modular exponentiation secured against hidden channel attacks / M.Ciet, B.Feix; Gemalto SA (FR). – № 12/666,892; decl. 02.05.2008; publ. 15.07.2010.

7. Patent US 7,020,281B2, Int.Cl. H04L9/00. Timing attack resistant cryptographic system / A.Vadekar, R.J.Lambert; Certicom Corp. (CA). – № 09/761,700; decl. 25.10.2001; publ. 28.03.2006.

8. Dubchak L.O. Model aparatnogo zasobu vyboru metodu modulyarnogo eksponentsiyuvannya // Naukovyj visnyk Chernivetskogo natsionalnogo universytetu imeni Yuriya Fedkovycha. Kompyuterni systemy ta komponenty. 2011. Volume 4. Part 2. Pp.44-48.

9. Dubchak L.O., Tymoshenko L.M., Yaremchuk T.O. Sposib vyboru metodu modulyarnogo eksponentsiyuvannya dlya pobudovy optymalnoi systemy zakhystu konfidentsijnoi informatsii // Informatsijna bezpeka. 2011. Volume №1(5). Pp.112-116.

10. Dubchak L.O. Metod obrobky nechitkykh danykh na osnovi mekhanizmu Mamdani // Systemy obrobky informatsii. 2012. Volume №7(105). Pp.131-134.

11. Spartan-3 Generation FPGA User Guide. Extended Spartan-3A, Spartan-3E, and Spartan-3 FPGA Families. UG331 [Electronic resource]// Xilinx Inc. - 2011. – Rev.1.8. – Web resource: http://www.xilinx.com/support/documentation/user_guides/ug331.pdf.

Рецензія/Peer review : 12.3.2015 р. Надрукована/Printed :15.5.2015 р.
Рецензент: д.т.н., проф. Березький О.М.