

ВІДГУК

офіційного опонента на дисертаційну роботу Гільгурта Сергія Яковича «Методи та засоби створення реконфігурованих сигнатурних засобів захисту інформації комп'ютерних систем і мереж», подану на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти

Актуальність теми.

Поява кристалів ПЛІС типу FPGA, які представляють собою несконфигуроване функціональне поле універсальних логічних елементів, дозволило вирішити питання апаратної реалізації алгоритмів шляхом зміни структури кристала на виконання необхідного алгоритму. Завдяки високим технічним характеристикам системи на базі програмованої логіки дозволяють в тому числі створювати ефективні технічні засоби інформаційної безпеки.

Збільшення об'ємів мережевого трафіку та зріст зловмисної активності останніми роками потребують розробки все більш ефективних засобів технічного захисту інформації, зокрема, реконфігурованих. Одним зі шляхів підвищення продуктивності таких засобів є об'єднання в одному пристрої різних схем розпізнавання з одночасним виконанням оптимізації всього пристрою за заданими критеріями. Але вирішення даної задачі неможливо без розробки швидких методів оцінки та порівняння варіантів побудови обчислювальної схеми.

Таким чином, дана дисертаційна робота, яка присвячена вирішенню важливої науково-прикладної проблеми розробки та розвитку методів побудови комбінованих обчислювальних структур для підвищення ефективності реконфігурованих сигнатурних технічних засобів захисту інформації, є *актуальною*.

Зв'язок дисертаційної роботи з науковими програмами, планами, темами. Дисертаційна робота виконувалась згідно плану науково-дослідних робіт Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України у рамках тематики НАН України, а також низки конкурсних наукових проектів щодо підтримки грид-сайту ІПМЕ ім. Г.Є. Пухова НАН України та створення і модернізації грид-сервіса централізованого синтезу конфігурацій для апаратних прискорювачів задач інформаційної безпеки в енергетичній галузі згідно Цільової комплексної програми наукових досліджень НАН України «Грид-інфраструктура і грид-технології для наукових і науково-прикладних застосувань» та Програми інформатизації НАН України.

ІПМЕ № 355
07.12.2020р.

Наукова новизна та теоретична цінність результатів. В дисертаційній роботі виконано теоретичне обґрунтування та отримано нове рішення актуальної науково-прикладної проблеми, що полягає в розробці та розвитку методів побудови комбінованих обчислювальних структур для підвищення ефективності реконфігурованих сигнатурних технічних засобів захисту інформації.

Наукова новизна відображена у наступних отриманих результатах, які мають теоретичну цінність:

- Метод прискореного обчислення технічних характеристик компонентів реконфігурованих сигнатурних засобів інформаційного захисту, який дозволяє швидко знаходити цільові функції для процедур оптимізації завдяки тому, що не потребує виконання витратних за часом процедур синтезу цифрових схем. Метод дозволяє також за рахунок формування математичного опису здійснювати оцінку та порівняння обчислювальних структур за визначеними параметрами.

- Метод прискорення процедури оптимізації паралельного комбінування, який завдяки впорядкуванню патернів в наборі за певним параметром дозволяє замість повного перебору завеликої кількості варіантів здійснювати поділ патернів за лінійний час. В результаті метод зменшує обчислювальну складність процесу оптимізації, а відтак і час розрахунків до прийнятних для практичного використання значень.

- Формалізація методу паралельного комбінування, який за рахунок паралельного з'єднання різнорідних блоків розпізнавання підвищує показники ефективності компонентів розпізнавання реконфігурованих сигнатурних засобів інформаційного захисту. Запропонований принцип комбінування надає можливість застосування розроблених методів прискорення, що знижує часові витрати на процес оптимізації до прийнятних для практичного використання значень.

- Формалізація методу послідовного каскадування, який за рахунок послідовного з'єднання різних за принципами побудови блоків розпізнавання та уточнення попереднього розпізнавання, використовуючи процедуру оптимізації поділу між ними питомих патернів по довжині, дозволяє підвищити показники ефективності модулю розпізнавання реконфігурованих сигнатурних засобів інформаційного захисту. Запропонований принцип комбінування надає можливість застосування розроблених методів прискорення, що знижує часові витрати на процес оптимізації до прийнятних для практичного використання значень.

- Розвиток методу сполучання в одному блоці кількох підходів або

технічних рішень з метою підвищення ефективності модулю розпізнавання реконфігурованих сигнатурних засобів інформаційного захисту. Використання запропонованої багатовимірної таблиці сумісності дозволяє формалізувати наявний досвід та спростити процедуру оптимізації вибору найбільш ефективною за наданих умов комбінації підходів або технічних рішень.

- Формалізація принципу комбінування методів комбінування, який за рахунок ієрархічного використання сформульованих, вдосконалених та розвинутих методів комбінування дозволяє підвищити показники ефективності модулю розпізнавання реконфігурованих сигнатурних засобів інформаційного захисту до значень, недосяжних при використанні кожного з методів комбінування окремо. Запропонований принцип також надає можливість застосування розроблених методів прискорення для зниження часових витрати на процес оптимізації до прийнятних для практичного використання значень.

Визначені основні наукові результати є *новими*.

Теоретичне значення роботи полягає у розвитку теоретичних основ та методів побудови високоефективних апаратних засобів технічного захисту інформації, які забезпечили підвищення продуктивності таких засобів за рахунок комбінування різних підходів до пізнання та їх модифікацій, а також за рахунок ефективного поводження з сигнатурними базами даних.

Практичне значення отриманих результатів полягає в можливості застосування запропонованих методів побудови реконфігурованих сигнатурних технічних засобів захисту інформації для створення більш ефективних засобів захисту з метою протидії зовнішнім та внутрішнім атакам на комп'ютерні системи та мережі. Здобуті результати також можуть бути використані в галузях штучного інтелекту та молекулярного аналізу.

Основні наукові результати дисертаційної роботи використано при виконанні комерційного проекту по створенню Системи автоматизації магістрального нафтопродуктопроводу "Полоцьк-Фаніполь" сумісно з вітчизняними розробниками з ТОВ «ГЕРАКС-К». Впровадження результатів наукової роботи дозволило знизити сукупну вартість володіння та підвищити рівень захисту інформації створюваної автоматизованої системи.

Результати, які стосуються підвищення ефективності реконфігурованих засобів захисту інформації впроваджено в навчальний процес закладів вищої освіти України. Зокрема, Методика побудови сигнатурних засобів захисту інформації на базі ПЛІС ознайомлює студентів з принципами побудови, класифікацією та основними показниками пристроїв прискорення обчислень на базі ПЛІС, а Методика підвищення ефективності реконфігурованих сигнатурних засобів захисту інформації комп'ютерних систем і мереж ознайомлює студентів з підходами до створення реконфігурованих апаратних

засобів прискореного вирішення ресурсномісткої задачі множинного розпізнавання рядків у сигнатурних системах захисту інформації.

Результати дисертаційної роботи також включено в програми, що підготовлено в рамках проекту ЄС «Інтернет речей: нова навчальна програма для потреб промисловості та суспільства», шифр ALIOT.

Результати дисертаційної роботи використано при виконанні науково-дослідних проектів в Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, у яких дисертант приймав безпосередню участь. Методологічні й наукові результати дисертаційної роботи також отримали використання у Національному аерокосмічному університеті ім. М.Є. Жуковського «ХАІ», в Національному авіаційному університеті та в Київському національному університеті ім. Тараса Шевченка.

Створена за безпосередньою участю дисертанта централізована система синтезу реконфігурованих пристроїв захисту інформації на базі гріду та хмарної інфраструктури отримала високу оцінку спеціалістів Лундського університету (Швеція), який є членом північноєвропейського консорціуму NorduGrid – розробника проміжного програмного забезпечення для грід-інфраструктури ARC.

Відповідні акти впровадження та лист підтримки наведено у Додатках дисертаційної роботи.

Обґрунтованість та достовірність отриманих результатів. Отримані результати є обґрунтованими та достовірними, це підтверджується значним обсягом здійснених досліджень, поданим фактичним матеріалом та його науковою інтерпретацією, практичним використанням запропонованих розробок та апробацією на наукових конференціях й семінарах.

У роботі коректно застосовано основні положення теорії обчислювальних систем, апарат булевої алгебри, теорія автоматів, теорія обчислень на рядках, елементи теорій графів, множин, комбінаторики та алгоритмів, методи комп'ютерного моделювання.

Достовірність висновків та рекомендацій підкріплена результатами обчислювальних експериментів і науковими публікаціями.

Оцінюючи зміст дисертаційної роботи в цілому, слід відмітити її обґрунтованість та практичну спрямованість, внутрішню єдність матеріалу. У цілому поставлені в розглянутій дисертації завдання вирішені повністю. Здобувачем у дисертації отримані науково обґрунтовані результати, які в сукупності розв'язують актуальну науково-прикладну проблему розробки та розвитку методів побудови комбінованих обчислювальних структур для підвищення ефективності реконфігурованих сигнатурних технічних засобів

захисту інформації. Дисертаційна робота оформлена згідно вимогам до докторських дисертацій.

Повнота викладу результатів роботи в опублікованих працях. Основні результати дисертації з достатньою повнотою відображено в 52 наукових роботах, які відповідають вимогам до опублікування результатів дисертацій, у тому числі: 30 – у наукових фахових журналах та збірниках наукових праць, з яких 6 – у наукових журналах, що індексуються міжнародними наукометричними базами даних, 21 публікація у працях і матеріалах наукових конференцій, один патент, 31 публікацію підготовлено одноосібно, англійською мовою – 3 публікації.

Аналіз внеску автора в сумісні публікації по питаннях, висвітлених в дисертації, показав, що внесок Гільгурта С.Я. є вирішальним.

Рекомендації щодо використання результатів. Отримані автором результати можуть бути використані при створенні централізованих систем інформаційного захисту комп'ютерних та мережевих інфраструктур як для підприємств та організацій, орієнтованих на використання інформаційних технологій, так і для промислових об'єктів, зокрема, для енергетичних підприємств України. Здобуті результати доцільно також використовувати в навчальному процесі, зокрема при викладанні курсів, пов'язаних з високопродуктивною обробкою даних та системами захисту інформації.

Автореферат повною мірою відображає зміст і основні положення дисертаційної роботи.

Недоліки дисертаційної роботи. Разом з тим дисертаційна робота має і ряд недоліків, серед яких необхідно відзначити наступні:

1. У розділі 1 дисертації не досить строго виявлено недоліки результатів попередніх досліджень з напрямку підвищення ефективності реконфігурованих засобів технічного захисту інформації.
2. Частку матеріалів об'ємного підрозділу 4.6. "Реалізація функцій оцінки для деяких схем розпізнавання" було б доцільно винести у додатки.
3. Введені автором визначення та твердження не відокремлені та не пронумеровані в тексті.
4. Прив'язка запропонованих методів до конкретної структури ПЛІС унеможлиблює їх застосування при використанні ПЛІС з іншими архітектурами.
5. Коефіцієнти нормалізації α , β та γ , які дозволяють звести облік ресурсів різного типу до єдиної одиниці виміру, автор відносить до властивостей реконфігурованого прискорювача, що не є коректним.

Зроблені зауваження суттєво не знижують якість виконаних автором наукових досліджень.

Загальний висновок по дисертації. Дисертація є завершеною науково-дослідною роботою, у якій отримано розв'язання актуальної науково-прикладної проблеми розробки та розвитку методів побудови комбінованих обчислювальних структур для підвищення ефективності реконфігурованих сигнатурних технічних засобів захисту інформації.

Робота є *актуальною*, містить *нові наукові результати*, автором дотримано цілісність підходу.

Дисертаційна робота за темою «Методи та засоби створення реконфігурованих сигнатурних засобів захисту інформації комп'ютерних систем і мереж» є завершеним науковим дослідженням, відповідає вимогам пп. 9, 10 «Порядку присудження наукових ступенів», затвердженого постановою Кабінету Міністрів України № 567 від 24 липня 2013 р. (зі змінами), а її автор – Гільгурт Сергій Якович заслуговує присудження наукового ступеня доктора технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти.

ОФІЦІЙНИЙ ОПОНЕНТ



Провідний науковий співробітник
відділу мікропроцесорної техніки
Інституту кібернетики
ім. В.М. Глушкова НАН України,
доктор технічних наук, професор

Опанасенко В.М.