ВІДГУК

офіційного опонента про дисертаційну роботу Гільгурта Сергія Яковича «Методи та засоби створення реконфігуровних 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

1. Актуальність теми дисертаційної роботи та її зв'язок з науковими програмами, планами, темами

В останні роки відбувається значне збільшення обсягів інформації, що накопичується, зберігається та оброблюється за допомогою інформаційних систем. При цьому концентрування в єдиних базах даних інформації різного призначення та різної належності і різке розширення кола користувачів, що мають безпосередній доступ до ресурсів інформаційної системи, породжують проблему забезпечення їх захисту від різного роду вторгнень. Зростання складності апаратно-програмних засобів та існуючі недоліки сучасних ІТ призводять до постійного збільшення методів зламу захисту і, як наслідок, до вторгнення в інформаційну систему з метою порушення її нормального функціонування. Особливо гостро постає проблема забезпечення інформаційної безпеки об’єктів критичної інфраструктури, зокрема, в енергетичній галузі. Злам захисту таких об’єктів призводить не тільки до значних матеріальних втрат, але також погрожує катастрофічними екологічними наслідками, несе загрозу здоров’ю та життю людини.

Програмні засоби технічного захисту інформації не завжди можуть забезпечити потрібний рівень безпеки, особливо систем зі швидкоплинними процесами. Тому актуальним завданням стає розробка апаратних засобів захисту інформації. Перспективною платформою для таких засобів є ПЛІС завдяки їх технологічності та можливостям реконфігурування. Тому вибір предмету дисертаційного дослідження – реконфігуровні апаратні сигнатурні засоби технічного захисту інформації в комп’ютерних системах і мережах, та визначення мети дослідження – підвищення ефективності реконфігуровних сигнатурних технічних засобів захисту інформації в комп’ютерних системах і мережах є обґрунтованими та відповідають темі дисертаційної роботи.

Тема досліджень та одержані результати відповідають планам наукової діяльності Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України у рамках тематики НАН України і безпосередньо пов’язані з науково-дослідними роботами «Дослідження та розробка методів оцінювання захищеності інформації в розподілених високопродуктивних інформаційних

системах при вирішенні задач енергетики» (ДР № 0114U002361), «Розвиток теорії, розробка новітніх інформаційних технологій в задачах комплексного моделювання та управління процесами перетворення та використання енергії» (ДР № 0117U004347) та проектами Цільової комплексної програми наукових досліджень НАН України «Грід-інфраструктура і грід-технології для наукових і науково-прикладних застосувань» та Програми інформатизації НАН України (ДР № 0115U002876, № 0116U006907, № 0118U001370, № 0119U001812).

Таким чином, усе сказане обумовлює актуальність теми дисертаційної роботи Гільгурта С.Я. і наукову новизну сформульованих в ній задач досліджень.

2. Наукова новизна результатів роботи

У результаті виконання дисертаційної роботи набув подальшого розвитку науковий напрям, пов’язаний із підвищенням ефективності сигнатурних засобів захисту інформації, що реалізуються на базі ПЛІС.

Виходячи з того, що нові наукові результати - це нові знання в певній галузі фундаментальних чи прикладних наук, можна вважати основними науковими результатами дисертації таке:

- вперше запропонований метод прискореного обчислення технічних характеристик компонентів реконфігуровних апаратних сигнатурних засобів технічного захисту інформації (РАСЗТЗІ), що використовуються в якості цільових функцій процедур оптимізації, який на відміну від відомих методів проектування реконфігуровних пристроїв не потребує виконання витратних за часом процедур синтезу цифрових схем і забезпечує за рахунок формування математичного опису швидке оцінювання та порівняння обчислювальних структур за визначеними показниками ефективності;

- вперше запропонований метод прискорення процедури оптимізації паралельного комбінування, який відрізняється впорядкуванням патернів в наборі за певним параметром, що дозволяє замість повного перебору комбінаторно великої кількості варіантів здійснювати поділ патернів між блоками розпізнавання, що комбінуються, за лінійним законом часу, послідовно змінюючи параметр впорядкування;

- вперше запропонований метод паралельного комбінування, який за рахунок паралельного з'єднання різних за принципами побудови блоків розпізнавання дозволяє підвищити показники ефективності модулю розпізнавання РАСЗТЗІ;

- вперше запропонований метод 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 РАСЗТЗІ.

- удосконалений метод вертикального об'єднання, який відрізняється від відомих методів використанням багатовимірної таблиці сумісності, що дозволяє формалізувати наявний досвід численних дослідників та спростити процедуру оптимізації вибору найбільш ефективної, за наданих умов, комбінації задіяних даним методом підходів або технічних рішень.

- вперше запропонований принцип комбінування методів комбінування, який за рахунок ієрархічного використання методів комбінування забезпечує підвищення показників ефективності модулю розпізнавання РАСЗТЗІ до значень, недосяжних при використанні кожного з методів комбінування окремо.

3. Ступінь обґрунтованості наукових положень дисертації та їх достовірність

Наукові положення, висновки і рекомендації, викладені в дисертаційній роботі, є достатньо обґрунтованими за рахунок коректного використання відомих принципів побудови реконфігуровних пристроїв, елементів теорії автоматів та апарату булевої алгебри, теорії обчислень на рядках, елементів теорій графів, множин, комбінаторики та алгоритмів,.

Достовірність основних наукових результатів роботи підтверджується наведеною в розд. 3-6 системою визначень, тверджень та формальних методик, яка не містить логічних протиріч, низкою прикладів, а також збіжністю результатів авторських обчислювальних експериментів з результатами експериментів інших науковців.

4. Цінність дисертаційної роботи для науки

Наукова цінність проведеного дослідження полягає в тому, що в ньому запропоновано нове вирішення важливої науково-прикладної проблеми в теорії проектування реконфігуровних обчислювальних систем.

Змістовний аспект запропонованого рішення, який спрямований на розширення класу методів і засобів синтезу обчислювальних структур сигнатурного аналізу, що забезпечують підвищення ефективності за визначеними показниками, не був відомий раніше.

5. Практична корисність роботи

Практична корисність роботи обумовлена тім, що використання запропонованих в ній моделей, формальних методів, конкретних рішень і рекомендацій дозволяє створювати більш досконалі, порівняно з відомими, реконфігуровні засоби захисту інформації, які використовуються для протидії зовнішнім та внутрішнім атакам на комп'ютерні системи та мережі.

Практичне значення роботи підтверджується впровадженням результатів досліджень в Національному аерокосмічному університеті ім. Н.Є Жуковського "Харківський авіаційний інститут", на приватному підприємстві "Геракс", в Національному авіаційному університеті та в Київському національному університеті ім. Т.Г. Шевченка

Наукові результати дисертаційної роботи також було використано в рамках проекту Європейського Союзу «Інтернет речей: нова навчальна програма для потреб промисловості та суспільства», шифр ALIOT (номер проекту 573818-EPP-1-2016-1-UK-EPPKA2-CBHE-JP, 2016 – 2019 рр.).

Корисність роботи для практичного застосування обумовлена ще й реалізацією запропонованих методів та алгоритмів у вигляді побудованого на базі кластера Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України макетного зразку веб-сервісу централізованого створення реконфігуровних засобів інформаційної безпеки STRAGS, що використовує високопродуктивні ресурси гріду та хмарних обчислень.

6. Оцінка змісту дисертації, її завершеності й оформлення

Побудова дисертації відповідає прийнятим для наукового дослідження вимогам. Дисертація складається з анотації, списку термінів та умовних скорочень, вступу, 7 розділів, загальних висновків, додатків, списку використаних джерел.

У вступі надано загальну характеристику дисертаційної роботи, обґрунтовано актуальність та важливість теми дослідження, сформульовано його мету та задачі, окреслено об’єкт і предмет, визначено наукову новизну та практичну цінність. Також наведено відомості про апробацію і впровадження результатів роботи та про структуру дисертації.

У першому розділі проведено аналіз проблем технічного захисту інформації, які доцільно вирішувати реконфігуровними засобами, і аналіз технічних можливостей сучасних ПЛІС як апаратної бази для вирішення складних обчислювальних задач інформаційного захисту. В результаті порівняльного аналізу сигнатурних засобів захисту з іншими підходами, а також різних апаратних платформ для їх реалізації, обґрунтовано обрано предметом дослідження реконфігуровні апаратні сигнатурні засоби технічного захисту інформації.

У другому розділі проаналізовано відомі принципи функціонування та побудови реконфігуровних засобів інформаційного захисту на прикладі систем виявлення вторгнень. Сформована узагальнена структура реконфігуровного пристрою такого типу. Виявлено специфічну особливість реконфігуровних засобів як апаратної платформи сигнатурних систем захисту, яка полягає в

необхідності регулярного проведення повторного синтезу деяких компонентів сигнатурних засобів захисту. З метою оцінювання та порівняння властивостей розробок сигнатурних засобів захисту та їх компонентів, сформульовані і класифіковані показники ефективності.

Виокремлено три найефективніші підходи до побудови апаратних засобів інформаційного захисту та технології, на яких вони базуються. Такими виявилися: асоціативна пам'ять на базі цифрових компараторів, фільтр Блума на базі геш-функцій та алгоритм Ахо-Корасік, апаратно реалізований на базі скінченних автоматів.

Третій розділ присвячено дослідженню властивостей кожного з виокремлених підходів. З метою ефективного комбінування різних схем розпізнавання та їх численних модифікацій класифіковано властивості кожного з підходів, використовуючи сформульовані показники ефективності. При цьому враховувалися переваги та недоліки кожного підходу, потенціал щодо покращення показників, складнощі реалізації на ПЛІС та можливості їх подолання.

Четвертий розділ присвячено питанням кількісного оцінювання виокремлених підходів та їх модифікацій.

Досліджено властивості баз даних сигнатур сучасних сигнатурних систем захисту інформації. Запропоновано техніку впорядкування елементів цих баз. Запропоновані необхідні для подальшого дослідження визначення функції розподілу довжин сигнатур та декількох функцій самоподоби. Введено єдину метрику обчислення апаратних витрат.

Розроблено метод прискореного обчислення технічних характеристик компонентів реконфігуровних засобів захисту, який полягає в обчислені функцій оцінки, які подаються у вигляді аналітичних виразів. що описують залежність основних характеристик схем розпізнавання від властивостей сигнатур, з одного боку, та від параметрів реконфігуровних обчислювачів – з іншого.

Використання функцій оцінки дозволяє швидко знаходити з певною точністю кількісні характеристики майбутніх схем розпізнавання без використання витратного за часом та потрібними обчислювальними ресурсами повного циклу компіляції цифрового проєкту з використанням відповідної САПР.

З метою пояснення принципів побудови функції оцінки та для здійснення можливості проведення експериментальних розрахунків сформовано такі функції для низки найбільш перспективних схем та модифікацій на базі виокремлених раніше підходів.

У п'ятому розділі автором сформульовано та вдосконалено методи, що базуються на комбінуванні різних схем розпізнавання і реалізують різнорідні підходи до побудови компонентів реконфігуровних сигнатурних засобів захисту. Розглянуті питання вибору цільових функції процесу оптимізації.

Крім паралельного та послідовного методів автор запропонував метод вертикального об'єднання, суть якого полягає у поєднанні рис різних підходів в єдину схему розпізнавання без необхідності поділу сигнатур. Запропоновано інформаційну структуру, яка дозволяє формалізувати досвід використання відомих підходів та їх модифікацій та спростити процедуру оптимізації їх вибору. Сформульовано підхід до комбінування методів комбінування, який дозволяє ще більше підвищити показники ефективності компонентів сигнатурних засобів технічного захисту інформації.

У шостому розділі розроблено алгоритми та програмні засоби, що реалізують запропоновані автором методи.

Наведено кількісні оцінки зниження апаратних витрат на побудову компонентів реконфігуровних сигнатурних засобів захисту інформації, що підтвердили ефективність запропонованих автором методів.

Порівняння з опублікованими даними щодо існуючих розробок дозволило перевірити результати теоретичних досліджень та продемонструвати переваги запропонованих підходів порівняно з відомими досягненнями.

Сьомий розділ присвячено створенню веб-сервісу централізованого синтезу компонентів апаратних засобів захисту інформації та програмування ПЛІС реконфігуровних прискорювачів з використанням грід- та хмарних обчислень.

7. Рекомендації щодо використання результатів дисертації.

Запропоновані в роботі методи та алгоритми можуть бути використані для побудови високоефективних засобів сигнатурного аналізу не лише в галузі інформаційної безпеки, але й у галузях мережевих задач обробки даних, data mining та при аналізі структури молекул.

Крім того, на базі розробленого у вигляді макетного зразка веб-сервісу STRAGS можливо створення комерційних систем централізованого програмування реконфігуровних прискорювачів для вирішення широкого кола обчислювальних задач у різних галузях науки і техніки.

8. Повнота викладення основних результатів дисертації.

Основні результати дисертації достатньо повно відображені в 52 наукових працях, серед яких статті у наукових виданнях, що входять до переліку фахових видань України з технічних наук та індексуються в міжнародних науково-метричних базах, та пройшли апробацію на багатьох

міжнародних науково-технічних конференціях.

9. Автореферат дисертації.

Зміст автореферату повністю відображає основні положення дисертації.

10. Зауваження щодо змісту і оформлення дисертації:

1. У роботі не сформульована чітко задача реконфігурування обчислювальних структур. Реконфігурування може здійснюватися з метою налаштування на розв'язання певної обчислювальної задачі (програмована архітектура обчислювача за визначенням Каляєва А.В.) або з метою забезпечення правильного функціонування в разі виникнення відмов в апаратурі (відмовостійки апаратні засоби).

2. У першому розділі основна задача, що розв'язується створюваними засобами, формулюється як "Задача множинного розпізнавання патернів", однак, в інших розділах дисертаційної роботи вона згадується як "Задача множинного розпізнавання рядків".

3. У підрозділі 3.2 наведено визначення другої функції самоподоби множини патернів, однак далі ця функція ніде не використовується.

4. Запропоновані автором в четвертому розділі функції оцінки містять ресурсну та часову складові, однак, у шостому розділі описуються експерименти, що проводяться лише зі значеннями витрат апаратних ресурсів, але жодного експерименту щодо швидкісних властивостей досліджених структур не наведено.

5. Автор не пояснює, яким чином формуються HDL-описи модуля розпізнавання за його структурою після знаходження оптимального рішення згідно загальної структури використання методів комбінування, що наведена на рис. 6.1.

6. Результати розрахунків щодо принципу комбінування методів комбінування були б більш наочними в разі їх подання у вигляді тривимірного графіку.

7. У розділі 6 для порівняння з відомими даними використана інформація з досить застарілих публікацій.

8. У тексті дисертації та автореферату спостерігається багато тавтологій, наприклад, "метод МПрКм", де скорочення МПрКм починається зі слова "метод", або "задача ЗМРП", тобто, задача "Задача множинного розпізнавання патернів".

9. В авторефераті рис. 17а ("склад ресурсних витрат схеми HRCmp") дещо відрізняється від рис. 6.11, що відповідає йому в дисертаційній роботі.

10. В описах експериментів не вказано, скільки часу займає виконання розрахунків.

11. Доцільно було б навести рекомендації стосовно конкретних випадків застосування методів паралельного комбінування, послідовного каскадування і вертикального об’єднання блоків розпізнавання.

11. Загальна оцінка дисертації

Оцінюючи роботу в цілому, вважаю, що в дисертації отримано нове вирішення важливої науково-прикладної проблеми в теорії побудови реконфігуровних сигнатурних засобів захисту інформації комп'ютерних систем і мереж. Дисертація є завершеною науково-дослідною роботою.

Вважаю, що за актуальністю вибраної теми, обсягом і рівнем виконаних теоретичних і експериментальних досліджень, достовірністю і обґрунтованістю висновків, новизною досліджень, значенням отриманих результатів для науки і практики, рівнем апробації та публікацій дисертаційна робота задовольняє вимогам п. 9, 10, 12 і 13 «Порядку присудження наукових ступенів», затвердженого Постановою КМУ від 19 серпня 2015 року № 656, 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
завідувач кафедри захисту інформації
Вінницького національного
технічного університету,
д.т.н., професор В.А. Лужецький

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ * ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ * Ідент. код 02070693

Підпис Лужецького В.А
ПОСВІДЧУЮ
Зав. канцелярією