ВІДГУК

офіційного опонента, кандидата технічних наук, доцента,
доцента кафедри комп'ютерних систем та мереж
Національного університету «Запорізька політехніка»
Грушко Світлани Сергіївни
на дисертаційну роботу Іванової Олени Миколаївни
на тему
«Моделі та методи гібридного маскування даних у процесі моніторингу програмного коду FPGA-компонентів інформаційних систем»,
представлену на здобуття ступеня доктора філософії за спеціальністю 122 – «Комп'ютерні науки», галузь знань 12 – «Інформаційні технології»

1 Актуальність обраної теми дисертації

Дисертаційна робота Іванової О.М. присвячена замаскованому зберіганню контрольних даних, необхідних для виконання прихованого моніторингу програмного коду FPGA-компонентів інформаційних систем. Такі компоненти відіграють важливу роль у сучасних інформаційних системах, забезпечуючи реалізацію високопродуктивних обчислювальних процесів із програмним керуванням. Їх застосування є характерним для систем критичного призначення, що функціонують у таких галузях, як авіаційно-космічна галузь, енергетичний сектор, транспортна інфраструктура, промислове виробництво, телекомунікаційні мережі, медичні інформаційні системи, фінансовий сектор, автоматизовані системи керування технологічними процесами та сфера штучного інтелекту.

За умов постійного зростання кількості кібератак та випадків несанкціонованого впливу на роботу інформаційних систем особливої актуальності набуває проблема організації прихованого контролю цілісності та безпечності програмного коду FPGA-компонентів. Важливим аспектом реалізації такого контролю є забезпечення надійного та непомітного зберігання контрольної інформації, яка використовується для перевірки безпекових параметрів програмного коду. Дисертаційне дослідження Іванової О.М. спрямоване на розроблення підходів до збільшення обсягу

прихованого зберігання контрольних даних у програмному коді FPGA-компонентів інформаційних систем. Поширені методи моніторингу програмного коду FPGA-компонентів передбачають зберігання контрольної інформації або безпосередньо в структурі програмного коду, або в централізованих сховищах даних. Подібна організація створює додаткові ризики компрометації та підроблення контрольних даних. У зв'язку з цим значний науковий інтерес становить використання стеганографічних технологій, які дають можливість інтегрувати контрольні дані у програмний код у прихованому вигляді. Проте більшість наявних рішень базується на застосуванні еквівалентних трансформацій програмного коду та характеризується недостатньою ємністю стеганографічного контейнера. Це суттєво обмежує можливість розміщення контрольних даних великого обсягу.

У дисертаційній роботі запропоновано підхід, що ґрунтується на використанні гібридної технології прихованого зберігання контрольної інформації в програмному коді FPGA-компонентів. Запропоноване рішення має науково-прикладне значення, оскільки дозволяє підвищити результативність прихованого моніторингу за рахунок розширення доступного обсягу для вбудовування контрольних даних. Практична реалізація такого підходу сприяє підвищенню рівня захисту інформаційних систем, у структурі яких використовуються FPGA-компоненти.

2 Аналіз форми та змісту дисертаційної роботи

Дисертаційна робота містить вступ, чотири розділи, висновки, список використаних джерел та додатки.

У вступі обґрунтовано актуальність теми, визначено мету, завдання та методи дослідження, розкрито наукову новизну й практичну цінність результатів, наведено відомості про апробацію та публікації.

Перший розділ присвячено аналізу методів зберігання контрольних даних під час моніторингу програмного коду FPGA-компонентів. Розглянуто традиційні та стеганографічні підходи, визначено їх недоліки та

обґрунтовано потребу у створенні нових моделей та методів гібридного замаскованого зберігання контрольних даних.

У другому розділі запропоновано моделі прихованого зберігання даних у програмному коді FPGA. Виявлено надлишкові ресурси блоків LUT, придатні для прихованого зберігання даних, а також розроблено й експериментально перевірено метод нееквівалентного прихованого зберігання даних.

Третій розділ описує гібридні підходи, що поєднують еквівалентні та нееквівалентні перетворення програмного коду FPGA-компонентів. На їх основі створено методи прихованого зберігання контрольних даних і формування стеганографічного ключа, ефективність яких підтверджено експериментально.

У четвертому розділі розроблено підсистему замаскованого зберігання контрольних даних для системи прихованого моніторингу програмного коду FPGA-компонентів. Проведене тестування підтвердило її працездатність і готовність до практичного використання.

У висновках узагальнено результати дослідження та показано досягнення поставленої мети роботи.

Робота відзначається логічною структурою та цілісним викладом матеріалу, повною мірою відображає проведені дослідження та їх результати.

3 Ступінь обґрунтованості наукових положень, висновків та рекомендацій

Обґрунтованість наукових положень, висновків і рекомендацій дисертації забезпечується всебічним аналізом проблеми, комплексним підходом до вирішення задач дисертації, логічною послідовністю етапів дослідження, коректним застосуванням математичного апарату та наукових методів, вірним плануванням експериментів.

Наукові положення, висновки та рекомендації роботи достатньою мірою обґрунтовані, оскільки базуються на аналізі сучасних та загальновизнаних літературних джерел у таких галузях, як арифметичні та алгоритмічні основи комп'ютерних обчислень, теоретичні основи цифрової стеганографії та цифрових водяних знаків, комп'ютерне моделювання, методи та алгоритми розв'язання прикладних задач комп'ютерних наук, а також на значній кількості експериментальних досліджень.

4 Достовірність отриманих результатів

Достовірність наукових положень, висновків і рекомендацій дисертації підтверджується: збіжністю теоретично отриманих результатів з експериментальними результатами та результатами впровадження; наявністю патенту на винахід, в основу якого лягли положення дисертації; результатами впровадження отриманих у дисертації теоретичних положень та інструментальних засобів; успішною апробацією результатів дисертації на науково-практичних конференціях; публікацією результатів у рецензованих міжнародних та вітчизняних наукових виданнях, зокрема тих, що індексуються в наукометричних базах Scopus та Web of Science.

5 Наукова новизна одержаних результатів

У роботі сформульовано наукові положення, що забезпечують вирішення актуальної науково-прикладної задачі підвищення обсягу замаскованого зберігання контрольних даних у середовищі низькорівневого програмного коду FPGA-компонентів під час прихованого моніторингу цього програмного коду. Основні наукові результати дослідження полягають в наступному:

– вперше розроблено модель замаскованого зберігання даних в середовищі програмного коду FPGA-компонентів, яка основана на використанні нееквівалентних перетворень програмного коду FPGA та

враховує особливості виконання наближених арифметичних операцій у середовищі FPGA, що дозволяє визначити множину надлишкових інформаційних ресурсів, які виникають у процесі виконання таких обчислень та можуть бути використані для прихованого зберігання контрольних даних;

– вперше розроблено метод нееквівалентного замаскованого зберігання даних в середовищі програмного коду FPGA-компонентів, що характеризується використанням надлишковості програмного коду FPGA, яка виникає при виконанні наближених арифметичних операцій, що дозволяє збільшити обсяг, доступний для прихованого зберігання контрольних даних у задачах моніторингу характеристик безпеки програмного коду FPGA;

– вперше розроблено метод гібридного замаскованого зберігання даних в середовищі програмного коду FPGA, який відрізняється поєднанням еквівалентного та нееквівалентного підходів до перетворення програмного коду FPGA, а також поєднанням процесів стеганографічного вбудовування та відновної обфускації даних, що дозволяє збільшити обсяг контрольних даних, які можуть бути приховано вбудовані в програмний код FPGA, не збільшуючи при цьому здатність традиційних методів стегоаналізу до виявлення цих даних в програмному коді;

– дістав подальшого розвитку метод формування стеганографічного ключа для замаскованого збереження даних в програмному коді FPGA, який відрізняється можливістю адаптації до структури зв’язків між елементарними одиницями FPGA та до необхідного обсягу контрольних даних, що дозволяє виконувати балансування між обсягом частини програмного коду, яка модифікується в результаті вбудовування даних та ефективним обсягом стеганографічного контейнера, потрібним для збереження контрольних даних.

Зазначені положення наукової новизни сформульовані відповідно до тематики дослідження, відповідають меті дисертації та демонструють високий рівень володіння здобувачкою методологією наукової діяльності.

6 Практичне значення роботи

На основі моделей та методів, які були запропоновані в дисертації, реалізовано підсистему гібридного замаскованого зберігання контрольних даних для інформаційної системи прихованого моніторингу програмного коду FPGA-компонентів. Практичне впровадження створеної підсистеми та її перевірка в межах експериментів підтвердили збільшення обсягу замаскованого зберігання контрольних даних в середовищі програмного коду FPGA-компонентів. Завдяки цьому стало можливим вбудовувати більший обсяг контрольних даних у програмний код FPGA-компонентів, використовувати контрольні дані більшої розрядності та розширити кількість різновидів прихованого моніторингу, контрольні дані яких зберігаються в замаскований спосіб.

Розроблені в межах дисертаційного дослідження програмні засоби впроваджено в діяльність товариства з обмеженою відповідальністю ТЕХНО.КОМ. Також практичне значення роботи підтверджується впровадженням її результатів у навчальний процес закордонних університетів за ERASMUS+ проєктом “ALIOT – Internet of Things: Emerging Curriculum for Industry and Human Applications”, та в науково-дослідні роботи і навчальні програми Національного університету «Одеська політехніка».

7 Повнота викладення результатів дисертації в опублікованих працях

Результати дисертаційного дослідження висвітлено у 14 наукових працях. До їх числа входять 5 статей, опублікованих у міжнародних виданнях, що індексуються в базах Scopus та Web of Science Core Collection, 4 публікації у фахових наукових виданнях України категорії Б, а також матеріали міжнародних і всеукраїнських конференцій. За підсумками виконаної роботи автором отримано патент України на винахід, що

підтверджує практичну цінність дослідження. Всі наукові положення та результати, отримані в ході дисертаційного дослідження, знайшли відображення в опублікованих роботах.

Ключові результати та положення роботи пройшли апробацію під час міжнародних і всеукраїнських науково-практичних конференцій. Зокрема, вони були представлені на конференціях Computer Modeling and Intelligent Systems, CMIS-2021; Інформатика, управління та штучний інтелект, ІУШІ-2021; Сучасні інформаційні технології, МІТ-2021 та Перспективні напрямки сучасної електроніки, інформаційних і комп'ютерних систем, MEICS-2023, де отримали фахове обговорення й позитивну оцінку.

Отже, дисертація повністю відповідає встановленим вимогам щодо кількості та характеру наукових публікацій, в яких висвітлено її наукові результати.

8 Дотримання академічної доброчесності

Наукові результати дисертації опубліковані у рецензованих наукових виданнях, що здійснюють ретельну попередню перевірку на наявність запозичень. Також результати дослідження було обговорено і опубліковано в матеріалах міжнародних та всеукраїнських конференцій. Зазначене є підтвердженням дотримання здобувачем принципів академічної доброчесності. Аналіз тексту дисертаційної роботи та публікацій показує відсутність порушень академічної доброчесності. Фактів порушення академічної доброчесності в дисертації здобувачки не виявлено.

9 Дискусійні положення та зауваження щодо змісту дисертації

1. У 1-му розділі доцільно було б описати, наскільки великою є частка наближених обчислень загалом серед обчислень, які зазвичай виконуються в середовищі FPGA-компонентів. Приклади реальних класів задач, де

наближені обчислення на FPGA є типовими, в 1-му розділі описані, але цей опис є занадто стислим.

2. Обговорення в 1-му розділі напрямку IP watermarking, суміжного до тематики роботи, слід було зробити більш розвинутим. Порівняльний аналіз з цим напрямком дозволив би чіткіше спозиціонувати роботу та продемонструвати відмінності між цими напрямками.

3. В аналітичному розділі дисертації доцільно було б зіставити стеганографічний підхід до захисту низькорівневого програмного коду FPGA-компонентів з промисловими механізмами захисту, такими як: шифрування конфігурації AES-256, автентифікація бітстріму (HMAC, ECDSA), hardware root of trust, anti-tamper моніторинг, PUF-базована ідентифікація.

4. У розділі 2 детально описано процес отримання даних про структуру блоків LUT та їх зв’язки з внутрішньої бази даних САПР за допомогою TCL-додатка LUTListExtractor (стор. 89–91), а в розділі 4 наведено функціональне тестування підсистеми на рівні її внутрішніх об'єктів (стор. 167–170). Проте зворотний шлях, яким чином модифіковані програмні коди блоків LUT повертаються до проєкту САПР для формування оновленого низькорівневого програмного коду, у тексті роботи не описано.

5. Пункти 2.1.1 та 2.1.2 з 2-го розділу більш підходять для аналітичного розділу дисертації.

6. Експериментальні дослідження в роботі проводилися тільки на основі FPGA-компонентів та програмних засобів компанії Intel/Altera. Незрозуміло, чому так було обмежено середовище проведення експериментів.

7. У тексті дисертації присутні деякі стилістичні та граматичні неточності.

Наведені зауваження мають дискусійний характер, не впливають на загальну позитивну оцінку дисертаційної роботи та не знижують наукової і практичної цінності отриманих результатів.

10 Загальний висновок

Представлена дисертаційна робота є завершеною кваліфікаційною науковою працею, яка містить раніше не захищені наукові положення та одержані автором нові науково обґрунтовані результати в галузі замаскованого зберігання даних у низькорівневому програмному коді FPGA-компонентів інформаційних систем. Зміст дисертаційної роботи відповідає спеціальності 122 – «Комп'ютерні науки», галузі знань 12 – «Інформаційні технології». З огляду на актуальність вирішеної науково-прикладної задачі збільшення доступного обсягу для замаскованого зберігання контрольних даних у процесі прихованого моніторингу програмного коду FPGA-компонентів, внесок авторки в розвиток теорії прихованого зберігання даних, високий рівень виконаних досліджень та оволодіння здобувачкою методологією наукової діяльності вважаю, що дисертаційна робота «Моделі та методи гібридного маскування даних у процесі моніторингу програмного коду FPGA-компонентів інформаційних систем» відповідає вимогам «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженому Постановою Кабінету Міністрів України від 12 січня 2022 р. № 44, а її авторка Іванова Олена Миколаївна заслуговує на присудження їй наукового ступеня доктора філософії за спеціальністю – 122 «Комп'ютерні науки», галузь знань – 12 «Інформаційні технології».

Офіційний опонент
кандидат технічних наук, доцент,
доцент кафедри комп'ютерних систем
та мереж Національного університету
«Запорізька політехніка» Світлана ГРУШКО