ВІДГУК
ОФІЦІЙНОГО ОПОНЕНТА

доктора технічних наук, професора, завідувача кафедри кібербезпеки
Західноукраїнського національного університету
Яцківа Василя Васильовича
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 Загальна характеристика та актуальність теми дисертації

Сучасні інформаційні системи критичного застосування широко використовують FPGA-компоненти для реалізації високопродуктивних програмно-керованих обчислень. Ці компоненти використовуються в інформаційних системах, які забезпечують функціонування сфер підвищеного ризику, таких як: енергетика, швидкісний транспорт, промисловість, телекомунікації. Зростання кількості кіберзагроз і випадків несанкціонованого втручання в роботу таких систем обумовлює необхідність забезпечення ефективного прихованого моніторингу програмного коду FPGA-компонентів. Однією з ключових задач у цій галузі є замасковане зберігання контрольних даних, необхідних для перевірки безпекових характеристик, щодо програмного коду FPGA-компонентів. Дисертаційна робота Іванової О.М. спрямована на розв'язання задачі збільшення доступного обсягу прихованого зберігання контрольних даних у програмному коді FPGA-компонентів інформаційних систем.

Наявні підходи до моніторингу програмного коду FPGA-компонентів базуються на зберіганні контрольних даних разом із програмним кодом або в централізованих базах даних, що створює ризики їх фальсифікації. Перспективним напрямом є використання стеганографічних методів, які забезпечують приховане вбудовування контрольних даних у програмний код FPGA-компонентів. Проте наявні методи ґрунтуються переважно на еквівалентних перетвореннях програмного коду та характеризуються обмеженим обсягом доступного стеганографічного контейнера, що не дозволяє забезпечити зберігання контрольних даних великої розмірності.

Запропонований в дисертаційній роботі підхід, який базується на застосуванні гібридного замаскованого зберігання контрольних даних у програмному коді FPGA-компонентів, є актуальним науково-прикладним завданням. Вирішення цього завдання дозволяє підвищити ефективність прихованого моніторингу програмного коду FPGA-компонентів за рахунок усунення дефіциту обсягів для прихованого зберігання контрольних даних моніторингу. Це, у свою чергу, сприяє підвищенню захищеності інформаційних систем критичного застосування, до складу яких входять FPGA-компоненти, в умовах сучасних загроз.

2 Структура та зміст дисертації

Дисертація складається зі вступу, чотирьох розділів, висновків, списку використаних джерел та додатків.

У **вступі** наведена загальна характеристика роботи: актуальність, мета й задачі досліджень, представлені методи досліджень, вказані новизна і практичне значення отриманих результатів, сформульовані основні положення, що виносяться на захист, наведені відомості про апробацію, публікації та реалізацію результатів дослідження.

У **першому розділі** міститься аналітичний огляд проблематики замаскованого зберігання контрольних даних при виконанні прихованого моніторингу низькорівневого програмного коду FPGA-компонентів. Розглянуто традиційні підходи на основі збереження криптографічно захищених контрольних даних разом з інформаційним об’єктом програмного коду в файлової системі, пам’яті або в централізованій базі даних та стеганографічні підходи. Окреслено обмеження наявних підходів і обґрунтовано потребу в розробці нових моделей та методів гібридного замаскованого зберігання контрольних даних, що слугує підґрунтям для постановки мети да задач дослідження.

У **другому розділі** запропоновано моделі замаскованого зберігання даних в середовищі програмного коду FPGA-компонентів. Моделі дозволяють виділити два види надлишкових ресурсів у складі програмного коду FPGA, що можуть бути використані зі метою замаскованого зберігання даних: несуттєві блоки LUT та несуттєві розряди програмного коду блоків LUT. Проведено експериментальне дослідження, яке підтвердило наявність зазначених надлишкових інформаційних ресурсів, а також дозволило їх локалізувати та оцінити їх частку в загальному обсязі

програмного коду блоків LUT FPGA. На основі запропонованих моделей розроблено метод нееквівалентного замаскованого зберігання даних в середовищі програмного коду FPGA-компонентів, та проведено експериментальне дослідження його ефективності.

У **третьому розділі** запропоновано підходи до гібридного замаскованого зберігання даних в програмному коді FPGA-компонентів, які поєднують еквівалентні та нееквівалентні перетворення програмного коду для вбудовування даних, а також дають можливість застосування відновної обфускації в процесі вбудовування додаткових даних в програмний код. На основі запропонованих підходів розроблено метод гібридного замаскованого зберігання контрольних даних в середовищі програмного коду FPGA та метод формування стеганографічного ключа для прихованого збереження контрольних даних в програмному коді FPGA Виконано експериментальне дослідження, яке підтвердило ефективність розроблених методів.

У **четвертому розділі** дисертаційної роботи розроблено підсистему гібридного замаскованого зберігання контрольних даних в складі інформаційної системи прихованого моніторингу програмного коду FPGA-компонентів. Проведено комплексне тестування розробленої підсистеми, що довело її готовність до використання в складі інформаційної системи прихованого моніторингу програмного коду FPGA-компонентів.

У **висновках** викладено основні наукові та практичні результати дослідження, показано досягнення поставленої мети та виконання всіх задач дослідження.

Загалом, зміст дисертаційної роботи є послідовним, логічно побудованим, він достатньо повно відображає проведені дослідження та їх результати.

3 Оцінка обґрунтованості та достовірності наукових положень, висновків і рекомендацій

Обґрунтованість наукових положень, висновків та рекомендацій дисертації забезпечена коректним застосуванням теоретичної бази та відповідного математичного апарату: арифметичних та алгоритмічних основ комп’ютерних обчислень, теорії наближених обчислень, булевої алгебри, теорії множин, теоретичних основ цифрової стеганографії та цифрових водяних знаків, комп’ютерного моделювання, методів та

алгоритмів розв’язання прикладних задач комп’ютерних наук та сучасні технології програмування.

Методика досліджень та методи вирішення поставлених в дисертації задач ґрунтуються на всебічному аналізі проблеми, яка розв’язується в роботі, узагальнені робіт відомих авторів, отриманні нових наукових результатів та експериментальній перевірці їх ефективності з застосуванням сучасних підходів та програмного забезпечення.

Достовірність наукових положень, висновків та рекомендацій дисертації забезпечується повнотою розгляду об’єкта досліджень, застосуванням методів, що повною мірою відповідають предмету досліджень, коректною постановкою проблеми, мети та задач дослідження, використанням сучасних підходів до проведення дослідження. Достовірність підтверджується тим, що теоретичні положення дисертації доведені здобувачем до практичної реалізації, в середовищі якої були проведені експерименти з підтвердження несуперечливості та ефективності цих положень.

Також достовірність наукових положень та результатів дисертаційного дослідження ґрунтується на її апробації в межах чотирьох міжнародних та всеукраїнських науково-технічних конференцій та публікації результатів в вітчизняних рецензованих наукових виданнях та у рецензованих закордонних виданнях, що індексуються в наукометричних базах Scopus та Web of Science.

Крім того достовірність результатів дисертації базується на їх впровадженні у виробничу діяльність, а також на використанні результатів в ERASMUS+ проєкті “ALIOT – Internet of Things: Emerging Curriculum for Industry and Human Applications”.

4 Новизна наукових положень

В роботі отримано ряд наукових положень, які в сукупності забезпечують вирішення актуальної науково-прикладної задачі збільшення доступного обсягу для приховування контрольних даних в процесі таємного моніторингу програмного коду FPGA-компонентів інформаційних систем в умовах атак на систему моніторингу.

Основні наукові результати, отримані в роботі, 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 в середовищі FPGA, що дозволяє визначити множину надлишкових інформаційних ресурсів, які виникають в 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 в 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 вбудованими 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.

5 Практичне значення отриманих результатів

Практичне значення результатів дисертаційного дослідження полягає в розробці підсистеми гібридного замаскованого зберігання контрольних даних в складі інформаційної системи прихованого моніторингу програмного коду FPGA-компонентів. Використання цієї підсистеми в

процесі експериментальних досліджень та у практичній діяльності дозволило збільшити обсяг інформаційно замаскованого зберігання контрольних даних у процесі прихованого моніторингу програмного коду FPGA-компонентів, що дало змогу підвищити розрядність контрольних даних, які можуть бути замасковано збережені в програмному коді FPGA та збільшити кількості різновидів прихованого моніторингу програмного коду.

Розроблені в роботі методи та інструментальні засоби впроваджені у діяльність товариства з обмеженою відповідальністю ТЕХНО.КОМ та знайшли відображення у навчальному та науково-дослідницькому процесі Національного університету «Одеська політехніка», а також в межах ERASMUS+ проєкту "ALIOT – Internet of Things: Emerging Curriculum for Industry and Human Applications".

6 Повнота викладу результатів у публікаціях та дотримання академічної доброчесності

Основні результати дисертаційної роботи викладено у 14 наукових публікаціях, серед яких 5 статей у періодичних закордонних наукових виданнях, проіндексованих у наукометричних базах Scopus та Web of Science Core Collection, 4 статті у виданнях категорії Б, що входять до переліку наукових фахових видань України, а також тези доповідей міжнародних та всеукраїнських наукових конференцій. За результати дисертації отримано патент України на винахід. Таким чином, вимоги щодо кількості та рівня наукових публікацій за темою дисертації виконано у повному обсязі.

Основні наукові положення та практичні результати дисертаційного дослідження були апробовані і обговорені на міжнародних та всеукраїнських науково-практичних конференціях, зокрема: міжнародній науково-технічній конференції "Computer Modeling and Intelligent Systems, CMIS-2021" (Запоріжжя, 2021); міжнародній науково-технічній конференції "Інформатика, управління та штучний інтелект, ІУШІ-2021" (Харків, 2021); міжнародній науково-технічній конференції "Сучасні інформаційні технології, МІТ" (Одеса, 2021); всеукраїнській науково-практичної конференції "Перспективні напрямки сучасної електроніки, інформаційних і комп'ютерних систем, MEICS-2023" (Дніпро, 2023).

Публікація результатів дослідження у рецензованих наукових виданнях і матеріалах конференцій, які передбачають попередню перевірку

рукописів на наявність запозичень, є підтвердженням дотримання здобувачем принципів академічної доброчесності. Аналіз змісту дисертаційної роботи та відповідних публікацій свідчить про відсутність порушень академічної доброчесності.

7 Зауваження до дисертаційної роботи

1. Перший розділ дисертації містить аналіз сучасних підходів до зберігання контрольних даних, необхідних для виконання оперативного моніторингу програмного коду. Разом із тим, окремі оглядові фрагменти мають довідковий характер і могли б бути подані більш стисло.

2. В роботі не розглянуто сценарій при якому особа, зацікавлена в тому, щоб обійти моніторинг програмного коду FPGA-компонента, отримує доступ до двох версій програмного коду: версії до вбудовування та версії після вбудовування прихованих контрольних даних. Не описано, чи отримає в цьому випадку така особа доступ до контрольних даних та чи буде в цьому випадку стего-ключ скомпрометовано?

3. В 2-му розділі на рисунок 2.4 структури даних *A* та *B* позначені як операнди, але за змістом роботи ці структури даних є не операндами, а мантисами операндів.

4. Доцільно було б зробити порівняння обсягу другого виділеного в дисертації надлишкового ресурсу (несуттєвих бітів) програмного коду блоків LUT при виконанні наближених та точних обчислень.

5. В 4-му розділі дисертації згадується карта відповідності програмного коду FPGA, але не дається пояснень суті та функції цієї структури даних.

6. В 4-му розділі слід було надати більш детальний опис сценаріїв використання програмних засобів, що були розроблені на основі запропонованих методів.

7. У тексті дисертації подекуди зустрічаються поодинокі стилістичні та термінологічні неточності, які, однак, не впливають на основні наукові положення та результати дослідження.

Наведені зауваження не впливають на загальну позитивну оцінку дисертаційної роботи та не знижують її наукової новизни і практичної цінності.

8 Загальні висновки та оцінка дисертації

Дисертаційна робота Іванової Олени Миколаївни є завершеною кваліфікаційною науковою працею, в якій вирішено актуальну науково-прикладну задачу збільшення доступного обсягу для замаскованого зберігання контрольних даних в процесі прихованого моніторингу програмного коду FPGA-компонентів інформаційних систем шляхом розробки моделей та методів гібридного стеганографічного зберігання цих даних. Робота відзначається актуальністю тематики, науковою новизною отриманих рішень, достатнім рівнем теоретичної обґрунтованості та експериментальним підтвердженням одержаних результатів. Практична цінність роботи підтверджена впровадженням рішень, які було розроблено на основі теоретичних пропозицій дисертації. Зміст дисертаційної роботи відповідає спеціальності 122 «Комп'ютерні науки», галузі знань 12 «Інформаційні технології», а сама робота – відповідає вимогам чинного Порядку присудження ступеня доктора філософії.

Враховуючи викладене, вважаю, що дисертаційна робота Іванової Олени Миколаївни на тему «Моделі та методи гібридного маскування даних у процесі моніторингу програмного коду FPGA-компонентів інформаційних систем» відповідає вимогам Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у закладах вищої освіти (наукових установах), затвердженого Постановою Кабінету Міністрів України від 23 березня 2016 року № 261 (зі змінами) та вимогам п.п. 5 – 9 Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженого постановою Кабінету Міністрів України від 12.01.2022 №44 (зі змінами), а її автор Іванова Олена Миколаївна заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки», галузь знань 12 «Інформаційні технології».

Офіційний опонент:
завідувач кафедри кібербезпеки
Західноукраїнського національного університету,
доктор технічних наук, професор Василь ЯЦКІВ