РЕЦЕНЗІЯ

офіційного рецензента, кандидата технічних наук, доцента,
доцента кафедри комп'ютеризованих систем та програмних технологій
Національного університету «Одеська політехніка»
Сперанського Віктора Олександровича
на дисертаційну роботу Іванової Олени Миколаївни
«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

Для сучасних комп'ютерних та інформаційних систем характерним є стійке зростання частки програмованих компонентів. Така тенденція зумовлена необхідністю забезпечення високого рівня адаптивності, масштабованості та функціональної гнучкості систем, що функціонують в умовах динамічних змін вимог до них. Використання програмованих компонентів дозволяє оперативно модифікувати логіку роботи системи без потреби фізичної заміни обладнання, що суттєво підвищує ефективність їх експлуатації та скорочує витрати на модернізацію.

Особливе місце серед програмованих компонентів займають FPGA. Їх ключовою особливістю є можливість реконфігурації внутрішньої апаратної структури під впливом завантаженого програмного коду. На відміну від традиційного програмного забезпечення, конфігураційний код FPGA безпосередньо визначає архітектуру апаратної реалізації обчислювальних процесів, що забезпечує високу продуктивність, паралельність обробки даних та гнучкість застосування.

У зв'язку з цим питання захисту конфігураційного коду FPGA-компонентів набуває особливої актуальності. Несанкціонований доступ до конфігураційних даних, їх модифікація або копіювання можуть призвести не лише до порушення функціонування інформаційної системи, але й до витоку інтелектуальної власності, компрометації критичних алгоритмів чи впровадження шкідливих апаратних модифікацій.

Забезпечення безпеки програмного коду FPGA-компонентів потребує ефективних засобів прихованого моніторингу. Найпоширеніші методи моніторингу ґрунтуються на використанні контрольних даних, що зберігаються локально разом із кодом або у централізованих сховищах та характеризуються вразливістю до інсайдерських атак і фальсифікації.

Одним із перспективних підходів є стеганографічне вбудовування контрольної інформації у програмний код на основі еквівалентних перетворень. Це дозволяє приховати як самі контрольні дані, так і факт моніторингу. Проте обмежена місткість прихованого зберігання суттєво знижує ефективність таких методів. У зв'язку з цим підвищення обсягу прихованого зберігання контрольних даних у середовищі програмного коду FPGA-компонентів безумовно є актуальною науково-прикладною задачею.

2 Характеристика змісту дисертації

Дисертаційна робота структурована у вигляді вступу, чотирьох розділів, підсумкових висновків, переліку використаних джерел та додатків.

У *вступі* обґрунтовано наукову та практичну актуальність обраної проблематики, сформульовано мету й основні завдання дослідження, визначено застосовані методи, а також висвітлено наукову новизну та практичне значення отриманих результатів. Також наведено інформацію щодо апробації результатів роботи та наукові публікації.

Перший розділ присвячено дослідженню наявних підходів до зберігання контрольних даних в процесі моніторингу програмного коду FPGA-компонентів. Проведено аналіз традиційних і стеганографічних методів, визначено їхні обмеження та недоліки. На основі отриманих результатів аргументовано доцільність розроблення нових моделей і методів гібридного прихованого зберігання контрольних даних.

У *другому розділі* запропоновано моделі замаскованого зберігання інформації у програмному коді FPGA. Досліджено надлишкові можливості LUT-блоків, які можуть бути використані для зберігання прихованих даних. Розроблено метод нееквівалентного прихованого зберігання даних у програмному коді FPGA-компонентів, ефективність якого підтверджено експериментальними дослідженнями.

Третій розділ присвячено розробці гібридного методу прихованого зберігання контрольних даних у програмному коді FPGA-компонентів. Метод базується на комбінуванні еквівалентних і нееквівалентних перетворень програмного коду. Описані в розділі результати експериментальної перевірки показують ефективність запропонованих рішень.

У *четвертому розділі* представлено опис розробки інструментальних засобів, які втілюють теоретичні положення дисертації. Описано розроблену підсистему замаскованого зберігання контрольних даних, призначену для

систем прихованого моніторингу програмного коду FPGA-компонентів. Проведені випробування підтвердили коректність функціонування підсистеми та можливість її практичного впровадження.

У *висновках* узагальнено результати проведеного дослідження та продемонстровано практичний ефект їх застосування.

Дисертаційну роботу викладено в чіткій та логічно впорядкованій формі, що забезпечує цілісне сприйняття наукового матеріалу. У змісті повно й послідовно висвітлено основні етапи дослідження, а також узагальнено отримані наукові результати.

3 Науковий рівень, новизна та теоретичне значення

Дисертаційна робота присвячена розв'язанню актуальної науково-прикладної задачі збільшення доступного обсягу для приховування контрольних даних в процесі таємного моніторингу програмного коду FPGA-компонентів інформаційних систем. За результатами проведених досліджень здобувачем отримано нові науково обґрунтовані результати, які становлять внесок у розвиток методів замаскованого зберігання даних, а саме:

– 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.

Сформульовані результати, що характеризують наукову новизну роботи, логічно пов'язані з предметом дослідження, відповідають задачам дисертації та підтверджують належний рівень оволодіння здобувачкою методологією наукової діяльності.

4 Практичне значення дисертаційної роботи

Практичне значення отриманих результатів полягає в розробці комплексу програмних інструментальних засобів, які в сукупності забезпечують процеси замаскованого зберігання контрольних даних у програмному коді FPGA-компонентів. У дисертаційній роботі запропоновано та реалізовано спеціалізовану підсистему гібридного замаскованого зберігання контрольних даних, орієнтовану на функціонування в інформаційній системі прихованого моніторингу програмного коду FPGA-компонентів. Результати експериментальних досліджень у середовищі зазначеної підсистеми підтвердили ефективність запропонованого підходу щодо збільшення доступного обсягу замаскованого зберігання контрольних даних у програмному коді FPGA-компонентів. Отримані результати дали змогу вбудувати більший обсяг контрольних даних, застосовувати контрольні дані підвищеної розрядності та розширити функціональні можливості засобів прихованого моніторингу, що використовують механізми замаскованого зберігання.

Також підтвердженням практичного значення дисертації є отриманий патент України на винахід, в основу якого лягли результати втілення запропонованих моделей та методів.

Розроблені програмні рішення було використано у практичній діяльності товариства з обмеженою відповідальністю ТЕХНО.КОМ. Окремо варто відзначити впровадження результатів дослідження в освітню та наукову сферу, зокрема в межах міжнародного проєкту ERASMUS+ “ALIOT – Internet of Things: Emerging Curriculum for Industry and Human Applications”. Також результати роботи застосовуються у навчальних курсах та науково-дослідних розробках Національного університету «Одеська політехніка».

Результати дисертації можна рекомендувати до використання в організаціях і на підприємствах, які займаються розробкою, впровадженням й експлуатацією комп’ютерних та інформаційних систем на базі FPGA-компонентів для підвищення ефективності моніторингу характеристик безпеки цих систем в умовах потенційно можливих атак на процеси моніторингу.

5 Ступінь обґрунтованості наукових положень, висновків та рекомендацій

Наукові результати, які представлено в дисертації, відзначаються високим рівнем аргументованості, що забезпечується застосуванням системного підходу та залученням значного масиву сучасної наукової літератури. Теоретичну основу роботи становлять актуальні дослідження у сферах прихованого зберігання додаткових даних у програмному коді FPGA-компонентів, цифрової стеганографії, методів моніторингу безпекових характеристик програмного коду, а також арифметичних основ комп’ютерних систем. Використані рішення відповідають сучасному стану розвитку комп’ютерних наук і узгоджуються з практикою наукових досліджень у цій галузі.

Обґрунтованість отриманих результатів підтверджується результатами експериментальних досліджень та коректним використанням математичного апарату, сучасних засобів комп’ютерного моделювання та програмної реалізації розроблених рішень. Практична апробація запропонованих моделей і методів засвідчила їх прикладну значущість та можливість застосування в реальних умовах функціонування інформаційних систем.

Додатковими аргументами на користь достовірності наукових положень є отримання патенту на винахід, що базується на результатах дисертаційного дослідження, апробація основних положень на науково-

практичних конференціях, а також публікація результатів у рецензованих вітчизняних і міжнародних виданнях, включно з тими, що індексуються в наукометричних базах Scopus і Web of Science.

6 Повнота викладення результатів дисертації в опублікованих працях

Основні результати дисертаційної роботи опубліковано у 14 наукових працях, серед яких:

– 5 статей у рецензованих міжнародних наукових виданнях, що індексуються в наукометричних базах Scopus та Web of Science Core Collection;

– 4 статті у фахових наукових виданнях України категорії Б;

– 3 публікації у матеріалах міжнародних і всеукраїнських науково-практичних конференцій;

– 1 патент України на винахід;

– 1 навчальний посібник, який додатково висвітлює результати дисертації.

Основні наукові положення роботи за результатами доповідей було опубліковано в матеріалах наступних науково-технічних конференцій:

– 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-практичній конференції “Перспективні напрямки сучасної електроніки, інформаційних і комп’ютерних систем, MEICS-2023” (Дніпро, 2023).

Усі наукові результати, висновки та положення дисертаційного дослідження повною мірою відображено в опублікованих працях автора. Таким чином, дисертаційна робота відповідає чинним вимогам стосовно обсягу та змісту наукових публікацій, у яких представлено основні результати проведеного дослідження.

7 Аналіз дотримання академічної доброчесності

Опрацювання тексту дисертації та наукових праць здобувачки не виявило ознак порушень принципів академічної доброчесності.

Також дотримання академічної доброчесності підтверджується тим, що основні положення та результати дисертаційного дослідження було опубліковано у фахових рецензованих закордонних та вітчизняних наукових виданнях, у яких здійснюється ретельна перевірка матеріалів на наявність неправомірних запозичень.

Крім того, результати роботи пройшли апробацію на міжнародних і всеукраїнських наукових конференціях та відображені у відповідних збірниках матеріалів. Зазначена апробація результатів дослідження є додатковим підтвердженням дотримання принципів академічної доброчесності, оскільки представлення матеріалів у науковому середовищі передбачає їх відкритий фаховий розгляд, обговорення та критичну оцінку науковою спільнотою.

Отже, аналіз дисертаційної роботи, наукових публікацій здобувачки та результатів апробації підтверджує належне дотримання принципів академічної доброчесності в дисертаційному дослідженні.

8 Зауваження щодо змісту дисертації

1) Перший розділ дисертації містить аналіз сучасних підходів до моніторингу програмного коду FPGA-компонентів. Разом із тим, окремі оглядові фрагменти щодо структури та принципів функціонування FPGA мають довідковий характер і могли б бути викладені в більш стислій формі.

2) Не наведено обмежень запропонованих методів за параметрами часової складності та складності за пам’яттю.

3) На рис. 2.5 стор. 77 відсутні верхні індекси у підмножин блоків LUT, хоча в тексті, який пояснює цей рисунок, зазначені індекси присутні.

4) В роботі не приділено уваги організаційному аспекту застосування запропонованих методів та засобів. А саме, не визначено коло осіб та організацій, які мають право застосовувати запропоновані методи та засоби; не визначено умови, за яких застосування зазначених методів та засобів буде вважатися правомірним.

5) В роботі не роз’яснено, чи є запропоновані в дисертації методи універсальними в плані застосування до FPGA-компонентів різних виробників.

6) При описі запропонованого методу на стор. 87 зазначено, що розряди впорядковуються відповідно до первинного впорядкування блоків LUT, однак у подальшому в тексті роботи принцип первинного впорядкування не пояснюється.

7) В тексті дисертації присутні окремі орфографічні та стилістичні неточності.

Вказані зауваження не впливають на загальну позитивну оцінку дисертаційної роботи в цілому та не знижують наукової і практичної цінності отриманих результатів.

9 Загальний висновок про відповідність роботи встановленим вимогам

Дисертаційна робота Іванової Олени Миколаївни на тему «Моделі та методи гібридного маскування даних у процесі моніторингу програмного коду FPGA-компонентів інформаційних систем» є завершеним самостійним науковим дослідженням, яке вирішує важливу науково-прикладну задачу збільшення доступного обсягу для приховування контрольних даних в процесі таємного моніторингу програмного коду FPGA-компонентів інформаційних систем. Зміст дисертаційної роботи відповідає спеціальності 122 – Комп’ютерні науки, галузі знань 12 – Інформаційні технології.

Вважаю, що дисертаційна робота 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 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). Авторка дисертаційної роботи – Іванова Олена Миколаївна заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 122 – Комп’ютерні науки, галузь знань 12 – Інформаційні технології.

Офіційний рецензент,
кандидат технічних наук, доцент,
доцент кафедри комп’ютеризованих
систем та програмних технологій
Національного університету
«Одеська політехніка» Віктор СПЕРАНСЬКИЙ