

Голові разової спеціалізованої вченої ради
в Національному університеті
«Одеська політехніка»
доктору технічних наук, професору
Щербаковій Г.Ю.

РЕЦЕНЗІЯ

офіційного рецензента, кандидата технічних наук, доцента кафедри комп'ютеризованих систем та програмних технологій Навчально-наукового Інституту комп'ютерних систем Національного університету «Одеська політехніка» ГРИГОРЕНКО Світлани Миколаївни на дисертацію ІВАНОВОЇ Олени Миколаївни за темою: **«Моделі та методи гібридного маскування даних у процесі моніторингу програмного коду FPGA-компонентів інформаційних систем»** подану до захисту в разову спеціалізовану вчену раду Національного університету «Одеська політехніка» Міністерства освіти і науки України на здобуття наукового ступеню доктора філософії за спеціальністю 122 – «Комп'ютерні науки», галузь знань 12 – «Інформаційні технології»

1. Актуальність теми дисертації

Дисертаційну роботу ІВАНОВОЇ Олени Миколаївни присвячено актуальній проблемі, а саме: вирішенню науково-прикладної задачі 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. Це дає змогу підвищити розрядність контрольних даних, які можуть бути замасковано збережені в програмному коді FPGA та збільшити кількість різновидів прихованого моніторингу програмного коду, контрольні дані яких зберігаються в такий спосіб.

Дефіцит доступного обсягу замаскованого зберігання контрольних даних при застосуванні еквівалентних перетворень програмного коду приводить до спрощення процесу потенційного зловмисного обходу моніторингу. Причиною такого спрощення є використання тільки контрольних даних малої розмірності та зменшення кількості видів прихованого моніторингу, які одночасно можуть бути застосовані до програмного коду FPGA-компонентів.

Спроби збільшити цей обсяг в межах наявних стеганографічних підходів до маскування контрольних даних стикаються з протиріччям між тим фактом, що програмний код FPGA являє собою точні дані, спотворення яких не є можливим, та неможливістю забезпечення достатнього для задач прихованого моніторингу обсягу зберігання даних за рахунок еквівалентних перетворень програмного коду FPGA.

Таким чином, тема дисертації, присвячена розробці моделей та методів гібридного стеганографічного зберігання контрольних даних в процесі прихованого моніторингу програмного коду FPGA-компонентів інформаційних систем, є **актуальною**. Вона відповідає поточним науковим і практичним розробкам, сприяючи підвищенню надійності та ефективності застосування розроблених програмних засобів і запропонованих моделей та методів, що в свою чергу дозволяє збільшити, порівняно з традиційними підходами, обсяг потенційно доступних додаткових даних, які можуть бути приховано вбудовані в

програмний код FPGA .

Зміст дисертаційної роботи, її основні задачі, відповідають пп. 1.2.1.1, 1.2.1.2, 1.2.1.4 і 1.2.4.6 «Основних наукових напрямів та найважливіших проблем фундаментальних досліджень у галузі природничих, технічних, суспільних і гуманітарних наук Національної академії наук України на 2019–2023 роки» (постанова Президії НАН України від 30.01.2019 р. № 30).

На основі теоретичних результатів дисертації було отримано патент України на винахід.

Дослідження та розробка моделей та методів гібридного інформаційно маскованого зберігання контрольних даних для прихованого моніторингу програмного коду FPGA-компонентів інформаційних систем виконувалися у відповідності до планів дослідницьких робіт Національного університету «Одеська політехніка» в межах держбюджетної НДР № 99-145 (ДР №0115U000833).

Таким чином, можна констатувати, що дисертаційна робота ІВАНОВОЇ Олени Миколаївни є, безперечно, *актуальною* та має важливе науково-практичне значення.

2. Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації

Аналіз змісту дисертаційної роботи і наукових публікацій ІВАНОВОЇ Олени Миколаївни дають змогу зробити висновок про те, що основні наукові положення, висновки і рекомендації, які сформульовано в дисертаційній роботі, відповідають темі досліджень, їх достовірність забезпечено коректністю визначення об'єкту та предмету дослідження, які узгоджено з метою і задачами наукового дослідження.

Дисертаційна робота включає вступ, чотири розділи, висновки, список використаних джерел і додатки.

У вступі обґрунтовано актуальність та доцільність дисертаційного дослідження; показано зв'язок роботи з науковими програмами, планами, темами; сформульовано мету та задачі дослідження, наукову новизну та практичне значення одержаних результатів; визначено методи дослідження; зазначено особистий внесок здобувача, наведено дані про апробацію результатів дисертаційних досліджень та публікації. Кожен наступний розділ чи підрозділ органічно пов'язано з попереднім і гармонійно доповнює його.

Для дисертації характерна системність та ясність викладення матеріалу, чітка аргументація.

Достовірність наукових положень, висновків і рекомендацій, отриманих у дисертаційній роботі, підтверджена результатами теоретичних та експериментальних досліджень а також впровадженням запропонованих рішень.

Достовірність отриманих результатів додатково підтверджується даними числових експериментів, результати яких повністю узгоджуються з теоретичними засадами і концепціями у галузі інформаційних технологій.

Наукові положення, висновки та рекомендації, що виносяться до захисту, і які сформульовано в дисертації, відповідають вимогам Міністерства освіти і науки України до подібних досліджень, що підтверджує їх коректність та аргументованість. Ступінь обґрунтованості сформульованих автором наукових положень, висновків і рекомендацій підтверджуються системним аналізом літературних джерел з досліджуваної теми, а також, не останньою чергою, забезпечено завдяки вдалому застосуванню комплексу

загальнонаукових і спеціальних методів дослідження.

Висновки по дисертаційній роботі підкреслюють наукову новизну та практичну цінність проведених досліджень. Вони цілком обґрунтовані, коректні та логічно впливають з викладеного матеріалу.

Список використаних джерел свідчить про те, що під час роботи було проаналізовано сучасні результати наукових досліджень.

Ознайомлення з текстом дисертації дозволяє констатувати актуальність розробки автором досліджуваної проблематики в цілому, відокремлення найбільш важливих задач у межах предмету проведеного дослідження, а також, обґрунтованість наявних наукових положень, висновків і рекомендацій, сформульованих у роботі.

3. Наукова новизна одержаних результатів

Дисертація ІВАНОВОЇ Олени Миколаївни є завершеною кваліфікаційною науковою роботою, що присвячена вирішенню актуальної науково-прикладної задачі 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. У дисертаційній роботі сформульовано і обґрунтовано низку теоретичних положень, пропозицій та висновків, які містять ознаки наукової новизни, а саме:

- розроблено модель замаскованого зберігання даних в середовищі програмного коду FPGA-компонентів, *яка ґрунтується 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;*

- 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;*

- 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 приховані 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.*

Таким чином, на базі запропонованих моделей та розроблених методів, створено програмну підсистему гібридного замаскованого зберігання контрольних даних в складі

інформаційної системи прихованого моніторингу програмного коду FPGA-компонентів. Використання розробленої підсистеми, а також запропонованих моделей та методів дозволило збільшити порівняно з традиційним підходом обсяг потенційно доступних додаткових даних, які можуть бути приховано вбудовані в програмний код FPGA в стеганографічний спосіб.

Основні результати дисертації висвітлено у 14 наукових публікаціях, 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 збірниках матеріалів міжнародних і всеукраїнських науково-практичних конференцій.

Дисертаційна робота відповідає чинним вимогам щодо обсягу та змісту наукових публікацій, у яких представлено основні результати виконаного дослідження.

Участь у наукових семінарах та конференціях додатково свідчить про ознайомлення наукової спільноти з результатами дисертаційного дослідження. Кількість опублікованих праць відповідає вимогам, що встановлені МОН України щодо дисертацій на здобуття ступеню доктора філософії.

Таким чином, вимоги Постанови КМУ від 06.03.2019 № 167 «Про присудження ступеня доктора філософії» зі змінами згідно Постанови КМУ №979 від 21.10.2020 та від 09.06.2021 №608 до кількості публікацій виконано.

4. Значення роботи для науки та практики

Наукові досягнення, які здобуто в дисертаційній роботі, підкреслено, зокрема, в емпіричній базі дисертаційної роботи, а саме: висновками, які отримано в результаті серії експериментальних досліджень ефективності запропонованих моделей та методів. Використання розроблених програмних засобів, а також запропонованих моделей та методів дозволило збільшити, порівняно з традиційним підходом, обсяг потенційно доступних додаткових даних, які можуть бути приховано вбудовані в програмний код FPGA в стеганографічний спосіб в середньому від 22,6% до 34,0% за рахунок використання надлишкового ресурсу несуттєвих блоків LUT FPGA та збільшити цей обсяг в середньому від 93,7% до 105,1% за рахунок використання двох видів виявлених надлишкових ресурсів: несуттєвих блоків LUT FPGA та несуттєвих розрядів суттєвих блоків LUT FPGA. Це дає змогу підвищити розрядність контрольних даних, які можуть бути замасковано збережені в програмному коді FPGA та збільшити кількості різновидів прихованого моніторингу програмного коду, контрольні дані яких зберігаються в такий спосіб.

На основі теоретичних результатів дисертації було отримано патент України на винахід.

Розроблені в роботі методи та інструментальні засоби впроваджені у діяльність товариства з обмеженою відповідальністю ТЕХНО.КОМ (довідка про впровадження від 10 грудня 2025 року).

Отримані в роботі результати, а також програмні засоби впроваджено в навчальний процес європейських університетів за міжнародним ERASMUS+ проектом “ALIOT – Internet of Things: Emerging Curriculum for Industry and Human Applications” 573818-EPP-1-2016-1-UK-EPPKA2-CBHE-JP, а також в навчальний процес Національного університету «Одеська політехніка» при викладанні дисципліни “Технології захисту інформації”.

5. Відсутність (наявність) порушення академічної доброчесності

В результаті вивчення дисертаційної роботи порушень академічної доброчесності не виявлено. Всі запозичення, які є в роботі, мають посилання на відповідні джерела, інші – є загальноновживаними і не є плагіатом.

Публікації здобувачем результатів досліджень у рецензованих виданнях, які передбачають попередню перевірку матеріалів на відсутність запозичень, є одним із важливих підтверджень відсутності порушень академічної доброчесності.

6. Дискусійні положення та зауваження щодо змісту дисертації

Дисертаційну роботу написано на високому науковому рівні, робота містить значну кількість прикладів, що сприяє кращому розумінню матеріалу.

Проте є окремі зауваження:

1. В дисертаційній роботі, в алгоритмі локалізації ресурсів, недостатньо чітко формалізовано критерій та межі допустимої похибки.

2. Етапи 2, 3 та 4 в гібридному методі зберігання замаскованих даних виконуються в послідовності, яка задана вектором пріоритетів. Тому прив'язка номерів етапів до назв стего-ресурсів, які ці етапи використовують, ускладнює розуміння суті методу.

3. Оцінка стійкості виглядає суто емпіричною.

4. У третьому розділі на стор.123 згадується можливість замаскованого зберігання додаткових даних еквівалентним способом поверх вже прихованих у нееквівалентний спосіб даних. Однак надалі в роботі ця можливість не згадується. Доцільно було б дослідити та оцінити таку можливість збереження додаткових даних.

5. В дисертаційній роботі доцільно було б більше уваги приділити висвітленню питання обчислювальної складності базового алгоритму локалізації несуттєвих LUT для великомасштабних FPGA-проектів».

6. В тексті недостатньо розмежовані терміни «стеганографічний ресурс» та «стеганографічний простір» а також не має пояснення співвідношення між термінами «програмний код FPGA» та «інформаційний об'єкт програмного коду FPGA».

7. В тексті дисертаційної роботи присутні стилістичні та граматичні огріхи та помилки.

В цілому, вказані зауваження не впливають на високий науковий рівень роботи і самого проведеного дисертаційного дослідження.

7. Загальний висновок про відповідність роботи встановленим вимогам

Дисертаційна робота, яка представлена на рецензію, є закінченою кваліфікаційною науковою працею, яка містить раніше не захищені наукові положення і одержані автором нові науково обґрунтовані результати в області сучасної стеганографії.

В підсумку, з оглядом на актуальність проблеми та науковий внесок автора в теорію і практику області розвитку і впровадження підходів до зберігання контрольних даних, що базуються на стеганографічних методах, а також високий рівень виконаних досліджень та результати практичного впровадження, 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 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 січня 2022 року №44, із змінами, внесеними згідно з Постановою КМ № 341 від 21.03.2022, № 502 від 19.05.2023 та № 507 від 03.05.2024, а її автор О.М. Іванова, заслуговує на присудження їй ступеня доктора філософії за спеціальністю – 122 Комп’ютерні науки, галузь знань – 12 Інформаційні технології.

Кандидат технічних наук,
доцент кафедри
комп’ютеризованих систем та
програмних технологій
Національного університету
«Одеська політехніка»

Світлана ГРИГОРЕНКО