Голові спеціалізованої вченої ради Д 26.002.29
у Національному технічному університеті України
«Київський політехнічний інститут
імені І. Сікорського»

03056, м. Київ, пр. Берестейський 37

ВІДГУК

офіційного опонента
на дисертацію Прогонова Дмитра Олександровича
«Структурний синтез та параметрична оптимізація методів побудови стегодетекторів для цифрових зображень»,
представлену до захисту на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 — системи захисту інформації

Актуальність теми дисертаційної роботи. Розвиток методів боротьби з стеганографічними каналами несанкціонованої передачі даних є важливою частиною сучасної інформаційної безпеки в контексті боротьби зі складними та прихованими загрозами.

Актуальність представленої роботи визначається низкою важливих практичних та наукових викликів існуючих у сфері стегоаналізу цифрових зображень. Сучасні стегодетектори часто покладаються на наявність апріорних даних щодо особливостей стеганографічних методів, що обмежує їх ефективність. Для надійного виявлення стеганограм у випадках, коли рівень заповнення зображення стегоданими є мінімальним, існуючі методи демонструють обмежену точність. Зокрема, труднощі виникають при застосуванні методів пакетної стеганографії, де традиційні стеганодетектори не забезпечують достатньо високої точності виявлення прихованих повідомлень.

Практична актуальність цієї теми також підкреслюється необхідністю обробки великих обсягів цифрових зображень, що мають різні статистичні, спектральні та структурні параметри. Нелінійна залежність точності стегодетекторів від характеристик оброблюваних зображень вимагає адаптації або використання ансамблів стегодетекторів, що значно ускладнює їх налаштування та збільшує час обробки.

Ще одна проблема полягає в деструкції стеганограм. Використання деструктивних методів часто призводить до змін характеристик зображення, що демаскує факт втручання та може викликати зміну параметрів стеганографічних методів, що використовуються зловмисниками.

Вирішення вищеозначених проблем обумовлює актуальність дисертаційної роботи Прогонова Д.О. на тему «Структурний синтез та параметрична оптимізація методів побудови стегодетекторів для цифрових зображень», яка присвячена побудові високоточних методів виявлення стеганограм, здатних надійно працювати в умовах відсутності апріорних допоміжних даних щодо використаних стеганографічних методів та малого ступеня заповнення зображення-контейнера

приховуваними даними.

Зв'язок роботи з науковими програмам, планами, темами. Тематика роботи та отримані результати безпосередньо пов'язані зі «Стратегією національної безпеки України» від 14 вересня 2020 № 392/2020 та Законом України «Про основні засади забезпечення кібербезпеки України» від 24.10.2020 №2163-VIII у контексті гарантування кібербезпеки національної інформаційної інфраструктури, зокрема в умовах цифрової трансформації, а також розвитку та вдосконалення системи технічного і криптографічного захисту інформації, визначених в Концепції забезпечення національної системи стійкості, ухваленої Указом Президента України № 479/2021 від 27.09.2021 року. Робота проводилася у рамках науково-дослідних робіт кафедри інформаційної безпеки КПІ ім. Ігоря Сікорського, у тому числі держбюджетній науково-дослідній роботі «Кета» (держ. реєстр. № 0114U004643).

Загальна характеристика роботи. Дисертаційна робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел з 255 найменувань та додатків. Загальний обсяг роботи становить 434 сторінки з яких 266 сторінок основного тексту.

У вступі обґрунтовано актуальність теми дисертаційної роботи, показано зв'язок роботи з науковими темами, сформульовано мету і завдання дослідження, визначено об'єкт, предмет та методи досліджень, сформульовано наукову новизну та практичне значення отриманих результатів.

За *мету* роботи обрано вирішення важливої науково-прикладної проблеми – розробки методів синтезу стеганографічних детекторів з високою вірогідністю виявлення стеганограм в умовах відсутності апріорних даних щодо стегометоду та мінімальним заповнення зображення-контейнера приховуваними даними. У якості *об'єкту дослідження* обрано процеси виявлення стеганограм при обробці, зберіганні та передачі цифрових зображень в інформаційно-комунікаційних системах. Оцінка ефективності в роботі побудована на забезпеченні надійності виявлення стеганограм та мінімізації змін статистичних, спектральних та структурних параметрів оброблюваних зображень при знищені вбудованих даних. Для досягнення поставленої мети сформульовано ряд наукових задач, які досить повно розглянуті у розділах дисертації.

Перший розділ присвячено проведенню всебічного аналізу сучасного стану досліджень по проблематиці роботи, а саме аналізу сучасних моделей і методів приховування інформації у цифрових зображеннях та методів виявлення стеганограм. Особлива увага приділяється новітнім методам виявлення стеганограм з використанням статистичного, спектрального та структурного аналізу, а також штучних нейронних мереж. Встановлено, що ключова увага при розробці сучасних стеганографічних методів спрямована на мінімізацію змін у статистичних, спектральних та структурних параметрах контейнеру при створенні стеганограм. Результати порівняльного аналізу ефективності виявлення стеганограм, створених за новітніми адаптивними стегометодами, показали, що висока ймовірність виявлення прихованих повідомлень (понад 90%) досягається лише при середньому рівні заповнення зображення приховуваними даними не менше ніж 10%.

Підвищення точності виявлення при низькому рівні заповнення вимагає значного ускладнення обробки зображень, що ускладнює адаптацію стегодетекторів до нових типів стеганографічних методів. Штучні нейронні мережі дозволяють подолати ці обмеження, але лише при обробці зображень, статистичні характеристики яких схожі з навчальною вибіркою. Для забезпечення високої точності виявлення стеганограм такі стегодетектори потребують використання прикладів стеганограм під час налаштування, що ускладнює їх застосування для виявлення нових, раніше невідомих стеганографічних методів.

Результати проведеного у першому розділі аналізу дозволили обґрунтувати необхідність розробки нової концепції побудови стегодетекторів для проведення «сліпого» стегоаналізу зображень, які здатні ефективно виявляти стеганограми без наявності попередньої інформації про використовувані методи. Досягнення цієї мети вимагає визначення факторів, що найбільше впливають на точність існуючих стегодетекторів, а також розробки методів, які забезпечать високу точність виявлення стеганограм навіть без апріорних даних про використовувані стеганографічні методи.

У другому розділі досліджено межі ймовірності виявлення стеганограм залежно від наявних апріорних даних щодо стеганографічного методу та статистичних параметрів цифрових зображень. Також запропоновано методи, які дозволяють наблизити точність роботи стегодетектора до встановлених меж, незалежно від типу використовуваного стегометоду.

Для подолання обмежень сучасних підходів, запропоновано інтегральну модель оцінки точності роботи стегодетектора, яка враховує впливи попередньої обробки зображень, визначення їхніх параметрів та класифікації. Також була оцінена ефективність кластерів векторів, що відповідають статистичним параметрам стеганограм та зображень-контейнерів. Особливу увагу приділено методам оцінки відстаней між розподілами яскравості пікселів зображень-контейнерів та стеганограм за допомогою таких метрик, як відстань Хеллінгера, Бхаттачарайї, χ^2 і спектр відстаней Реньї. Дослідження показали, що відстань Хеллінгера є більш точною в порівнянні з іншими методами, забезпечуючи значне підвищення точності виявлення стеганограм, зокрема при використанні новітніх стеганографічних методів (HUGO, MiPOD та інші).

Також запропоновано оптимальні методи попередньої обробки зображень для мінімізації помилки класифікації стеганограм в умовах обмеженості апріорних даних. Ці методи дозволяють реконструювати оригінальні зображення-контейнери та видаляти спотворення, які викликані приховуванням даних, що може бути корисним для деструкції стеганограм та маскування факту втручання в канал зв'язку.

Експериментальні результати підтвердили ефективність запропонованих методів, які дозволяють суттєво підвищити точність виявлення стеганограм навіть у випадку низького ступеня заповнення зображень-контейнерів приховуваними даними. Зокрема, використання методу $\mathcal{K}_{opt}^{CE}(\mathbf{X}, \mathbf{Y})$ дозволило зменшити помилку класифікації на 20%, що є значним результатом в умовах слабкого заповнення.

Нарешті, запропоновано математичний апарат для синтезу структури та параметричної оптимізації стегодетекторів, що використовує спеціальні системи функцій для обробки зображень. Це дозволяє підвищити точність виявлення стеганограм навіть при використанні новітніх методів і забезпечує стабільність роботи стегодетектору незалежно від типу стеганографічного методу.

Зважаючи на отриману високу точність роботи стегодетекторів, заснованих на використанні запропонованого методу, у випадку виявлення стеганограм від відомих стегометодів, подальший інтерес автора був направлений на дослідження точності стегодетектору у найбільш складних випадках стегоаналізу, а саме виявлення апріорно невідомих стеганографічних методів при обробці нових пакетів цифрових зображень.

У третьому розділі проведено порівняльний аналіз точності роботи новітніх стегодетекторів, а також запропонованого методу синтезу стегодетекторів у найбільш складних випадках стегоаналізу цифрових зображень). До цих випадків належать відсутність апріорних даних щодо стеганографічного методу та значна варіативність статистичних, спектральних і структурних параметрів зображень.

На основі запропонованого методу синтезу високоточних стегодетекторів було розроблено програмний комплекс для стегоаналізу цифрових зображень, названий *Blind-Steg*. Особливістю цього комплексу є те, що він не потребує апріорних даних про використаний стегометод, що дозволяє ефективно виявляти стеганограми навіть у складних умовах. Експерименти показали, що *Blind-Steg* здатен суттєво знизити помилку класифікації стеганограм (до чотирьох разів) у порівнянні з сучасними стегодетекторами, при цьому забезпечуючи швидку обробку зображень — до трьох секунд на одне зображення.

Крім того, *Blind-Steg* продемонстрував високу точність реконструкції зображень-контейнерів, що відкриває нові можливості для деструкції стеганограм. Це також створює потенціал для вирішення сучасних задач у сфері стегоаналізу, таких як вилучення та підміна прихованих повідомлень.

Четвертий розділ присвячено аналізу перспектив використання комплексу *Blind-Steg* для вирішення задач надійної деструкції даних та визначення шляхів для екстракції прихованої інформації. У розділі показано, що застосування методу попередньої обробки цифрових зображень шляхом декомпозиції з використанням спеціальних систем функцій дозволяє значно знизити кількість пікселів, які залишаються незміненими після деструкції стеганограм. Це забезпечує ефективну деструкцію навіть у складних випадках слабкого заповнення зображень-контейнерів стегоданими.

Результати показали, що застосування запропонованого методу дозволяє до 12 разів зменшити кількість пікселів, які не були змінені в процесі деструкції (з 89,65% до 7,12%), що підвищує надійність деструкції. Це також зменшує зміни статистичних, спектральних і структурних параметрів оброблюваних стеганограм до шести разів у порівнянні з сучасними методами деструкції. Такий підхід сприяє ефективній протидії роботі стеганографічних каналів передачі інформації, маскуючи сам факт деструкції від приймальної сторони.

Також у розділ показано, що точність визначення позицій пікселів, використаних для приховування стегоданих, є надзвичайно високою. Це відкриває нові

можливості для вилучення або підміни бітів стегоданих без необхідності деструкції всієї стеганограми. Запропонований метод дозволяє до чотирьох разів підвищити точність локалізації таких пікселів у порівнянні з мережею SR-Net, і ця висока точність зберігається навіть у випадку слабкого заповнення стегоданими.

Таким чином, методи, реалізовані у комплексі *Blind-Steg*, відкривають нові можливості для вирішення найскладніших задач стегоаналізу. Це включає вилучення та підміну прихованих повідомлень без необхідності проведення повної деструкції стеганограм. Висока точність визначення позицій пікселів, що перевищує 60%, навіть при слабкому заповненні контейнеру стегоданими, підтверджує перспективність застосування запропонованого підходу для роботи з новітніми стеганографічними методами.

Висновки дисертаційної роботи підкреслюють наукову новизну та практичну цінність проведених досліджень. Основні результати мають як теоретичну, так і практичну складову, створюючи в сукупності методологію розробки ефективної крипто-стеганографічної системи для потокових контейнерів.

У додатках містяться документи, що підтверджують впровадження результатів дисертаційної роботи, а також результати дослідження точності виявлення стеганограм при використанні сучасних статистичних стегодетекторів цифрових зображень та стегодетекторів, сформованих на основі запропонованого методу синтезу структури та оптимізації їх параметрів.

Таким чином, усі положення, які винесені на захист, висвітлені в тексті дисертації. Зміст дисертаційної роботи відповідає її назві. Дисертація написана науковою мовою та оформлена відповідно до існуючих нормативних документів. Побудова дисертації відповідає прийнятим для наукового дослідження вимогам. Зміст та структура роботи у повній мірі відповідають завданню з викладення основних результатів вирішення поставленої наукової проблеми та сформульованим окремим задачам дослідження, які відповідають паспорту спеціальності 05.13.21 — системи захисту інформації.

Ступінь обґрунтованості наукових положень, висновків та рекомендацій, сформульованих в дисертації, їх достовірність. Обґрунтованість та достовірність наукових положень, висновків та рекомендацій дисертаційної роботи Прогонова Д.О. підтверджується ґрунтовним аналізом сучасних літературних джерел, чітким формулюванням мети, основних завдань досліджень та шляхів їх реалізації. Достовірність наукових положень дисертації підтверджується значним обсягом експериментальних досліджень. Інтерпретація результатів досліджень узгоджуються з фундаментальними положеннями методів спектрального та компонентного аналізу, методів статистичного моделювання, методів теорії оптимізації та розпізнавання образів, даними інших дослідників.

Достовірність результатів досліджень підтверджується численними результатами тестування відомих та запропонованих стегодетекторів на стандартних пакетах тестових зображень ALASKA, VISION та MIRFlickr-1M загальною кількістю близько 1 мільйона зображень.

Отримані результати апробовані на авторитетних міжнародних вітчизняних та закордонних конференціях.

Наукова новизна отриманих автором результатів. У результаті виконання дисертаційної роботи набув подальшого розвитку науковий напрям стеганографії, пов'язаний з синтезом стеганографічних детекторів з високою вірогідністю виявлення приховуваних даних. Виходячи з того, що нові наукові результати – це нові знання в певній галузі фундаментальних чи прикладних наук, основними науковими результатами дисертації можна вважати такі:

1. *Вперше визначено оптимальні методи* попередньої обробки досліджуваних зображень за критерієм мінімізації помилки виявлення стеганограм при розробці стегодетектору, що спрямовані на визначення положення та подальше вилучення локальних збурень значень яскравості пікселів контейнеру, обумовлених прихованням повідомлень. Застосування запропонованих методів при синтезі стегодетекторів дозволило наблизити точність їх роботи до теоретичних оцінок досяжної ймовірності виявлення стеганограм у всьому діапазоні змін ступеня заповнення зображення-контейнера стегоданими, що є недосяжним при використанні відомих методів попередньої обробки, заснованих на знешумленні оброблюваних зображень.

2. *Вперше розроблено метод* для забезпечення надійного виявлення змін статистичних, спектральних та структурних параметрів контейнеру, обумовлених вбудовуванням стегоданих, який заснований на реконструкції вихідного виду зображення-контейнеру із застосуванням спеціальних систем функцій в якості базису перетворення досліджуваного зображення, що дозволяє створювати високоточні стегодетектори, які здатні надійно працювати в умовах «сліпого» стегоаналізу цифрових зображень, при збереженні відносно низької обчислювальної складності процедури налаштування стегодетектору.

3. *Вперше запропоновано метод* визначення положення пікселів контейнеру, використаних для приховання окремих стегобітів повідомлення, який заснований на представленні задачі локалізації пікселів як задачі сегментації досліджуваного зображення. Це дозволило не тільки підвищити ефективність методів деструкції стегоданих при забезпеченні мінімального впливу на статистичні та спектральні параметри цифрового зображення, а й створити передумови для розробки методів вилучення (екстракції) стегоданих зі стеганограм.

4. *Удосконалено метод* синтезу структури та оптимізації параметрів високоточних стегодетекторів шляхом заміни декількох складних етапів налаштування стегодетектору на вирішення оптимізаційної задачі максимізації відстані Хеллінгера між кластерами векторів, що відповідають статистичним параметрам зображення-контейнеру та сформованих стеганограм. Це дало можливість забезпечити високу вірогідність виявлення стеганограм незалежно від способу їх формування.

5. *Удосконалено метод* робастної оцінки відмінностей між імовірнісними розподілами значень яскравості пікселів зображення-контейнеру та стеганограм, що відрізняється використанням спеціальних показників, а саме відстані Хеллінгера, відстані Бхаттачарайя, χ^2-квадрат відстані та спектру відстаней Реньї. Це дозволило суттєво (до двох разів) підвищити точність виявлення стеганограм навіть в умовах обробки пакетів цифрових зображень, що характеризуються високим ступенем варіації статистичних, спектральних та структурних параметрів.

6. *Удосконалено методи* підвищення точності роботи стегодетектору у випадку обмеженості апріорних даних щодо використаного стегометодів шляхом зниження впливу нелінійних зв'язків між статистичними параметрами досліджуваних зображень за рахунок проекції векторів, які відповідають статистичним параметрам зображення-контейнеру та сформованих стеганограм, до простору вищої розмірності. Це дозволяє збільшити кількість інформативних параметрів цифрового зображення при проведенні стегоаналізу та, відповідно, підвищити точність виявлення стеганограм без необхідності використання обчислювально складних методів попередньої обробки.

7. *Набули подальшого розвитку методи* деструкції стеганограм за рахунок використання варіаційних методів аналізу багатовимірних сигналів для зниження впливу адитивних шумів при проведенні реконструкції вихідного виду зображення-контейнеру за наявними (зашумленими) даними, що дає можливість підвищити точність оцінки його параметрів у широкому діапазоні зміни параметрів адитивних завад та, відповідно, забезпечити надійну деструкцію стеганограм.

Практичне значення результатів, отриманих в дисертаційній роботі полягає в доведенні здобувачем отриманих наукових результатів до реалізації конкретних методів і алгоритмів, що можуть бути використане для проведення стегоаналізу цифрових зображень при вирішення широкого спектру задач з виявлення, вилучення та деструкції повідомлень, вбудованих в зображення.

1. Доведено, що сучасні методи стегоаналізу цифрових зображень мають обмеження через необхідність використання апріорних даних про стеганографічні методи та статистичні параметри зображень. Це ускладнює швидку адаптацію до нових стеганографічних методів. Запропонований метод синтезу високоточних стегодетекторів вирішує цю проблему, не вимагаючи апріорних даних.

2. Розроблено метод формування спеціальних функцій для точного відновлення вихідного зображення-контейнера навіть за наявності значних адитивних завад. Метод є ефективний і не потребує великої кількості вихідних даних, що робить його перспективним для аналізу різних типів сигналів.

3. Метод реконструкції зображення-контейнера показав свою ефективність у складних випадках, зокрема для маскування втручання в стеганографічний канал. Він мінімізує зміни параметрів зображення і надійно знищує вбудовані стегодані.

4. Алгоритмічна реалізація запропонованих методів дозволила розробити програмний комплекс стегоаналізу цифрових зображень, який може виявляти, вилучати та знищувати вбудовані повідомлення. Комплекс ефективний навіть в умовах "сліпого" стегоаналізу і може використовуватися для протидії стеганографічним каналам в інформаційних системах.

Практичне значення отриманих результатів підтверджене актами впровадження у діяльність ДСНС України, конструкторського бюро «Шторм», центру досліджень та розробок «Самсунг РнД Інститут Україна», а також в навчальний процес механіко-математичного факультету КНУ ім. Тараса Шевченка, кафедри

телекомунікаційних та радіоелектронних систем Національного авіаційного університету і кафедри інформаційної безпеки КПІ ім. Ігоря Сікорського.

Цінність дисертаційної роботи для науки. Рекомендації щодо використання результатів дисертації. Цінність дисертації полягає в тому, що в ній запропоновано нове рішення важливої науково-технічної проблеми в теорії побудови ефективних стеганографічних детекторів аналізу цифрових зображень. Змістовний аспект запропонованих рішень спрямовано на розробку науково-обґрунтованої методології, орієнтованої на пошук стеганограм у цифровому зображені, і значно покращує ефективність порівняно з сучасним станом в цій сфері. Запропоновані у роботі методи побудови стегодетекторів для цифрових зображень можуть бути використані при реалізації ефективних систем стеганографічного аналізу.

Відповідність теми і змісту дисертації паспорту спеціальності, за якою вона подана на захист. Тема дисертації та її зміст відповідають формулі й галузі досліджень відповідно до положень, що викладені у паспорті спеціальності 05.13.21 – системи захисту інформації.

Ідентичність змісту автореферату й основних положень дисертації. Автореферат дисертації за своїм змістом з необхідною повнотою відповідає викладеним у дисертаційній роботі результатам, в ньому ідентично відображено загальну характеристику, основній зміст та висновки роботи. Стиль викладення автореферату в цілому забезпечує повноту та доступність сприйняття. Наукові задачі дослідження та шляхи їх вирішення викладені чітко і лаконічно. З тексту зрозуміла наукова і практична значущість роботи та особистий внесок здобувача.

Мова та стиль дисертації. Дисертація написана державною мовою. Виклад матеріалу в роботі має логічну послідовність, наукова термінологія є загальновизнаною, розділи взаємопов'язані та цілком розкривають поставлену мету, стиль викладення результатів досліджень, нових наукових положень та висновків забезпечує доступність їх сприйняття. Результати проілюстровані високоякісними рисунками та графіками.

Розглянувши звіт подібності за результатами перевірки дисертаційної роботи на текстові співпадіння, можна зробити висновок, що дисертаційна робота Прогонова Д.О. є результатом самостійних досліджень і не містить елементів фальсифікації, компіляції, фабрикації, плагіату та запозичень. Використані ідеї, результати і тексти інших авторів мають належні посилання на відповідне джерело.

Повнота викладення та апробації основних результатів дисертаційної роботи у наукових публікаціях. Результати дисертації достатньо повно відображені у ***54*** наукових працях, у тому числі: ***21*** статті у фахових виданнях (з них *8* у міжнародних наукових журналах, що входять до наукометричних баз Scopus та Web of Science), ***3*** міжнародні патенти на винахід та ***30*** тез доповідей на міжнародних науково-практичних конференціях і семінарах в Україні та закордоном. Усього одноосібних статей - ***16***. Зазначені публікації повною мірою висвітлюють основні наукові положення дисертації як на вітчизняному,

так і на міжнародному рівнях.

Таким чином, кількість опублікувань результатів роботи та їх якість відповідає вимогам ВАК України до докторських дисертацій.

Дискусійні положення та зауваження щодо дисертаційної роботи:

1. У першому розділі, автор аналізуючи стан наукових досліджень у сфері криптоаналізу обрав у якості об'єкту досліджень найбільш поширені стегометоди: багатоетапні та адаптивні методи приховання повідомлень у цифрові зображення, зокрема засновані на вбудовуванні повідомлень в просторовій області та в області перетворення зображення-контейнеру. Але це не охоплює весь перелік відомих стегометодів для цифрових зображень, бо існують й інші стегометоди (наприклад, приховування в альфа-каналі, приховування через векторне кодування (VQ Steganography), розсіяного приховування (Spread Spectrum), приховування на основі фракталів та інші), дослідження яких слабо представлено у науковій літературі. За логікою, зловмисник для досягнення своєї мети має обрати один з цих слабо досліджених методів. Тому, при аналізі сучасного стану криптоаналізу зображень, автору доцільне було більш ґрунтовно аргументувати границі свого дослідження стеганометодів, проаналізувати переваги та недоліки інших методів, оцінити можливість застосування розробленої технології синтезу стеганодетекторів або її модифікації до таких методів.

2. Слід було б навести більш детальне обґрунтування використання в якості класифікатору зображень-контейнерів та стеганограм саме ансамблю лінійних дискримінантів Фішера замість поширених методів класифікації, зокрема методу опорних векторів (Support Vector Machine, SVM), багатошарового персептрона тощо.

3. В дисертації використовується теоретична оцінка досяжної точності виявлення стеганограм при використанні квадратичного закону (англ. Square Root Law), який використовується для дослідження ϵ-стійких методів приховання повідомлень. Зокрема, розглянуто випадок оцінки значення помилки виявлення стеганограм P_E^{lim}, запропонованої в роботах Фрідріх Д., проте не наведено даних щодо результатів дослідження при використанні інших методів оцінок P_E^{lim}.

4. Бажано б було навести оцінки швидкодії запропонованих методів при роботі у реальних системах контролю та моніторингу інформаційно-комунікаційних систем або їх модулів для виявлення прихованих каналів передачі даних.

5. Також становить інтерес дослідження ефективності запропонованих методів виявлення стеганограм при використанні різних пакетів тестових зображень, зокрема пакету BOSS, а також новітніх методів приховання повідомлень у просторовій області (наприклад Synch) та пакетних методів (зокрема J2-UNIWARD, Clustered-SI).

Представлені зауваження не носять визначальними характеру та жодним чином не знижують позитивне враження про роботу та її наукову новизну та практичну значимість результатів.

Загальний висновок щодо відповідності дисертації встановленим вимогам. Дисертаційна робота Прогонова Дмитра Олександровича «Структурний синтез та параметрична оптимізація методів побудови стегодетекторів для

цифрових зображень» є завершеним науковим дослідженням, виконаною здобувачем самостійно, характеризується єдністю змісту, містить нові наукові положення та обґрунтовані теоретичні результати, які підтверджено результатами проведених експериментів і відповідними документами впровадження. В цілому робота забезпечує суттєвий внесок в теорію та практику побудови високоточних стегодетекторів для цифрових зображень.

Усі результати, що виносяться на захист є достовірними та отримані автором особисто. Робота відповідає принципам академічної доброчесності. Наявність академічного плагіату, фабрикації, фальсифікації не виявлено. Використання результатів, які виносилися на захист в кандидатській дисертації, у даній роботі не виявлено.

Вважаю, що за актуальністю обраної теми, обсягом та рівнем теоретичних і експериментальних досліджень, достовірністю та обґрунтованістю висновків, новизною досліджень, значенням отриманих результатів для науки і практики дисертаційна робота задовольняє вимогам пп.7, 8 та 9 «Порядку присудження та позбавлення наукового ступеня доктора наук», затвердженого Постановою Кабінету Міністрів України від 17 листопада 2021 року №1197, а її автор, **Прогонов Дмитро Олександрович**, ***заслуговує*** присудження наукового ступеню доктора технічних наук за спеціальністю 05.13.21 – системи захисту інформації.

Офіційний опонент -
професор кафедри кібербезпеки та математичного моделювання
Національного університету «Чернігівська політехніка»,
заслужений діяч науки і техніки України,
лауреат Державної премії України в галузі науки і техніки,
доктор технічних наук, професор **М. Шелест**

«01» жовтня 2024 року

Підпис професора кафедри кібербезпеки
та математичного моделювання
Національного університету
«Чернігівська політехніка»,
д.т.н. М.Є.Шелеста
засвідчую проректор з наукової роботи А.Л. Приступа