Вченому секретареві
спеціалізованої вченої ради Д 26.062.17
у Національному авіаційному університеті
03680, м. Київ, пр. Космонавта Комарова, 1

В І Д Г У К

офіційного опонента, професора кафедри безпеки інформаційних систем і технологій Харківського національного університету імені В.Н. Каразіна доктора технічних наук, професора Кузнецова Олександра Олександровича на дисертацію Кінзерявого Олексія Миколайовича «Стеганографічні методи приховування даних у векторні зображення, стійкі до активних атак на основі афінних перетворень», подану на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації

1. Актуальність теми дисертації

Відповідно до законів України "Про основи національної безпеки України", "Про інформацію", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про Національну систему конфіденційного зв'язку" та інших нормативно-правових актів із захисту національного інформаційного простору України, серед основних реальних та потенційних загроз національній безпеці в інформаційній сфері найпоширенішими та найнебезпечнішими визнаються комп'ютерна злочинність та комп'ютерний тероризм. Стрімкий розвиток новітніх інформаційних технологій та розповсюдження сучасних комп'ютерних систем та мереж, окрім надання якісних інформаційних послуг, зумовлюють і суттєве збільшення ризиків та можливих загроз інформаційній безпеці, загостюють існуючі протиріччя між необхідністю оброблення та передачі великих обсягів інформації у визначені терміни та підвищення вимог до їх вірогідності та безпеки. Саме тому серед основних напрямків державної політики з питань національної безпеки України в інформаційній сфері є впровадження новітніх технологій для розвитку національної інформаційної інфраструктури та ресурсів, вжиття комплексних заходів щодо захисту національного інформаційного простору, розробка та дослідження сучасних методів та обчислюваних алгоритмів криптографічного та стеганографічного перетворення.

Стеганографічні системи та протоколи набувають останніми роками бурхливого розвитку. Це пов'язано із можливим їх застосуванням для забезпечення різних послуг інформаційної безпеки, зокрема, для підтвердження автентичності, справжності, авторського права у складі цифрових водяних знаків, для забезпечення конфіденційності інформації та прихованості каналів управління, інших методів протидії комп'ютерній злочинності та комп'ютерному тероризму. Саме дослідженню стеганографічних методів

захисту інформації присвячено дисертаційну роботу Кінзерявого О.М., в якій розглядаються питання приховування даних у нерухомих зображеннях-контейнерах із використанням як структурних особливостей побудови самого контейнера, так і властивостей органів зорового сприйняття людини. Тема дисертації є актуальною та пов'язаною із виконанням: «Основних наукових напрямів та найважливіших проблем фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук на 2009–2013 роки» (затверджених наказом МОН України та НАН України № 1066/609 від 26.11.2009), держбюджетної науково-дослідної роботи «Організація систем захисту інформації від кібератак» (№ 0111U000171), «Методи та моделі стеганографічного захисту інформації від кібератак» (№ 101/14.01.06), «Методи забезпечення конфіденційності державних інформаційних ресурсів в інформаційно-комунікаційних системах» (№ 61/09.01.08), що проводились за планами НДР Національного авіаційного університету.

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

2.1. **У першому розділі** дисертаційної роботи проведено аналіз вітчизняної та зарубіжної літератури за темою дисертаційного дослідження. Зокрема, автором обґрунтовано вибір напрямку дослідження стеганографічних методів захисту інформації для організації резервного (прихованого та захищеного) каналу зв'язку з дипломатичними установами. При цьому в якості контейнерів пропонується використовувати невеликі файли в популярних форматах (наприклад, зображення з фотографіями місцевих визначних пам'яток). Файли невеликого розміру можуть легко передаватися по мережах з невисокою швидкістю передачі даних, навіть у разі їх високої завантаженості. На підставі того, що стеганографічні методи, які використовують растрові, фрактальні зображення, погано протистоять активним стеганоатакам, автор робить висновок про перевагу саме векторних зображень у якості перспективних контейнерів-зображень. Далі автором проводиться короткий огляд відомих стеганографічних методів із застосуванням векторних зображень, розглядається сутність застосовуваних перетворень, розкриваються їхні переваги та недоліки. Також розглядаються відомі активні атаки на стеганосистеми з векторними зображеннями, акцентується увага на афінних перетвореннях та проводяться порівняльні дослідження стійкості відомих стеганоалгоритмів до відповідних атак. Розділ закінчується постановкою задачі дисертаційного дослідження, в якій, на підставі аналізу характеристик сучасних мобільних мереж передачі даних та середньостатистичних властивостей векторних зображень, обґрунтовуються конкретні обмеження та параметри стеганосистеми (кількість вбудованої інформації в контейнер, множина припустимих атак, коефіцієнт візуального спотворення зображення, тощо). У висновках по розділу акцентується увага за здобутих результатах та напрямках подальшого дослідження.

Недоліки та зауваження по першому розділу дисертації.

1. Автор наголошує на створенні резервних каналів зв'язку з дипломатичними установами. Але спочатку потрібно переконатися, що такі канали взагалі потрібні. Тобто треба отримати погодження із профільними міністерствами та відомствами, або, принаймні, вказати, згідно з якими нормативно-правовими актами, планами, темами проводяться такі дослідження. У вказаних науково-дослідних роботах немає згадки про зацікавленість саме дипломатичних установ. Загалом, проведені дослідження цікаві не тільки для побудови закритих каналів з дипломатичними установами, коло можливого впровадження результатів роботи може бути значно ширшим.
2. Найбільшу цінність в першому розділі має п. 1.2 «Аналіз стеганографічних методів приховування інформації у векторні зображення», бо саме змістовна частина цього підрозділу свідчить про глибоке розуміння автором проблематики дослідження, його обізнаність з останніми досягненнями світової науки у певній галузі знань. Однак, поряд із викладенням сутності основних стеганоперетворень, потрібно було б і критично висвітлити ті проблемні питання та недоліки, які притаманні тим чи іншим методам, наведені результати не досить змістовні. Наприклад, на с. 26 вказується: «…методи характеризуються слабкою стійкістю до активних атак…». Але кількісна оцінка стійкості не проводилася, наведені в таблиці 1.1. (с. 33) порівняння носять якісний характер.
3. Висновки по розділу скоріше нагадують анотацію – це найпоширеніша помилка здобувачів. Наприклад, п.2: «Проведено аналіз сучасних методів приховування інформації, що використовують у якості контейнера векторні зображення». Треба наголосити на результатах проведеного аналізу, що вони дають нового для теорії чи практики в певній галузі знань.

2.2. **Другий розділ** дисертації присвячено формалізації вимог до вибору контейнера, визначенню параметрів приховування інформації у векторні зображення та розробці методів вбудовування даних у точково-задані криві. Зокрема, автором вводяться основні визначення та аналітичні співвідношення, які застосовуються при обробці векторної графіки, акцентується увага на окремих параметрах, значення яких безпосередньо впливає на вибір контейнера та процес вбудовування/вилучення інформації (ступінь кривої, відстань між опорними точками кривої та їх точність, припустима похибка, тощо). У розділі розробляються два методи приховування даних: метод побітового приховування інформації (п. 2.3) та метод шаблонного приховування (п. 2.4). Наведені приклади дозволяють наглядно переконатися в конструктивності запропонованих рішень. Розділ закінчується розробкою структурної моделі процесу прихованої передачі інформації резервним каналом зв'язку із наведенням псевдокоду процедур попереднього шифрування. Саме цей розділ

дисертації містить нові наукові результати, отримані автором особисто, викладені положення свідчать про високий рівень підготовки здобувача та його здатність самостійно вирішувати складні наукові завдання.

Недоліки та зауваження по другому розділу.

1. Другий розділ за задумом автора містить викладення головних ідей та гіпотез дисертаційного дослідження, які покладено в основу вирішення наукового завдання. Саме це, на мою думку, і є головним результатом діяльності дослідника. Запропоновані ідеї та розробки дійсно є оригінальними та новими, але не вирішують всіх проблем приховування даних у векторних зображеннях, зокрема:
   - наголошується стійкість запропонованих методів до активних атак на основі афінних перетворень. На жаль, зовсім не розглянуто випадок перезапису зображення в іншому форматі з повторним перезаписом у векторному вигляді. Ця активна атака буде, на мою думку, досить ефективною, вбудована інформація буде втрачена. Вже відомі методи, на які автор посилається і з якими порівнює свої пропозиції (на основі ортогональних перетворень, наприклад, Фур'є) будуть, вочевидь, мати певний запас стійкості. Отже, можна говорити про досягнення стійкості тільки до афінних перетворень, запропоновані методи мають переваги в вузькому класі застосувань;
   - запропоновані методи мають й інші недоліки. Зокрема, побітний метод призводить до значного збільшення обсягу зображення, пропорційного обсягу вбудованих даних (точніше, числу одиниць в повідомленні). Шаблонний метод призводить до збільшення складності перетворень (по експоненті із збільшенням довжини повідомлення зростає обсяг таблиці відповідностей).
2. Стиль викладення п. 2.1 «Принцип вбудовування інформації у векторні зображення» більше підходить до навчального посібника, як і висновки за розділом. У висновках у вигляді анотацій наголошено на тому, що зроблено (розроблено методи, запропоновано модель). Потрібно було наголосити на результатах дослідження цих моделей та методів, на властивостях отриманих результатів, їхніх характеристиках, обмеженнях до застосування, рекомендаціях, тощо.

2.3. **У третьому розділі** дисертаційної роботи розробляються обчислювальні алгоритми стеганографічного приховування інформації запропонованими методами. Для цього автор спочатку досліджує типи кривих, що використовуються у векторній графіці, вивчає їхні властивості, аналізує алгоритми побудови та розбиття кривих Без'є для їх подання через сукупність сегментів. Потім докладно розробляє алгоритми приховування секретних повідомлень у криві Без'є векторних зображень як побітним, так і шаблоним методом, які були запропоновані у другому розділі дисертації. Розділ добре проілюстровано наведеними псевдокодами розроблених процедур та

прикладами приховування та вилучення даних, що наочно демонструють конструктивність та працездатність розроблених алгоритмів. Висновки по розділу узагальнюють отримані результати та конкретизують їх можливості та переваги.

Третій розділ є, на мою думку, найбільш вдалою частиною дисертації, стиль та мова викладення найбільш природньо розкривають змістовну частину, а саме – результати розробки та дослідження обчислювальних алгоритмів стеганографічних перетворень із застосуванням кривих Без'є. Як на мне, цей розділ свідчить про високий рівень підготовки здобувача саме як програміста, здатного формалізувати складні обчислювальні процеси та реалізовувати їх у програмному вигляді.

2.4. **У четвертому розділі** автором проводяться експериментальні дослідження ефективності розроблених методів та алгоритмів. Спочатку викладається методика проведення експериментальних досліджень, потім розробляється необхідне програмне забезпечення на мові програмування C++ в середовищі Microsoft Visual Studio 2012. За текстом дисертації наводяться зображення користувальницького інтерфейсу із докладним описом застосовуваних полів та органів керування, описано режими роботи програмної реалізації та вихідні дані для проведення досліджень. Далі досить докладно викладаються отримані результати експериментів: оцінка швидкості перетворень, коефіцієнтів візуального спотворення, порівняння кількості втрачених біт при різних афінних перетвореннях, результати порівняння із іншими методами – найближчими аналогами. Проведені дослідження є досить масштабними, бо тільки викладення основних результатів займає майже 40 сторінок основної частини дисертації та 30 сторінок додатків, кожен випадок тестувався на багатьох прогонах моделі із усередненням результатів. Загалом, змістовна частина цього розділу свідчить про зрілість та підготовленість здобувача, вміння планувати проведення експерименту, обробляти його результати, узагальнювати отримані дані та робити обґрунтовані висновки.

Недоліки та зауваження по четвертому розділу дисертації.

1. Наведені результати експериментальних досліджень усереднювалися за 100 ітераціями (прогонами моделі). Але для обґрунтування вірогідності отриманих результатів потрібно було навести оцінки точності та довірчої ймовірності, або, принаймні, показники розсіювання (купчастості) відносно статистичного середнього.
2. Оцінка швидкості стеганографічних перетворень проведена на різних обчислювальних платформах із використанням процесорів різних виробників, і це добре. Однак, окрім апаратної складової, на швидкодію впливають також особливості програмного забезпечення, операційна система, інтегровані спеціальні графічні пакети програм, тощо. Доцільно було дослідити й ці питання, як впливає зміна операційної системи чи застосовані графічні пакети на оцінки швидкодії.

3. Не проведено дослідження «негативних ефектів» запропонованих методів, тобто тих чинників, які є «платою» за досягнення корисного ефекту. Наприклад, для побітового методу такою «платою» є збільшення обсягу зображення. Для шаблонного методу із збільшенням довжини приховуваного повідомлення повинно спостерігатися збільшення складності перетворень. Саме ці ефекти і є найбільш цікавими, бо саме вони розкриють галузь практичного використання здобутих результатів.

3. Достовірність отриманих результатів

Достовірність результатів, які отримав автор дисертаційної роботи, підтверджується збіжністю отриманих результатів експериментальних досліджень шляхом імітаційного та комп'ютерного моделювання з теоретичними результатами та аналітичними співвідношеннями. Достовірність результатів обґрунтовується їх несуперечністю основним положенням теорії захисту інформації, методам математичного та комп'ютерного моделювання, об'єктно-орієнтованого програмування, тощо.

Для підтвердження отриманих наукових положень автором проведено експериментальне дослідження щодо перевірки швидкісних характеристик, коефіцієнту візуального спотворення, зміни розмірів стеганоконтейнерів та стійкості розроблених алгоритмів до атак на основі афінних перетворень, результати яких показали ефективність запропонованих алгоритмів приховування інформації у векторні зображення.

4. Новизна отриманих результатів

У дисертаційній роботі Кінзерявого О.М. «Стеганографічні методи приховування даних у векторні зображення, стійкі до активних атак на основі афінних перетворень» отримано теоретичне узагальнення та нове вирішення актуальної науково-технічної задачі, яка полягає в розробці нових та удосконалені існуючих стеганографічних методів приховування інформації у векторні зображення з метою підвищення стійкості до активних атак на основі афінних перетворень.

Найбільш суттєві наукові результати дисертаційної роботи.

1. Вперше визначено множину параметрів приховування даних, які враховують особливості побудови векторних зображень та особливості стеганографічних перетворень, що дозволяє формалізувати вимоги до вибору контейнерів та впливати на процес приховування інформації у точково-задані криві.

2. Вперше розроблено метод побітового приховування інформації у точково-задані криві, який дозволяє приховувати один біт секретного повідомлення при поділі кривих на сегменти, забезпечуючи при цьому високу

швидкодію приховування/вилучення даних та підвищує стійкість до атак на основі афінних перетворень.

3. Вперше розроблено метод шаблонного приховування інформації у точково-задані криві, який дозволяє приховувати блок секретного повідомлення при поділі кривих на сегменти, при цьому зменшуючи розміри стеганоконтейнерів, підвищуючи швидкість вбудовування та стійкість до атак на основі афінних перетворень.

5. Завершеність, стиль викладення, публікації

5.1. Аналіз сукупності наукових результатів і положень, характеристику яких наведено в пп. 2–4, дозволяє зробити висновок про їх внутрішню єдність і засвідчує особистий внесок автора у науку. У дисертаційній роботі отримано розвиток нових стеганографічних методів приховування інформації у векторні зображення для підвищення стійкості до активних атак на основі афінних перетворень. Це має суттєве значення для розбудови сучасних систем захисту інформації та дає можливість підвищити ефективність стеганографічного перетворення інформації.

5.2. Дисертація є завершеною науковою роботою, виконаною і оформленою відповідно до затверджених вимог.

5.3. Дисертаційна робота написана зрозуміло і грамотно, науково-технічна термінологія використовується коректно, структура роботи логічна.

5.4. Основні результати досліджень опубліковані досить повно в 14 наукових працях, з них: 7 статей у фахових виданнях України (6 з яких входять до міжнародних наукометричних баз даних), а також 7 тез доповідей на конференціях. В дисертаційній роботі та в авторефераті наведено дані щодо особистого внеску здобувача до всіх праць, які опубліковані у співавторстві.

5.5. Структура і зміст автореферату повністю відповідає тексту дисертації.

6. Практична значимість дисертаційної роботи полягає в наступному.

6.1. Розроблено структурну модель процесу прихованої передачі інформації резервним каналом зв'язку, що дозволяє формувати множину стеганоконтейнерів, стійких до афінних перетворень.

6.2. Розроблено нові стеганографічні алгоритми приховування інформації у криві Без'є третього ступеня, що можуть бути використані для підвищення стійкості до атак на основі афінних перетворень.

6.3. Розроблено методики та програмні засоби для проведення експериментальних досліджень, що дозволяє оцінити ефективність приховування інформації запропонованими методами.

6.4. Практична цінність роботи підтверджена актами впровадження у науково-технічних розробках ТОВ «Сайфер ЛТД», ТОВ «Каскад Груп Україна»

та у навчальному процесі кафедри безпеки інформаційних технологій Національного авіаційного університету.

7. Недоліки та зауваження

Основні недоліки та зауваження викладено при аналізі наукових результатів дисертанта (п.2). Додатково слід відзначити необхідність засвідчувати авторський пріоритет шляхом патентування власних розробок автора дисертації.

Вказані недоліки та зауваження не впливають на загальний позитивний висновок про дисертаційну роботу.

8. Загальні висновки

8.1. Дисертація є закінченою науково-дослідною роботою, яка містить теоретичне узагальнення та нове рішення актуальної науково-технічної задачі, яка полягає в розробці нових та удосконалені існуючих стеганографічних методів приховування інформації у векторні зображення, з метою підвищення стійкості до активних атак на основі афінних перетворень.

8.2. Здобувач отримав нові науково-обґрунтовані результати, що в сукупності мають суттєве значення як для розвитку окремих методів сучасної теорії захисту інформації, так і для вирішення прикладних питань з підвищення ефективності стеганографічного перетворення.

8.3. Зміст дисертації відповідає паспорту спеціальності 05.13.21 – системи захисту інформації.

8.4. Дисертаційна робота Кінзерявого О.М. «Стеганографічні методи приховування даних у векторні зображення, стійкі до активних атак на основі афінних перетворень» має певну наукову новизну і практичну значимість у галузі безпеки інформаційних систем і технологій, відповідає вимогам п. 9, 11 та 12 «Порядку присудження наукових ступенів і присвоєння вченого звання старшого наукового співробітника», а її автор заслуговує присудження наукового ступеня кандидата технічних наук.

Професор кафедри безпеки інформаційних систем і технологій
Харківського національного університету ім. В.Н. Каразіна
доктор технічних наук, професор О.О. Кузнецов

"14" 09 2015 р.

Підпис доктора технічних наук, професора Кузнецова О.О. засвідчую