# ВІДГУК

**офіційного опонента на дисертацію**
**Кінзерявого Олексія Миколайовича**
**"Стеганографічні методи приховування даних у векторні зображення, стійкі до активних атак на основі афінних перетворень",**
**представлену на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації**

Детальний аналіз дисертації Кінзерявого О.М. "Стеганографічні методи приховування даних у векторні зображення, стійкі до активних атак на основі афінних перетворень" дозволяє сформулювати наступні узагальнені висновки щодо актуальності, ступеня обґрунтованості основних наукових положень, висновків, рекомендацій, достовірності, наукової новизни, практичного значення, а також загальної оцінки роботи.

**Актуальність.** З розвитком у нашій країні інформаційного суспільства інформаційна безпека стала важливою частиною національної безпеки держави. Значна увага приділяється науковому та технічному забезпеченню розробки сучасних методів та засобів захисту інформації, що викликано рядом проблем у галузі безпеки інформаційних технологій. Для їх ефективного вирішення використовується ціла низка заходів до яких можуть включатися стеганографічні засоби захисту. До сучасних стеганографічних систем та методів накладають ряд вимог яким вони повинні володіти для забезпечення надійного захисту, а саме: повинні мати здатність протидіяти відомим методам стеганографічного аналізу та мати запас стійкості із врахуванням тенденцій розвитку засобів електронно обчислювальної техніки й стеганографічної науки, повинні забезпечувати безпомилкову передачу даних та інші. Одними із атак застосовуваних до стеганографічних методів, які використовують в якості контейнерів зображення, є афінні перетворення. Останні дослідження показали слабку стійкість існуючих методів до даних перетворень. Тому, існує необхідність в розробці нових та удосконалення існуючих методів приховування інформації в зображення з метою підвищення стійкості до атак на основі афінних перетворень. На вирішення цієї задачі спрямована дисертаційна робота Кінзерявого О.М. "Стеганографічні методи приховування даних у векторні зображення, стійкі до активних атак на основі афінних перетворень".

Одержані автором результати реалізовано в рамках держбюджетної науково-дослідної роботи "Організація систем захисту інформації від кібератак" (№ 0111U000171) та кафедральних науково-дослідних робіт "Методи та моделі стеганографічного захисту інформації від кібератак" (№ 101/14.01.06) і "Методи забезпечення конфіденційності державних інформаційних ресурсів в інформаційно-комунікаційних системах" (№ 61/09.01.08).

**Оцінка обґрунтованості та достовірності наукових положень, висновків та рекомендацій.**

Оцінка змісту дисертаційної роботи Кінзерявого В.М. дозволяє зробити висновок про те, що автор виконав роботу згідно з встановленою загальноприйнятою послідовністю, методологічно грамотно, структура і оформлення дисертаційної роботи відповідають державному стандарту України ДСТУ 3008-95. Матеріал дисертаційної роботи має збалансоване співвідношення між дослідженням стану питання, теоретичними дослідженнями обраного наукового напрямку і розробкою програмних засобів для практичної реалізації одержаних результатів.

Викладені наукові положення, висновки є повністю обґрунтованими, а достовірність теоретичних положень підтверджується результатами експериментальних досліджень запропонованих алгоритмів побітового та шаблонного приховування інформації у векторні зображення. Отримані під час експериментів дані відповідають теоретичним висновкам роботи і підтверджують їх.

У **вступі** автор виклав загальну характеристику роботи, обґрунтував актуальність, сформулював мету і задачі досліджень, відобразив наукову новизну і практичну цінність отриманих результатів, навів дані про їх апробацію та впровадження.

У **першому розділі** проаналізовано вітчизняну та зарубіжну літературу за темою дисертаційного дослідження. Розглянуто спосіб організації резервного каналу зв'язку через загальнодоступну мережу Інтернет, скритність передачі інформації по якому забезпечується стеганографічними методами захисту. Проведено аналіз сучасних стеганографічних методів приховування інформації у векторні зображення. Визначено можливі види активних атак застосовуваних до векторних зображень, серед яких були виділені атаки на основі афінних перетворень. Проведено порівняння стійкості існуючих методів до афінних перетворень, що дало можливість обґрунтувати необхідність розробки нових більш ефективних стеганографічних методів приховування інформації у векторні зображення, для реалізації прихованого каналу зв'язки через глобальну мережу Інтернет.

У **другому розділі** запропоновано принцип приховування інформації у точково-задані криві векторних зображень. Визначено множину параметрів приховування інформації у векторні зображення, що дозволяють впливати на вибір допустимих контейнерів та процес вбудовування/вилучення інформації. Розроблено методи побітового та шаблонного приховування інформації у точково-задані криві векторних зображень, які дозволяють вбудовувати дані за рахунок поділу кривих на сегменти. Розроблено структурну модель процесу прихованої передачі інформації резервним каналом зв'язку, яка дозволяє формувати множину стеганоконтейнерів, стійких до афінних перетворень.

У **третьому розділі** проаналізовано основні типи точково-заданих кривих векторних зображень, які можуть бути використанні для

вбудовування інформації, серед яких були виділені криві Без'є. На основі методу побітового приховування інформації та властивостей кривих Без'є розроблено алгоритм StegoBIT, який дозволяє приховувати інформацію у криві Без'є третього ступеня шляхом їх розбиття на сукупності сегментів. Також, розроблено алгоритм StegoTEMPL, який, за рахунок впливу послідовності даних на процес сегментації кривих згідно визначеної таблиці співвідношень значень елементів шаблону різним крокам зміни параметра побудови кривих, дозволяє вбудовувати дані у криві Без'є третього ступеня та забезпечує стійкість до афінних перетворень.

У **четвертому розділі** розроблено методику проведення експериментального дослідження, визначено його мету, завдання, вхідні параметри та послідовність необхідних дій. На основі запропонованих алгоритмів StegoBIT та StegoTEMPL розроблено програмні засоби StegoInSVG-Bitwise та StegoInSVG-Template, що дозволяють приховувати інформацію у криві Без'є третього ступеня SVG зображень. Одержані результати стійкості розроблених алгоритмів до афінних перетворень типу перенесення, поворот, майже поворот, зсув та масштабування. Порівняно стійкість алгоритмів StegoBIT та StegoTEMPL з методом Карпінцева-Яремчука, які показали підвищення стійкості до афінних перетворень.

У **додатках** приведені акти впровадження результатів дисертаційної роботи, параметри та результати експериментального дослідження стійкості розроблених алгоритмів до афінних перетворень, а також приведені лістинги програмних засобів (StegoInSVG-Bitwise та StegoInSVG-Template), що приховують інформацію у криві Без'є третього ступеня SVG зображень.

**Наукова новизна отриманих результатів.**

**1.** *Вперше* визначено множину параметрів приховування даних у векторні зображення, які, за рахунок врахування особливостей побудови векторних зображень та особливостей стеганографічних перетворень, дозволяють 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 векторних зображень, який, за рахунок впливу послідовності даних на процес сегментації кривих, забезпечує високу швидкодію приховування, вилучення секретного повідомлення та підвищує стійкість до активних атак на основі афінних перетворень.

**3.** *Вперше* розроблено метод шаблонного приховування інформації у точково-задані криві векторних зображень, який, за рахунок впливу послідовності даних на процес сегментації кривих згідно визначеної таблиці шаблонів, дозволяє зменшити розміри стеганоконтейнерів, підвищити швидкість вбудовування та стійкість до активних атак на основі афінних перетворень.

Основні положення дисертаційної роботи опубліковано у 7 статтях у фахових виданнях України (6 з яких входять до міжнародних наукометричних баз даних) та 7 тезах доповідей на конференціях.

Для основних положень дисертації та змісту автореферату характерна ідентичність.

**Значення результатів для науки та практики.**

Практична цінність роботи полягає у тому що: розроблено структурну модель процесу прихованої передачі інформації резервним каналом зв'язку, яка дозволяє формувати множину стеганоконтейнерів, стійких до афінних перетворень; розроблено два нові стеганографічні алгоритми приховування інформації у криві Без'є третього ступеня, що можуть бути використані для підвищення стійкості до активних атак на основі афінних перетворень; розроблено програмні засоби, що дозволяють приховувати інформацію у криві Без'є третього ступеня SVG зображень.

Отримані результати дисертаційної роботи впроваджено у навчальному процесі кафедри безпеки інформаційних технологій Національного авіаційного університету та у науково-технічних розробках ТОВ "Сайфер ЛТД", ТОВ "Каскад Груп Україна", що підтверджено відповідними актами впровадження.

**Дискусійні положення та зауваження щодо дисертаційного дослідження.**

Не дивлячись на істотні здобутки роботи дисертація Кінзерявого О.М. має вразливі місця, щодо яких необхідно зробити певні зауваження.

1. У табл. 1.1 наводиться порівняння стійкості стеганографічних методів приховування інформації у векторні зображення до афінних перетворень. Не зрозуміло, яким чином автор проводив порівняння розглянутих методів.

2. Запропоновані автором методи мають недоліки, що ускладнює їхнє використання: при вбудовування інформації суттєво збільшується розмір стеганоконтейнерів (більше ніж 2 рази); потрібно передавати адресату додаткову інформацію для вилучення секретного повідомлення.

3. Було б доцільно розглянути та порівняти можливості вбудовування інформації в інші точково-задані криві векторних зображень (наприклад: B-сплайни та NURBS-криві), що дозволило б краще оцінити ефективність розроблених автором методів.

4. У роботі автор досліджує стійкість запропонованих алгоритмів до атак на основі афінних перетворень. На мою думку, було б доцільно також провести дослідження стійкості даних алгоритмів до інших видів активних атак наведених у п.1.3 розділу 1.

5. У роботі порівнюється стійкість розроблених методів (алгоритмів) лише з одним методом приховування інформації на основі дискретно косинусного перетворення. Вважаю, доцільним проведення порівняння їх стійкості з більшою кількістю існуючих методів, що приведені в аналізі (розділ 1, п.1.2).

В той же час, як видно, висловлені зауваження мають дискусійний характер та не можуть вплинути на достатній науковий рівень, новизну та достовірність результатів дисертації Кінзерявого О.М.

**Загальна оцінка дисертаційної роботи**

У цілому дисертаційна робота Кінзерявого О.М. є закінченою науковою працею, яка містить нові науково обґрунтовані теоретичні та експериментальні результати, що у сукупності є суттєвими для розвитку наукового напрямку – цифрова стеганографія. Одержані наукові результати можуть також застосовуватися в інших галузях науки і техніки, де необхідно вирішувати задачі пов'язані із захистом електронних інформаційних ресурсів від атак на основі афінних перетворень.

Дисертаційна робота "Стеганографічні методи приховування даних у векторні зображення, стійкі до активних атак на основі афінних перетворень" повністю відповідає вимогам ДАК МОН України, а її автор Кінзерявий Олексій Миколайович заслуговує присудження наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації.

## ОФІЦІЙНИЙ ОПОНЕНТ

Завідувач кафедри програмного забезпечення,
Кіровоградського національного технічного університету
доктор технічних наук, професор О.А. Смірнов

«14» 09 2015 року

Підпис Смірнова О.А. засвідчую:
Проректор з наукової роботи
Кіровоградського національного технічного університету
д.е.н., професор О.М. Левченко