67-72-53/2
07.04.2023 р.

Голові спеціалізованої вченої ради Д35.052.18
у Національному університеті
«Львівська політехніка»

79013, м. Львів, вул. С. Бандери 12

ВІДГУК
офіційного опонента
на дисертацію Соколова Артема Вікторовича
«Методологія розробки ефективної крипто-стеганографічної системи»,
представлену до захисту на здобуття наукового ступеня доктора технічних наук
за спеціальністю 05.13.21 □ Системи захисту інформації

Актуальність теми дисертаційної роботи. Розвиток та широке впровадження у повсякдення інформаційних технологій робить завдання захисту інформації надзвичайно важливим як для забезпечення безпеки держави, так і для забезпечення безпеки і добробуту конкретного громадянина. Сучасний вектор розвитку інформаційних технологій передбачає повсюдне впровадження ресурсообмежених пристроїв, які оперують зростаючими потоками мультимедійного контенту. Означене потребує переосмислення деяких принципів побудови систем захисту інформації, зокрема, інтеграції криптографічної та стеганографічної складових. Виникле нове поняття «крипто-стеганографічна система».

Сучасні підходи побудови крипто-стеганографічних систем для мультимедійного середовища здебільше застосовують сингулярні розкладання та дискретні косинус перетворення. Це призводить до суттєвого збільшення обчислювальної складності таких систем, а, відповідно, збільшують їх габарити, енергоспоживання та зменшується час автономної роботи, що унеможливлює їх використання на ресурсобмежених пристроях.

Тобто склалося об'єктивне протиріччя між наявною необхідністю використання ресурсобмежених платформ при реалізації крипто-стеганографічних систем та наявністю ресурсозатратних стеганографічних перетворень контейнера.

З іншого боку, існуючий інструментарій побудови криптографічної компоненти крипто-стеганографічних систем базується лише на математичному апараті булевих функцій, та не враховує можливе уявлення криптографічних конструкцій функціями багатозначної логікі. Як показують останні дослідження, висока якість криптографічних примітивів при їх уявленні функціями багатознач-

ної логіки дозволяє значно підвищити рівень дифузії та конфузії, що є дуже перспективним для їх реалізації у складі крипто-стеганографічних систем ресурсообмежених пристроїв.

Вищеозначене обумовлює актуальність обраної теми дисертаційної роботи Соколова А. В., яка присвячена побудові методології розробки ефективних крипто-стеганографічних систем, що здатні працювати з потоковими контейнерами в режимі реального часу на сучасних ресурсообмежених пристроях, забезпечивши приховування шифрованої інформації у просторовій області контейнера.

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.

Загальна характеристика роботи. Дисертаційна робота складається зі вступу, шести розділів, висновків, списку використаних джерел з 336 найменувань і додатку.

У вступі обґрунтовано актуальність теми дисертаційної роботи, показано зв'язок роботи з науковими темами.

За мету обрано вирішення важливої науково-прикладної проблеми - забезпечення ефективної роботи крипто-стеганографічних систем в режимі реального часу на ресурсообмежених платформах шляхом розробки науково-обґрунтованої методології, яка орієнтована на приховування шифрованої інформації у просторовій області потокового контейнера. У якості об'єкту дослідження обрано процеси створення відповідних до мети крипто-стеганографічних систем. Оцінка ефективності роботи стеганографічної системи в роботі побудована на критеріях крипостійкості, швидкодії, стійкості до атак проти вбудованої інформації, забезпечення надійності сприйняття контейнеру та значної пропускної спроможності. Для досягнення поставленої мети сформульовано ряд наукових задач, які досить повно розглянуті у подальших розділах дисертації.

Перший розділ присвячено проведенню всебічного аналізу сучасного стану досліджень по проблематиці роботи, а саме: методів забезпечення ефективності стеганографічних перетворень, методів побудови та оцінки криптографічних примітивів, що володіють доведено високим рівнем криптографічної якості, ме-

тодів поєднання та узгодження роботи криптографічної та стеганографічної складових у єдину систему.

З аналізу витікає, що сучасні стеганографічні методи мультимедійного середовища застосовують просторові перетворення контейнеру, а найкращі методи, як правило, працюють в області сингулярного розкладання матриць блоків контейнера. Але такі методи є досить обчислювально складні, що фактично унеможливлює їх застосування на ресурсобмежених платформах.

З другого боку, криптографічні конструкції існуючих крипто-стеганографічних систем будуються лише із врахуванням їх представлення у вигляді компонентних булевих функцій, що робить їх вразливими до можливих атак за допомогою представлення у вигляді функцій багатозначної логіки. Це обмежує рівень дифузії та конфузії, який вони можуть забезпечити, а внаслідок ще й обмежує можливості для більш тісної інтеграції криптографічної та стеганографічної складових таких систем.

Таким чином, результати першого розділу підтверджують, що актуальна проблема забезпечення ефективності крипто-стеганографічних систем при їх роботі із потоковим контейнером на ресурсообмежених пристроях на сьогодні лишається невирішеною, що обумовлює актуальність теми дисертаційних досліджень.

Другий розділ дисертації присвячено розробці теоретичного базису для забезпечення заданих властивостей стенографічного перетворення при його виконанні у просторовій області потокового контейнеру, математичною основою якого є застосування перетворення Уолша-Адамара.

У розділі встановлено взаємозв'язок між двовимірними та одновимірними версіями перетворень Уолша-Адамара та дискретним косинус перетворенням (ДКП), який дозволив значно спростити подальші математичні викладки. Встановлено та доведено двома способами взаємозв'язок між трансформантами Уолша-Адамара та ДКП, а також сингулярним розкладанням матриць блоків контейнера, що дозволило сформулювати умови забезпечення певних властивостей стеганограми в області перетворень Уолша-Адамара, а також розробити концепцію кодового управління вбудовуванням додаткової інформації.

Розроблена концепція дозволяє шляхом використання того чи іншого кодового слова, яке додається до блоку контейнера у просторовій області, строго визначати вплив на ту чи іншу частотну складову контейнера, таким чином маніпулюючи властивостями стеганограми так, як це необхідно для конкретної поставленої задачі.

Третій розділ дисертації присвячений розробці та тестуванню стеганографічних методів з кодовим управлінням приховування інформації. Синтезовано бінарні та багаторівневі кодові слова, що здатні забезпечити зосереджений вплив на задані трансформанти перетворення Уолша-Адамара, і, відповідно, трансформанти перетворення ДКП. Введено поняття енергії та селективності кодового слова, доведено існування кодових слів, що володіють абсолютною селективністю. Теоретично підтверджено, що збільшення розміру кодового слова веде до збільшення стійкості стеганограми до атак на вбудоване повідомлення.

На основі розроблених бінарних та багаторівневих кодових слів представлено два стеганографічні методи з кодовим управлінням приховування додаткової інформації, тестування яких дозволило підтвердити, що незважаючи на те, що вони працюють у просторовій області, їх показники забезпечення надійності сприйняття і стійкості до атак перевищують подібні показники у відомих аналогів, зберігаючи при цьому пропускну спроможність на рівні найкращих з них.

У четвертому розділі розроблено стеганографічні методи з кодовим управлінням вбудовуванням додаткової інформації, які забезпечують множинний доступ до прихованого каналу зв'язку.

Проведені дослідження показали, що можливість організації множинного доступу до прихованого каналу зв'язку є природньою для концепції кодового управління вбудовуванням додаткової інформації, в результаті чого було розроблено два стеганографічні методи з множинний доступом: на основі кодів частотних розстановок та просторово-частотних матриць.

Розроблені методи мають значні переваги у порівнянні з існуючими аналогами: підвищена кількість зареєстрованих та активних абонентів, що працюють у системі, знижена обчислювальна складність, краще забезпечення надійності сприйняття, стійкість до атак проти вбудованого повідомлення, можливість незалежного вбудовування додаткової інформації користувачами системи у будь-який зручний для них час, гнучкість у розподіленні ресурсів прихованого каналу зв'язку.

Окрім цього, у четвертому розділі було покращено існуючий метод забезпечення множинного доступу до прихованого каналу зв'язку на основі технології MC-CDMA, в рамках чого за рахунок дослідження ймовірнісних характеристик трансформант Уолша-Адамара було підвищено пропускну спроможність групового тракту.

У п'ятому розділі розроблено теоретичний базис для оцінки криптографіч-

ної якості функцій багатозначної логіки, за допомогою яких можуть бути представлені існуючи криптографічні конструкції або які можуть стати основою для синтезу нових перспективних криптографічних конструкцій. Розроблено основні критерії криптографічної якості, які витікають з можливих атак криптоаналізу: алгебраїчна нелінійність, дистанційна нелінійність, критерій розповсюдження помилки та суворий лавинний критерій, критерій відсутності кореляційного зв'язку виходу функції багатозначної логіки та її вхідних змінних.

Представлено методи дослідження функцій багатозначної логіки на відповідність даним критеріям, що створює базу для оцінки та порівняння криптографічної якості практично застосовуваних функцій багатозначної логіки, що створює передумови для розробки нових, більш високоякісних криптографічних конструкцій для шифру прекодера, а також для розробки шифру для шифрування послідовності переліку станів, що забезпечуватиме узгодження криптографічної та стеганографічної складової крипто-стеганографічної системи.

Шостий розділ дисертаційної роботи присвячено проблемам підвищення криптографічної стійкості крипто-стеганографічних систем, а також дослідженню її характеристик при роботі із потоковим контейнером на ресурсобмеженому пристрою. Так, у розділі наводяться методи синтезу криптографічних примітивів, що володіють високим рівнем криптографічної якості як у сенсі представлення компонентними булевими функціями, так і компонентними функціями багатозначної логіки.

На основі розроблених криптографічних примітивів представлено шифр прекодера, спеціалізований шифр для шифрування послідовності переліку станів, а також модифіковано структурну схему крипто-стеганографічної системи на основі застосування кодового управління вбудовуванням додаткової інформації та шифрування послідовності переліку станів. Це дало можливість підвищити загальну криптозахищеність системи, забезпечити взаємозв'язок та врахувати взаємовплив її криптографічної та стеганографічної складових.

У розділі строго доведено гарантоване зниження обчислювальної складності стеганографічних методів що оперують у просторовій області у порівнянні з іншими методами, а також емпірично досліджено швидкодію запропонованої крипто-стеганографічної системи на сучасних ресурсообмежених пристроях, встановлено мінімально необхідні вимоги до процесора для підтримки роботи крипто-стеганографічної системи.

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, та лістинг розроблених програмних застосунків.

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 Соколова А.В. 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 матричного аналізу, теорії інформації та кодування, теорії досконалих алгебраїчних конструкцій, теорії Галуа, даними інших дослідників. 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, пов'язаний з методологією розробки стеганографічних систем, орієнтованих на приховування шифрованої інформації у просторовій області потокового контейнеру, та вирішено важливу науково-практичну проблему забезпечення ефективності роботи крипто-стеганографічної системи в режимі реального часу на ресурсообмежених платформах.

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 запропоновано науково-обґрунтовану методологію* розробки крипто-стеганографічної системи, яка забезпечує високу ефективність на ресурсообмежених платформах. Дана методологія базується на розробленій концепції

кодового управління вбудовуванням інформації та запропонованому методі здійснення стеганоперетворення із шифруванням послідовності переліку станів.

2. *Вперше встановлено взаємозв'язок* між трансформантами перетворення Уолша-Адамара, дискретним косинус перетворенням та сингулярним розкладанням матриці блоку контейнера, що дозволило сформулювати теоретичні основи достатніх умов забезпечення заданих властивостей стеганоповідомлення.

3. *Вперше сформовано достатні умови* забезпечення заданих властивостей стеганоповідомлення, що дозволило створити передумови для розробки теоретичних основ кодового управління вбудовуванням додаткової інформації у просторовій області контейнеру.

4. *Вперше розроблено стеганографічні методи* з кодовим управлінням вбудовуванням додаткової інформації, які характеризуються вищим рівнем ефективності при значно нижчій обчислювальній складності. Дані алгоритми побудовані на основі встановленого у роботі взаємозв'язку між трансформантами перетворення Уолша-Адамара, концепції кодового управління вбудовуванням додаткової інформації, а також синтезованих бінарних та багаторівневих кодових слів.

5. *Вперше запропоновано спосіб формування стеганографічного ключа, який* шифрує послідовність переліку станів, що дозолило підвищити криптографічну стійкість крипто-стеганографічної системи, забезпечити взаємозв'язок та врахувати взаємовплив її криптографічної та стеганографічної складової.

6. *Подальший розвиток технології множинного доступу* до прихованого каналу зв'язку за рахунок: використання кодів постійної амплітуди в технології MC-CDMA, двох запропонованих стеганографічних методів з множинним доступом, які базуються на кодах Ріда-Соломона та кодах просторових розстановок, що забезпечило підтримку роботи в системі до кількох тисяч користувачів та одночасну роботу кількох десятків користувачів, підвищило пропускну спроможність групового тракту в порівнянні з аналогами.

7. *Удосконалено математичний підхід* до дослідження якості криптографічних примітивів при їх представленні функціями багатозначної логіки, що дозволило синтезувати, дослідити та порівняти криптографічні примітиви при їх представленні функціями багатозначної логіки.

8. *Удосконалено криптографічні примітиви*, в рамках чого синтезовано множини S-блоків, які характеризуються високим рівнем криптографічної якості як при уявленні за допомогою компонентних булевих функцій, так і при уявленні

за допомогою функцій багатозначної логіки, що дозволило підвищити криптографічну якість конструкцій шифрів, які застосовуються у крипто-стеганографічних системах.

Практичне значення результатів, отриманих в дисертаційній роботі полягає в доведенні здобувачем отриманих наукових результатів до конкретних методів та алгоритмів, що можуть бути використані як складові систем захисту інформації.

Алгоритмічні реалізації розроблених методів дозволили забезпечити ефективність крипто-стеганографічних систем при роботі з потоковим контейнером на ресурсобмежених пристроях в режимі реального часу, зокрема, зменшенню кількості необхідних операцій для роботи стеганографічного методу з кодовим управлінням вбудовування додаткової інформації операцій.

На базі сконструйованих у роботі криптографічних примітиві розроблено спосіб формування стеганографічного ключа, а також удосконалений БСШ прекодер, які на відміну від відомих існуючих аналогів, враховують криптографічну якість не тільки компонентних булевих функцій, а і компонентних ФБЛ.

Практичне значення отриманих результатів підтверджене актами впровадження в діяльність ТОВ Компанія «Планета-Юг», ТОВ «Телекарт-прилад», ТОВ «Бізнес-центр НТЦ», ТОВ «Продукт – Постачання».

Рекомендації щодо використання результатів дисертації. Цінність дисертаційної роботи для науки. Цінність дисертації полягає в тому, що в ній запропоновано нове рішення важливої науково-технічної проблеми в теорії побудови ефективних крипто-стеганографічних систем. Змістовний аспект запропонованих рішень спрямовано на розробку науково-обґрунтованої методології, що орієнтована на приховуванні шифрованої інформації у просторовій області контейнера, не був відомий раніше. Запропоновані у роботі методи, технологія та конструкції можуть бути використані при реалізації ефективних систем крипто-стеганографічного захисту на ресурсообмежених платформах.

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.

Повнота викладення та апробації основних результатів дисертаційної роботи у наукових публікаціях. Результати дисертації достатньо повно відображені в **63** наукових працях, зокрема: 29 статей - у міжнародних виданнях (з них 26 у виданнях, що входять до наукометричних баз Scopus та Web of Science), а також 22 статті - у наукових фахових журналах та збірниках України. Усього одноосібних статей - 11. Основні положення дисертаційної роботи пройшли достатню апробацію на міжнародних науково-практичних конференціях та семінарах в Україні і закордоном та опубліковані у 17 матеріалах і тезах доповідей конференцій. В авторефераті і дисертації наведено дані щодо конкретного особистого вкладу здобувача. 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.

Зауваження щодо дисертаційної роботи та реферату.

1. У роботі розглядається питання стійкості стеганографічного методу з кодовим управління вбудовуванням додаткової інформації до атак стиском. Докладно в обчислювальних експериментах досліджено тільки алгоритм JPEG, однак на практиці можуть застосовуватися інші алгоритми (наприклад, WebP або JPEG2000).

2. Математичні основи та властивості стеганографічних методів з кодовим управлінням вбудовуванням додаткової інформації в роботі розглядаються для організації прихованого каналу зв'язку (розділ 3). Однак, немає ніяких принципових заперечень для використання цих методів для вбудовування цифрового водяного знаку, що розширює область застосування розроблених методів. В роботі це питання ніяк не висвітлене.

3. В якості показника степеню відповідності стеганоповідомлення критерію забезпечення надійності сприйняття обрано різницевий показник «пікове відношення «сигнал-шум» PSNR (співвідношення 3.3 і 3.4), але це ніяк не обґрунтовано в роботі. При цьому, навіть при високих своїх значеннях, цей показник не гарантує забезпечення надійності сприйняття стеганоповідомлення.

4. У запропонованому стеганографічному методі з множинним доступом на основі просторово-частотних матриць при застосуванні всіх частотних складових (табл. 4.8) різні користувачі матимуть різний рівень захищеності від атак проти вбудованого повідомлення, обумовлений частотними складовими, що потрапили у їх особистий набір частот, що застосовується для передавання інформації. Ця особливість не підкреслена у роботі.

5. Введена формула для визначення нелінійності функцій багатозначної логіки (співвідношення 5.52) для кількості змінних функцій багатозначної логіки $k \in [1,\infty)$, яка приймає значення у діапазоні $NL \in [0,\infty)$, що утруднює задачу порівняння між собою нелінійності функцій багатозначної логіки різних довжин для чого вочевидь було б доцільніше ввести показник нелінійності у відсотках відносно її максимального значення.

6. Відповідно до перетворення Ріда-Маллера над розширеними полями для значення $q = 16$ (співвідношення 5.28 і 5.31) стає очевидним, що алгебраїчний степінь нелінійності (як і алгебраїчна складність) конкретної функції багатозначної логіки може змінюватися відповідно до обраного ізоморфізму розширеного поля Галуа $GF(q)$, над яким знайдено АНФ. При цьому при збільшенні значення основи уявлення (наприклад, $q = 64, 256$) кількість можливих ізоморфізмів швидко зростає, що ставить задачу дослідження АНФ криптографічних конструкцій для всіх можливих ізоморфізмів. Цей аспект ніяк не висвітлено у дисертаційній роботі.

7. Незважаючи на заявлену можливість застосування розробленої криптостеганографічної системи у БПЛА, структурна схема системи, представлена на рис. 6.4, не дає принципового розуміння про те, яка саме інформація, що циркулює в інформаційній системі БПЛА, може бути захищеною за допомогою розробленої системи, виступаючи в якості додаткової інформації.

8. За рамками досліджень, представлених у дисертаційній роботі, залишилися питання щодо можливого розпаралелювання представлених стеганографічних методів, заснованих на концепції кодового управління вбудовуванням інформації, що має велике значення для архітектури сучасних обчислювальних систем, які орієнтовані на парадигму застосування багатоядерних процесорів.

Представлені зауваження не носять принципового характеру та жодним чином не знижують позитивне враження про роботу та її наукову та практичну цінність.

Оцінка змісту дисертації, її завершеність в цілому. Дисертаційна робота Соколова Артема Вікторовича «Методологія розробки ефективної крипто-

стеганографічної системи» 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, та вирішують важливу науково-прикладну проблему, пов'язану з методологією побудови крипто-стеганографічних систем реального часу на ресурсообмежених платформах, що орієнтовані на надійному приховуванні криптозахищеної інформації у просторовій області потокового контейнеру.

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 та 9 «Порядку присудження та позбавлення наукового ступеня доктора наук», затвердженого Постановою Кабінету Міністрів України від 17 листопада 2021 року №1197, а її автор, **Соколов Артем Вікторович**, ***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**

«12» березня 2023 року

Підпис професора кафедри кібербезпеки та математичного моделювання
Національного університету «Чернігівська політехніка», д.т.н. М.Є.Шелеста
засвідчую з наукової роботи Марасова В.Г.
вчений секретар

«__» березня 2023 року