67-72-53/1
07.04.2023р.

ВІДГУК

офіційного опонента

на дисертацію Соколова Артема Вікторовича «Методологія розробки ефективної крипто-стеганографічної системи»

подану до захисту на здобуття наукового ступеня доктора технічних наук

за спеціальністю 05.13.21 — Системи захисту інформації

1. Актуальність теми дисертації

Значне зростання обсягу мультимедійного контенту, зокрема цифрових відео, змінює вимоги до сучасних систем захисту інформації, призводить до необхідності одночасного застосування криптографічних та стеганографічних засобів захисту інформації, наслідком чого є формування поняття крипто-стеганографічної системи. Бурхливий розвиток мобільних пристроїв, кишенькових комп'ютерів, пристроїв Інтернету речей, БПЛА, вбудованих інформаційних систем, які активно працюють з потоковими контейнерами (у першу чергу, з цифровим відео), накладає суттєві обчислювальні обмеження на методи, що застосовуються для побудови систем захисту інформації. Означене часто призводить до неможливості застосування на вказаних пристроях крипто-стеганографічних систем, які на практиці замінюються лише криптографічним захистом, що призводить до суттєвого зниження загального рівня захищеності інформації.

Можна констатувати, що на сьогоднішній день важлива прикладна проблема забезпечення ефективності роботи крипто-стеганографічної системи на ресурсообмежених пристроях не знайшла свого розв'язку. Існуючі методи вбудовування криптозахищенної інформації передбачають застосування областей перетворення, що призводить до їх значної обчислювальної складності, збільшення рівня помилок при декодуванні через похибки округлення при переході з однієї області контейнера в іншу, порушення надійності сприйняття через непередбачуваність змін контейнера в просторовій області при впливі на нього в області перетворень. Застосовувані у сучасних крипто-стеганографічних системах криптографічні примітиви та шифри на їх основі побудовані лише із врахуванням їх уявленні за допомогою математичного апарату булевих функцій, що зменшує можливий рівень дифузії та конфузії, який вони здатні забезпечити, а, таким чином, збільшує необхідну кількість ітерацій основного кроку криптоперетворення та підвищує загальну складність шифру, відкриває можливості криптоаналітичних атак, заснованих на функціях багатозначної логіки, а також підвищує ймовірність перспективних атак квантового

криптоаналізу, що обумовлені структурною слабкістю шифру при його представленні за допомогою функцій багатозначної логіки.

Таким чином, актуальнім для сьогоднішнього стану розвитку інформаційних технологій та систем захисту інформації є створення методології розробки ефективних крипто-стеганографічних систем, орієнтованої на забезпечення ефективності вбудовування криптозахищенної додаткової інформації без застосування областей перетворень, тобто безпосередньо у просторовій області контейнера.

2. Загальна характеристика дисертаційної роботи

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

Перший розділ дисертації присвячений аналізу сучасних підходів до побудови стеганографічних систем, криптографічних систем та крипто-стеганографічних систем. У розділі зазначено, що формування сучасних систем захисту інформації має відбуватися із залученням як криптографічної, так і стеганографічної складової, однак, незважаючи на те, що на сьогодні введено визначення крипто-стеганографічної системи та розроблено ряд крипто-стеганографічних систем, що можуть функціонувати на потужних обчислювальних платформах за рахунок застосування ресурсномістких перетворень. Слід зазначити, що проблема роботи таких систем на повсюдно застосовуваних сьогодні ресурсообмежених пристроях із потоковим контейнером (насамперед, цифровим відео) лишається невирішеною. Тому створення передумови для формування методології розробки ефективної крипто-стеганографічної системи, яка базується на кодовому управлінні вбудовуванням інформації у часовій області із тісною інтеграцією криптографічного захисту інформації є актуальною.

Другий розділ присвячений розробці теоретичних засад кодового управління вбудовуванням додаткової інформації, зокрема встановлено взаємозв'язок між трансформантами двовимірного і одновимірного перетворення Уолша-Адамара та дискретне косинусне перетворення (ДКП), а також взаємозв'язок між трансформантами перетворення Уолша-Адамара, ДКП та сингулярного розкладання матриць блоків контейнера. Встановлений взаємозв'язок дозволив сформулювати та експериментально підтвердити достатні умови забезпечення заданих властивостей стеганоповідомлення в

області перетворень Уолша-Адамара, а також сформувати теоретичний базис кодового управління вбудовуванням інформації у просторовій області.

Третій розділ присвячено розробці та експериментальному дослідженню стеганографічних методів з кодовим управлінням вбудовуванням додаткової інформації. Побудовано множини бінарних кодових слів, на основі яких розроблено стеганографічний метод з кодовим управлінням вбудовуванням додаткової інформації, показники ефективності якого перевищують показники ефективності існуючих аналогів. Введено та обґрунтовано визначення енергії та коефіцієнта селективності кодового слова, що застосовується у стеганографічному методі з кодовим управлінням вбудовуванням додаткової інформації. Розраховано значення коефіцієнта селективності бінарних кодових слів. Представлено набір багаторівневих кодових слів, що забезпечують високі значення коефіцієнта селективності і впливають з високим ступенем вибірковості на задані трансформанти ДКП, на основі яких побудовано стеганографічний метод з кодовим управлінням вбудовуванням додаткової інформації, який дозволяє забезпечити найвищу стійкість до атак проти будованого повідомлення.

Четвертий розділ присвячено розробці стеганографічних методів, що забезпечують можливість множинного доступу до прихованого каналу, зокрема виведені і доведені співвідношення, що визначають як можливі значення коефіцієнтів перетворення Уолша-Адамара для заданого значення числа каналів N, що розділяються, так і ймовірності появи заданих значень коефіцієнтів перетворення Уолша-Адамара, що виключило необхідність набору відповідної статистики перебірним методом при побудові ефективних кодів, а також запропоновано застосування попереднього кодування інформації у груповому тракті С-кодами постійної амплітуди для підвищення пропускної спроможності прихованого каналу зв'язку. Розроблено два стеганографічних метода з кодовим управлінням вбудовуванням додаткової інформації, що засновані на частотних розстановках та просторово-частотних матрицях, і дозволяють значно підвищити кількість зареєстрованих та одночасно-працюючих у система абонентів, а також забезпечити незалежність процесу вбудовування інформації кожним користувачем.

П'ятий розділ присвячено розробці теоретичного базису дослідження якості криптографічних конструкцій при їх уявленні функціями багатозначної логіки. Запропоновано наступні критерії криптографічної якості: максимізація алгебраїчної нелінійності, максимізація дистанційної нелінійності, критерій розповсюдження помилки і суворий лавинний критерій, а також критерій незалежності виходу функції багатозначної логіки від її вхідних змінних. Розроблено методи дослідження рівня відповідності функцій багатозначної логіки вказаним критеріям криптографічної якості, які дозволяють

порівнювати ступінь криптографічної якості функцій багатозначної логіки та проводити їх обґрунтований вибір для побудови криптографічних конструкцій. Проведені у даному розділі дослідження створюють передумови для розробки криптографічних примітивів та шифрів, що підвищують ефективність крипто-стеганографічних систем.

Шостий розділ присвячено підвищенню криптографічної захищеності крипто-стеганографічних систем, зокрема у розділі проведено розробку криптографічних S-блоків, що відповідають критеріям криптографічної якості як при їх представленні компонентними булевими функціями, так і компонентними функціями багатозначної логіки. На основі розроблених криптографічних примітивів та концепції змінної фрагментації блоків запропоновано шифр прекодера та спеціалізований блоковий шифр для шифрування послідовності переліку станів. Запропоновано спосіб вбудовування додаткова інформація (ДІ) за допомогою стеганографічного методу з кодовим управлінням вбудовуванням додаткової інформації із шифруванням послідовності переліку станів блоків. Сформульовано твердження із строгим доказом, що доводить більшу обчислювальну ефективність застосування стеганографічних методів, що оперують у просторовій області у порівнянні із стенографічними методами, що оперують у областях перетворень. Проведені обчислювальні експерименти дозволили встановити можливість використання крипто-стенографічної системи для роботи з потоковими контейнерами у режимі реального часу, а також встановити мінімально необхідні вимоги до мікропроцесорів для підтримки роботи розробленої 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.

3. Наукова новизна результатів, отриманих в дисертаційній роботі

Тема дисертаційної роботи безпосередньо пов'язана зі Стратегією національної безпеки України від 14 вересня 2020 № 392/2020 у контексті п. 52 «Основне завдання розвитку системи кібербезпеки — гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури, зокрема в умовах цифрової трансформації»; Стратегією кібербезпеки України від 27 січня 2016 року №96/2016 у контексті п. 4.1. «Розвиток безпечного, стабільного і надійного кіберпростору має полягати, насамперед, у … розвитку та вдосконаленні системи технічного і криптографічного захисту інформації»; Законом України Про основні засади забезпечення кібербезпеки України від 24.10.2020 №2163-VIII у контексті п. 3 Статті 8 «Національна система кібербезпеки», а саме

«Функціонування національної системи кібербезпеки забезпечується шляхом … розвитку та вдосконалення системи технічного і криптографічного захисту інформації».

Наукова новизна отриманих у дисертаційній роботі результатів, на мій погляд, полягає у наступному:

1. *Вперше* на основі загального підходу до аналізу стану й технології функціонування інформаційних систем, теорії досконалих алгебраїчних конструкцій та теорії функцій багатозначної логіки створено науково-обґрунтовану методологію розробки ефективної крипто-стеганографічної системи, що дозволяє її застосування із потоковим контейнером на ресурсообмежених пристроях.

2. *Вперше* на основі достатніх умов забезпечення заданих властивостей стеганоповідомлення сформовано теоретичний базис для синтезу кодових слів, що при підсумовуванні із блоками контейнера у просторовій області здійснюють зосереджений вплив на задані трансформанти Уолша-Адамара та ДКП матриць блоків контейнера, що дозволило, здійснюючі стеганоперетворення у просторовій області, керувати його впливом на частотні складові контейнера.

3. *Вперше* на основі концепції кодового управління вбудовуванням додаткової інформації та теоретичного базису для синтезу кодових слів, що здійснюють зосереджений вплив на задані трансформанти Уолша-Адамара та ДКП, розроблено стеганографічні методи з кодовим управлінням вбудовуванням додаткової інформації на основі бінарних та багаторівневих кодових слів, що дозволили забезпечити ефективність стеганоперетворення при його здійсненні у просторовій області.

4. *Вперше* на основі технології кодового управління вбудовуванням додаткової інформації розроблено два повноцінних стеганографічних методи, що забезпечують множинний доступ до прихованого каналу зв'язку шляхом застосування частотних розстановок та просторово-частотних матриць, що дозволило підвищити кількість абонентів, які можуть бути зареєстровані в системі, та кількість одночасно працюючих абонентів.

5. *Подальший розвиток* на основі ефективних кодів та кодів постійної амплітуди отримала технологія MC-CDMA забезпечення множинного доступу до прихованого каналу зв'язку, в результаті чого було доведено два твердження, що визначають статистику появи коефіцієнтів перетворення Уолша-Адамара, та запропоновано С-код на основі бент-послідовностей, що дозволило підвищити пропускну спроможність прихованого каналу зв'язку.

6. *Подальший розвиток* на основі теоретичного базису забезпечення криптографічної якості функцій багатозначної логіки отримали методи синтезу високоякісних

криптографічних конструкцій, що дозволило створити S-блоки, які одночасно відповідають критеріям криптографічної якості при представленні компонентними булевими функціями та компонентними функціями багатозначної логіки.

7. *Удосконалено* на основі розроблених криптографічних конструкцій та концепції змінної фрагментації блоків криптографічну складову крипто-стеганографічних систем, що дозволило забезпечити врахування взаємозв'язку та взаємного впливу їх криптографічної та стеганографічної компоненти, підвищити їх криптографічну захищеність.

4. Ступінь обґрунтованості наукових положень, рекомендацій, наданих в дисертації, їхня достовірність

Обґрунтованість та достовірність наукових положень, висновків та рекомендацій, сформульованих у дисертації, визначається наступним:

— теоретичні дослідження базуються на фундаментальних положеннях і не суперечать відомим науковим фактам;

— теоретичні результати обґрунтовані коректним використанням математичного апарату — матричного аналізу, теорії збурень, методів обчислювальної лінійної алгебри, обчислювальних методів;

— коректністю поставлених задач при проведенні експериментальної перевірки отриманих теоретичних результатів;

— відповідністю результатів експериментів теоретичним положенням, набутим при проведенні дисертаційного дослідження;

— матеріали дисертації доповідалися і обговорювалися на18 Міжнародних і Всеукраїнських конференціях, форумах, семінарах, у тому числі на семінарі при Вченій раді НАН України «Технічні засоби захисту інформації» (2020-2022 рр.).

5. Практичне значення результатів, отриманих в дисертаційній роботі

Результати досліджень дисертаційної роботи використовувалися під час виконання НДР №0111U009481 «Підвищення ефективності методів цифрової обробки сигналів в радіотехнічних системах», НДР №0116U004923 «Оптимізація методів цифрової обробки інформації в корпоративних мережах та радіотехнічних системах», НДР №710-59 «Методи і технології радіаційного керування параметрами та стійкістю активних елементів електроніки до іонізуючих випромінювань».

Практична цінність роботи полягає в доведенні отриманих наукових результатів до конкретних методів та алгоритмів, що можуть бути використані як складові систем захисту інформації будь-якої організації та підприємства. Алгоритмічні реалізації розроблених методів дозволили забезпечити ефективність крипто-стеганографічних систем при роботі з потоковим контейнером на ресурсообмежених пристроях в режимі реального часу.

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

6. Повнота викладення наукових положень, висновків та рекомендацій, сформульованих у дисертаційному дослідженні та опублікованих у працях

Результати дисертаційного дослідження знайшли своє відображення в 63 наукових роботах, з них 22 статті у фахових виданнях України, 29 в міжнародних виданнях, 26 статей у виданнях, що входять до наукометричних баз Scopus та/або Web of Science (з яких 5 статей є перекладами статей у фахових виданнях України), 17 публікацій у збірниках праць міжнародних та регіональних конференцій.

Зазначені публікації повною мірою висвітлюють основні наукові положення дисертації як на вітчизняному, так і на міжнародному рівнях.

7. Зауваження до дисертаційної роботи

Не зважаючи на загальну позитивну оцінку дисертаційної роботи, слід зазначити наступні зауваження:

1. У роботі встановлено взаємозв'язок між коефіцієнтами перетворення Уолша-Адамара, ДКП і сингулярного розкладання матриць блоків контейнера для значень розміру блока $N = 4, 8, 16$ в результаті чого побудовано карти відповідності перетворень (рис. 2.3). Однак, при побудові крипто-стеганографічних систем можуть бути обрані інші значення розміру блоків, для яких інформацію про взаємозв'язок між коефіцієнтами перетворення Уолша-Адамара та ДКП і сингулярного розкладання матриць в дисертації не наведено.

2. Незрозумілою є висунута в роботі вимога збільшення амплітуди впливу на елементи контейнера з метою підвищення селективності впливу на задану трансформанту ДКП, оскільки в роботі наведені кодові слова, що вже володіють абсолютною селективністю (табл. 3.1), тобто значенням $\kappa = 1$.

3. Застосування багаторівневих кодових слів, (рис. 3.13), як показано у роботі, веде до суттєвого збільшення стійкості стенографічного методу з кодовим управлінням вбудовуванням ДІ до атак проти вбудованого повідомлення. Однак, враховуючи структуру таких кодових слів, здається ймовірним виникнення порушення надійності сприйняття стеганоповідомлення, зокрема в областях цифрове зображення з малими перепадами значень яскравості, що повинно обмежити область застосування відповідного стеганометоду, але в роботі це не обговорюється, обмеження на область застосування не вводяться.

4. Під час формулювання Твердження 4.1 і Твердження 4.2 зроблено припущення, що можливі значення від абонентів належать алфавіту $\{\pm 1\}$, однак, на практиці може скластися ситуація, коли один з абонентів не здійснює вбудовування інформації, тобто результуючі вектори належатимуть алфавіту $\{0,\pm 1\}$, що збільшить кількість можливих значень трансформант і змінить ймовірності їх появи.

5. Відомо, що для випадку представлення криптографічних конструкцій компонентними булевими функціями, для відповідності криптографічної конструкції критерію відсутності кореляційного зв'язку її вихідних та вхідних векторів, необхідною і достатньою умовою є відповідність її компонентних булевих функцій критерію кореляційного імунітету. З тексту дисертації незрозуміло, чи є у випадку застосування функцій багатозначної логіки необхідною і достатньою відповідність компонентних функцій багатозначної логіки Визначенню 5.5.6 для забезпечення відсутності кореляційного зв'язку між векторами виходу та входу.

6. З викладення методу синтезу максимально нелінійних S-блоків, що відповідають суровий лавинний критерій найвищих порядків, неясно, якою є потужність множини побудованих S-блоків (що мають властивості, аналогічні до S-блока (6.24)) для значення їх довжини $N = 32$, що є важливим параметром для їх практичного застосування.

7. У табл. 6.13 наведено розрахунки можливості роботи розробленої крипто-стеганографічної системи, виходячи з факту функціонування виключно даної системи на пристрої, однак на практиці процесор має виконувати і інші завдання, обумовлені призначенням пристрою, що підвищить фактичні апаратні вимоги для підтримки роботи системи.

8. Відповідність дисертації встановленим вимогам і загальні висновки

Вказані зауваження не є принциповими та не знижують загальне позитивне враження про роботу. Вважаю, що за актуальністю, науковою новизною, обсягом проведених експериментальних досліджень, їхньою науковою та практичною цінністю, дисертаційна робота Соколова Артема Вікторовича «Методологія розробки ефективної крипто-стеганографічної системи» є завершеною науковою роботою, не містить академічного плагіату та задовольняє вимогам, які висуваються до робіт на здобуття наукового ступеня доктора наук, п. 7 та 9 Порядку присудження та позбавлення наукового ступеня доктора наук, затвердженого постановою Кабінету Міністрів України від 17 листопада 2021 року № 1197. Реферат дисертації об'єктивно і достатньо повно відображає зміст, а також основні положення та висновки дисертації.

Таким чином вважаю, що Соколов Артем Вікторович заслуговує на присудження наукового ступеня доктора технічних наук за спеціальністю 05.13.21 — Системи захисту інформації.

Офіційний опонент
доктор технічних наук, професор
професор кафедри безпеки
інформаційних технологій факультету
кібербезпеки та програмної інженерії
Національного авіаційного університету **В.О. Хорошко**

МІНІСТЕРСТВО ОСВІТИ І НАУКИ НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ 01132330 МІСТО КИЇВ

підпис гр. _____
а с в і д ч у ю
Вчений секретар
Національного авіаційного університету
М. Ленівський