67-72-53/3
07.04.2023 р.

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

Повсюдне впровадження мобільних платформ, пристроїв IoT та вбудованих систем у життя суспільства, так само як і суттєві зміни, які відбуваються у структурі та характері світового трафіку на користь переваги у ньому мультимедійної складової, виносить проблеми захисту інформації на принципово новий рівень, потребує подальшого розвитку та переосмислення існуючих підходів до забезпечення кібербезпеки. Так, сучасні дослідники сходяться на думці, що в обставинах, які склалися на сьогоднішній день, а також, вочевидь будуть домінуючими у майбутньому, окреме застосування криптографічної складової для організації повноцінної системи захисту інформації є недостатнім, тоді як необхідний рівень захищеності може бути забезпечений лише із застосуванням комплексного рішення — крипто-стеганографічної системи.

Сучасні методи побудови крипто-стеганографічних систем передбачають застосування у них блоків перетворення вихідного контейнеру, що є необхідним для забезпечення їх ефективності із застосуванням існуючого математичного апарату. Причому, у більшості випадків, йдеться про обчислювально затратні перетворення, насамперед, сингулярне розкладання матриць блоків контейнера, що дуже ускладнює (а часто і практично виключає) застосування таких методів на ресурсообмежених пристроях та найчастіше унеможливлює для них використання крипто-стеганографічних систем. Таким чином, вимушеною мірою забезпечення безпеки ресурсообмежених пристроїв на сьогоднішній день є застосування лише

криптографічного захисту інформації, що веде до суттєвого зниження рівня безпеки таких пристроїв.

З іншого боку, ефективність застосування крипто-стеганографічних систем залежить від узгодженості та степені врахування взаємозв'язку та взаємного впливу їх криптографічної та стеганографічної складової, що потребує подальшого вдосконалення і криптографічної складової, яке, як показує досвід розвитку теорії сигналів, теорії завадостійкого та ефективного кодування, а також результати сучасних досліджень, може бути здійснено за рахунок розвитку та застосування математичного апарату функцій багатозначної логіки для задач підвищення крипостійкості крипто-стеганографічних систем, а також степеню узгодженості їх криптографічної та стеганографічної компоненти.

Наведені факти обумовлюють високу актуальність теми дисертаційного дослідження Соколова Артема Вікторовича, які ставлять метою розробку ефективної (у сенсі критеріїв ефективності) крипто-стеганографічної системи, яка була б здатна до роботи із потоковим контейнером в режимі реального часу на ресурсообмежених пристроях.

2. Загальна характеристика дисертаційної роботи

Дисертаційна робота складається із 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 присвячено проведенню аналітичного огляду сучасних літературних джерел щодо побудови крипто-стеганографічних систем, а також окремих криптографічних та стеганографічних методів захисту інформації. Проведений огляд дозволив підтвердити існування фундаментального протиріччя між необхідністю застосування

ресурсозатратних перетворень (насамперед, сингулярного розкладання матриць блоків контейнеру) для забезпечення ефективності крипто-стеганографічної системи і необхідністю мінімізації обчислювальних затрат крипто-стеганографічної системи при її роботі по вбудовуванню та вилученню криптозахищенної додаткової інформації на ресурсообмежених пристроях в режимі реального часу. У розділі показано, що для оцінки криптографічної якості існуючих криптографічних конструкцій, так само як і при розробленні нових криптографічних конструкцій, сьогодні застосовується лише математичний апарат булевих функцій, тоді як криптоаналітик не є обмеженим у застосовуванні будь-якого інструментарію, що підтверджується наявністю у відкритих літературних джерелах криптоаналітичних методів, заснованих на функціях багатозначної логіки. З іншого боку, застосування функцій багатозначної логіки є основою для покращення рівня реалізації криптографічними конструкціями концепцій дифузії та конфузії, що є важливим в умовах обмежених обчислювальних та енергетичних ресурсів, а також збільшення можливостей щодо інтеграції та узгодження криптографічної та стеганографічної складової крипто-стеганографічної системи, забезпечення врахування їх взаємозв'язку та взаємного впливу.

Другий розділ дисертації присвячено розробці теоретичного базису кодового управління вбудовуванням додаткової інформації. У розділі встановлено взаємозв'язок між трансформантами одновимірного та двовимірного аналогу перетворення Уолша-Адамара та ДКП, що дало можливість суттєво спростити математичні викладки у роботі. У розділі також встановлено взаємозв'язок між трансформантами перетворення Уолша-Адамара, ДКП та сингулярним розкладанням матриць блоків контейнера. Локалізовано конкретні розташування трансформант перетворення Уолша-Адамара, що відповідають низькочастотним, середньочастотним та високочастотним складовим матриці блоку контейнера. Зважаючи на те, що в області ДКП та сингулярного розкладання матриць блоків контейнера на сьогодні вже відомі достатні умови забезпечення заданих властивостей

стеганоперетворення, означене стало основою для формування достатніх умов забезпечення надійності сприйняття та нечутливості до атак проти вбудованого повідомлення, для формування кодових слів, що забезпечують зосереджений вплив на задану частотну складову матриці блоку контейнера, а також для розробки концепції кодового управління вбудовуванням додаткової інформації.

Третій розділ дисертації присвячений розробці двох стеганографічних методів на основі концепції кодового управління вбудовуванням криптозахищенної інформації: на основі бінарних та багаторівневих кодових слів. В якості основи розроблених методів у розділі синтезовано бінарні та багаторівневі кодові слова, що забезпечують зосереджений вплив на задані частотні складові блоків контейнера, до яких застосовано показник енергії та введено показник селективності кодового слова. Наведено результати численних експериментів, що підтверджують ефективність розроблених стеганографічних методів в умовах різноманітних атак: стисненням, зашумленням, розмиттям і т.д. Дані щодо проведених експериментів є вичерпними та підтверджують їх коректність. Результати експериментів чітко вказують на суттєво більш високу ефективність і гнучкість розроблених методів у порівнянні з існуючими аналогами, при цьому розроблені стеганографічні методи працюють у просторовій області контейнера, що зменшує їх обчислювальну складність, дозволяє їх використання з потоковим контейнером на ресурсообмежених пристроях в режимі реального часу.

Четвертий розділ дисертації присвячено підвищенню пропускної спроможності прихованого каналу зв'язку при застосуванні технології множинного доступу MC-CDMA. За рахунок доведених тверджень щодо ймовірнісних характеристик коефіцієнтів перетворення Уолша-Адамара, а також застосування створеного коду постійної амплітуди на основі бент-функцій було запропоновано схему множинного доступу до прихованого каналу зв'язку, що забезпечує більшу пропускну спроможність у порівнянні з аналогами. Окрім того, на основі концепції кодового управління

вбудовуванням додаткової інформації у розділі запропоновано два стеганографічних методи, що забезпечують множинний доступ до прихованого каналу зв'язку: на основі частотних розстановок та просторово-частотних матриць. Розроблені стеганографічні методи, окрім переваг, що притаманні технології кодового управління вбудовуванням додаткової інформації, забезпечують можливість незалежного вбудовування додаткової інформації користувачами, гнучкість розподілення ресурсів прихованого каналу зв'язку, підвищену кількість абонентів, що можуть бути зареєстрованими та одночасно працювати із прихованим каналом зв'язку.

П'ятий розділ дисертації присвячено створенню теоретичних основ оцінки та порівняння криптографічної якості функцій багатозначної логіки, які можуть бути застосовані криптоаналітиком для здійснення атаки на конструкції шифрів. У розділі запропоновано наступні критерії криптографічної якості, що відображають рівень стійкості криптографічної конструкції до атак криптоаналізу: критерій максимізації алгебраїчної нелінійності, критерій максимізації дистанційної нелінійності, критерій розповсюдження помилки та строгий лавинний критерій, а також критерій відсутності кореляційного зв'язку векторів виходу та входу криптографічної конструкції. Для кожного критерію криптографічної якості представлено методи дослідження функцій багатозначної логіки, що дозволяють провести оцінку їх відповідності даному критерію. Отримані у розділі результати створюють передумови для розробки нових класів криптографічних конструкцій, що є високоякісними як у сенсі їх уявлення за допомогою компонентних булевих функцій, так і при їх уявленні компонентними функціями багатозначної логіки. Такі криптографічні конструкції є основою для удосконалення шифрів прекодера і для створення нових криптографічних алгоритмів, що забезпечують узгодження криптографічної та стеганографічної складової крипто-стеганографічних систем.

Шостий розділ дисертації присвячений розробці криптографічних конструкцій, що відповідають критеріям криптографічної якості як при їх

уявленні компонентними булевими функціями, так і при їх уявленні компонентними функціями багатозначної логіки, зокрема: метод синтезу S-блоків, максимально нелінійних у двійковому та четвірковому сенсі, метод синтезу S-блоків з хорошими лавинними характеристиками компонентних булевих та четвіркових функцій, метод синтезу максимально нелінійних S-блоків, що відповідають строгому лавинному критерію найвищих порядків, метод синтезу трійкових S-блоків з ідеальною матрицею коефіцієнтів кореляції, модифікована схема Кіма для збільшення довжини оптимальних S-блоків. На основі запропонованих криптографічних конструкцій у розділі розроблено шифр прекодера та спеціалізований блоковий симетричний шифр для шифрування послідовності переліку станів, що у купі з методом шифрування послідовності переліку станів, забезпечує підвищення криптостійкості крипто-стеганографічної системи, узгодження її криптографічної та стеганографічної складової, врахування їх взаємозв'язку та взаємного впливу. У розділі проведено доказ твердження, що визначає гарантовано менші значення обчислювальної складності стеганографічних методів, що працюють у просторовій області у порівнянні із стеганографічними методами, що працюють в областях перетворення контейнеру. Проведено експериментальне дослідження розробленої крипто-стеганографічної системи, яке дозволило на практиці підтвердити її працездатність при роботі із потоковим контейнером на ресурсообмежених пристроях в режимі реального часу, а також встановити мінімально необхідні вимоги до процесорів для підтримки роботи системи.

Висновки належним чином відображають основні результати дисертаційної роботи.

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 полягає у наступному:

1. *Вперше* на основі загального підходу до аналізу стану й технології функціонування інформаційних систем, розробленої концепції кодового управління вбудовуванням додаткової інформації, а також розроблених теоретичних основ забезпечення криптографічної якості функцій багатозначної логіки запропоновано науково-обґрунтовану методологію розробки ефективної крипто-стеганографічної системи, що здатна працювати з потоковим контейнером на ресурсообмежених платформах в режимі реального часу.

2. *Вперше* на основі засад матричного аналізу встановлено однозначний взаємозв'язок між одновимірними та двовимірними аналогами перетворення Уолша-Адамара та ДКП, що дозволило значно спростити математичні викладки щодо обґрунтування достатніх умов забезпечення заданих властивостей стеганоповідомлення в області перетворень Уолша-Адамара, а також заклало основи розробки концепції кодового управління вбудовуванням додаткової інформації.

3. *Вперше* на основі засад матричного аналізу та встановленого взаємозв'язку між одновимірним та двовимірним аналогом перетворення Уолша-Адамара та ДКП встановлено взаємозв'язок між трансформантами

перетворення Уолша-Адамара та ДКП, а також сингулярним розкладанням матриці блока контейнера, що дозволило сформулювати достатні умови забезпечення надійності сприйняття стеганоповідомлення в області перетворень Уолша-Адамара, а також створити теоретичні основи для побудови кодових слів, що забезпечують вибірковий вплив на задані трансформанти перетворення Уолша-Адамара та ДКП.

4. *Вперше* на основі концепції кодового управління вбудовуванням додаткової інформації, а також синтезованих бінарних та багаторівневих кодових слів розроблено два стеганографічних методи, що дозволяють при забезпеченні процесу стеганоперетворення у просторовій області отримати показники ефективності, що перевищують показники ефективності найкращих відомих аналогів.

5. *Вперше* на основі розробленого спеціалізованого блокового симетричного шифру запропоновано спосіб вбудовування додаткової інформації із шифруванням послідовності переліку станів, який, на відміну від відомих аналогів, дозволив підвищити криптостійкість стеганоперетворення при забезпеченні врахування взаємозв'язку та взаємного впливу криптографічної та стеганографічної компоненти крипто-стеганографічної системи.

6. *Вперше* на основі технології кодового управління вбудовуванням додаткової інформації розроблено два повноцінних стеганографічних методи: на основі частотних розстановок та просторово-частотних матриць, що дозволило зробити процес вбудовування додаткової інформації користувачами незалежним, підвищити кількість зареєстрованих у системі абонентів, а також таких, хто одночасно працює.

7. *Удосконалено* на основі застосування розроблених С-кодів технологію MC-CDMA, що дозволило підвищити пропускну спроможність прихованого каналу зв'язку при організації множинного доступу.

8. *Удосконалено* на основі теорії функцій багатозначної логіки математичний підхід до оцінки якості криптографічних конструкцій, що дозволило проводити оцінку та порівняння якості криптографічних

конструкцій не тільки при їх представленні за допомогою компонентних булевих функцій, але і при їх представленні за допомогою компонентних функцій багатозначної логіки.

9. *Удосконалено* криптографічну складову крипто-стеганографічних систем за рахунок розробки методів синтезу криптографічних конструкцій, що є високоякісними як при представленні компонентними булевими функціями, так і компонентними функціями багатозначної логіки.

10. *Удосконалено* на основі розроблених криптографічних примітивів криптографічну складову крипто-стеганографічної системи за рахунок розробки шифру прекодера та спеціалізованого блокового симетричного шифру для шифрування послідовності переліку станів, що дозволило підвищити криптостійкість крипто-стеганографічної системи, забезпечити врахування взаємовпливу та взаємозв'язку її криптографічної та стеганографічної складової.

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

Викладені в дисертації основні наукові положення, висновки і результати, що отримані здобувачем, забезпечуються правильністю постановки задачі та їх подальшим теоретичним та експериментальним опрацюванням, підтверджені публікаціями в авторитетних вітчизняних та міжнародних рецензованих виданнях, апробацією на конференціях і семінарах. Усі наукові положення ґрунтуються на детальному аналізі об'єкта та предмета дослідження, узгоджуються з відомими на сьогодні результатами в стенографії та криптографії. Детальне ознайомлення з роботою та представленими в ній положеннями, дозволяє виділити наукову новизну та сформувати чіткий порядок викладення матеріалу.

Дисертація є самостійною завершеною науково-дослідною роботою. Її структура логічна, вона оформлена акуратно та згідно до встановлених вимог. Реферат повністю відображає зміст дисертації.

5. Практичне значення результатів, отриманих в дисертаційній роботі

Практична цінність роботи полягає в доведенні здобувачем отриманих наукових результатів до конкретних методів та алгоритмів, що можуть бути використані як складові систем захисту інформації будь-якого закладу, підприємства. Алгоритмічні реалізації розроблених у дисертаційній роботі теоретично обґрунтованих методів характеризуються наступними показниками ефективності, які перевищують показники ефективності найкращих відомих аналогів, зокрема:

— забезпечується рівень помилок в умовах атаки стиском проти вбудованого повідомлення з коефіцієнтом якості $QF = 10$, який у 8.125 разів менший від подібного показника найкращого відомого аналогу;

— значення показника PSNR складає 35.6 дБ, що на 3% перевершує значення найкращого відомого аналогу, який володіє сумірним рівнем стійкості до атак проти вбудованого повідомлення;

— крипто-стеганографічна система забезпечує кількість зареєстрованих у системі абонентів, що дорівнює $J = 4800$ (у 1200 разів більше, аніж у найкращого відомого аналогу), а також кількість одночасно працюючих абонентів при нульовому рівні внутрішньосистемних перешкод, що дорівнює $J = 64$ (у 16 разів більше, аніж у найкращого відомого аналогу);

— метод синтезу S-блоків, що відповідають суворому лавинному критерію компонентних 4-функцій та критерію максимального лавинного ефекту компонентних булевих функцій дозволяє покращити лавинні властивості криптографічних конструкцій, тоді як метод синтезу S-блоків з ідеальними матрицями коефіцієнтів кореляції $\left|R_{ij}\right| = 0, i, j = 1,2,...,k$ дозволяє покращити кореляційні властивості синтезованих криптографічних конструкцій на 12.5%.

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

Основні результати та висновки дисертаційної роботи в повному обсязі висвітлені 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 та реферату

1. Виходячи з даних, представлених у табл. 2.2 дисертації, можна дійти висновку, що рівень відповідності трансформант Уолша-Адамара та коефіцієнтів ДКП зростає із зростанням розміру блоку, принаймні для трьох наведених у прикладі трансформант. Тим не менш, інформації щодо степеню відповідності трансформант Уолша-Адамара та коефіцієнтів ДКП, а також характеру її змін із зміною розміру блоку, в дисертації не наведено.

2. Синтезовані багаторівневі кодові слова (рис. 3.12, 3.13, 3.14 дисертації, а також рис. 5 реферату дисертації) мають подібну структуру, що дозволяє говорити про можливість створення рекурентних методів синтезу таких кодових слів, що дозволило б уникнути необхідності вирішення системи рівнянь (3.19), що для великих значень розміру блока μ є обчислювально витратно. Однак, означені задачі в дисертації не розглядаються.

3. В дисертаційній роботі показано, що розроблені стеганографічні методи з кодовим управлінням вбудовуванням додаткової інформації є стійкими до

атак зашумленням (рис. 3.8 дисертації та рис. 4 реферату дисертації). Тим не менше, проблеми вибору кодових слів таким чином, щоб забезпечити максимізацію ефекту стійкості до атак зашумленням не розглядаються.

4. Тестування розроблених стеганографічних методів з кодовим управлінням вбудовуванням додаткової інформації, що забезпечують множинний доступ (на основі частотних розстановок та просторово-частотних матриць) відбувалося лише із застосуванням бінарних кодових слів — (табл. 4.5, табл. 4.8 дисертації), тоді як результати тестування даних методів при використанні багаторівневих кодових слів не представлені.

5. При застосуванні технології MC-CDMA забезпечення множинного доступу до прихованого каналу для кодування коефіцієнтів перетворення Уолша-Адамара у роботі застосовуються коди Гаффмана (табл. 4.2 дисертації та табл. 3 реферату дисертації), однак, вибір цих ефективних кодів ніяк не обґрунтовано з точки зору мінімізації середньої довжини кодового слова.

6. Для забезпечення працездатності стеганографічного методу з множинним доступом на основі просторово-частотних матриць у четвертому розділі дисертації запропоновано метод синтезу S-кодів просторових розстановок, що передбачає частковий перебір (розділ 4.2 та стор. 21 автореферату). Тим не менш, застосування часткового перебору може бути неможливим або невиправдано витратним для довжин кодових слів S-кодів просторових розстановок $N > 16$.

7. У п'ятому розділі дисертації виведено рекурентні конструкції для побудови прямих та зворотних матриць Ріда-Маллера для значень $q = 4,16$ (одна з таких конструкцій наведена у виразі (22) реферату дисертації), тоді як інші можливі значення основи представлення, наприклад $q = 32,64...$ залишилися за межами уваги, що звужує загальність розробленого критерію максимізації алгебраїчної нелінійності функцій багатозначної логіки.

8. Відповідність дисертації встановленим вимогам і загальні висновки

Наведені зауваження не можуть вважатися принциповими, та жодним чином не знижують наукову та практичну цінність дисертаційного дослідження. Вважаю, що дисертаційна робота Соколова Артема Вікторовича «Методологія розробки ефективної крипто-стеганографічної системи» є завершеною науковою роботою, в якій отримані нові науково-обґрунтовані результати, зокрема стосовно розробки крипто-стеганографічних систем, що здатні працювати з потоковим контейнером в режимі реального часу на ресурсообмежених платформах. Робота відповідає паспорту спеціальності 05.13.21 — Системи захисту інформації, не містить академічного плагіату, задовольняє чинним вимогам п.п. 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 заслуговує на присвоєння наукового ступеня доктора технічних наук за спеціальністю 05.13.21 — Системи захисту інформації.

Офіційний опонент
професор кафедри кібербезпеки
Національного технічного університету
«Харківський політехнічний інститут»,
доктор технічних наук, професор **О.В. Мілов**

Підпис Мілова О.В.
ЗАСВІДЧУЮ:
ВЧЕНИЙ СЕКРЕТАР
НАЦІОНАЛЬНОГО-ТЕХНІЧНОГО УНІВЕРСИТЕТУ
"ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"
ЗАЙЦЕВ Ю. І.
"____"

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ * Національний технічний університет "Харківський політехнічний інститут" * код 02071180 *