РЕЦЕНЗІЯ

на дисертаційну роботу Аль-Файюмі Халеда «Методи підвищення захищеності інформації на основі прихованості передавання сигнально-кодових конструкцій», подану на здобуття наукового ступеня доктора філософії за галуззю знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека

Відгук складено на основі вивчення дисертації, опублікованих здобувачем наукових праць, а також документів, що свідчать про реалізацію та впровадження наукових досліджень.

1. Обґрунтування вибору теми дослідження

Актуальність дисертації Аль-Файюмі Халеда, присвяченої вивченню методів підвищення захищеності інформації на основі прихованості передавання сигнально-кодових конструкцій, зумовлена зростаючими вимогами до забезпечення безпеки інформаційних систем в умовах постійного ускладнення загроз і методів несанкціонованого доступу до даних. Обраний Аль-Файюмі Халедом предмет дослідження також є обґрунтованим, бо сучасні методи захисту, що базуються на позиційних сигналах, виявляються недостатньо ефективними в контексті нових викликів кібербезпеки. З цього приводу запропоновано використання непозиційних таймерних сигнальних конструкцій, які мають більш складну структуру у порівнянні з позиційними сигналами. В дисертації запропоновано методи розширення спектра таймерних сигнальних конструкцій для ускладнення структури широкосмугового сигналу та забезпечення підвищення основних показників прихованості передачі. Досліджено статистичні та варіаційні можливості генераторів хаосу з метою оцінки по формуванню псевдовипадкових послідовностей для застосування їх в системах захисту інформації.

Аль-Файюмі Халедом запропоновано багаторівневий захист інформації від НСД та випадкових завад, в якому інтегруються процеси перетворення даних з поєднанням статистичного шифрування, завадостійкого кодування та декореляції помилок. Такий підхід дозволяє об’єднати функції шифрування, завадостійкого кодування та декореляції помилок в єдиний процес з метою збільшення криптографічної стійкості методів захисту від НСД.

2. Зв’язок дисертаційної роботи з науковими програмами, планами і темами

Обрані напрями дослідження в роботі безпосередньо пов’язані із науково-технічними завданнями, сформульованими в Постанові Кабінету Міністрів України № 942 від 7.09.2011 р. із змінами, внесеними постановою КМ № 463 від 9.05.2023 р. «Про затвердження переліку пріоритетних тематичних напрямів наукових досліджень і науково-технічних розробок на період до 2023 року». Таким чином, вважаю, що тема дисертаційної роботи Аль-Файюмі Халеда, яка присвячена розв’язанню науково-технічної проблеми підвищення прихованості передавання інформації в інформаційно-комунікаційних системах на основі розробки методів інтеграції процесів таймерного кодування, статистичного шифрування та завадостійкого кодування є актуальною і відповідає тематиці з галузі знань 12 – Інформаційні технології за спеціальністю 125 – Кібербезпека.

3. Оцінка змісту дисертації, її завершеності в цілому і оформлення

Робота Аль-Файюмі Халеда має чітку структуру: вона складається зі вступу, чотирьох розділів, висновків, списку використаних джерел (113 позицій) і двох додатків. Обсяг дисертації – 167 сторінок, із них основний текст дослідження – 140 сторінок.

На мою думку, зміст дисертації відповідає обраній темі. Текст викладено логічно з використанням відповідної технічної мови. Робота містить достатню кількість ілюстративних матеріалів, таких як рисунки та таблиці, а також додатки, що свідчать про її цілісність та завершеність.

У ***Вступі*** обґрунтовано актуальність теми, сформульовано мету, основні завдання, об'єкт і предмет дисертаційного дослідження, подано принципові теоретико-методологічні підходи й вказано методи, що застосовані в дисертації. Також визначені наукова новизна, теоретичне і практичне значення одержаних результатів.

У ***Розділі 1*** Аль-Файюмі Халед надає ґрунтовний аналіз проблем захисту передаваної інформації в умовах радіоелектронного конфлікту. Визначено ключові напрями досліджень, сформульовано наукову проблему та окреслено задачі, що підлягають вирішенню. Автор детально розглянув модель завадозахищеної системи зв'язку для аналізу сценаріїв засобів радіоелектронної боротьби (РЕБ) противника, що дає можливість визначити напрями забезпечення надійного передавання сигнально-кодових конструкцій від перехоплення та несанкціонованого доступу. Особлива увага приділена можливостям підвищення показників прихованості та завадостійкості на основі обраних критеріїв ефективності. Автором надано аналіз методам підвищення енергетичної та структурної прихованості з урахуванням сучасних можливостей засобів РЕБ: псевдовипадковий перескок робочої частоти; пряме розширення спектра за допомогою псевдовипадкових послідовностей; лінійно-частотної модуляції та хаотичних коливань. Значну увагу приділено перспективам інтегрованих методів захисту інформації, що поєднують статистичне шифрування, завадостійке кодування та декореляцію помилок, а також використання методів розширення спектра на основі непозиційних таймерних сигналів. Все це дозволяє забезпечити комплексний підхід для завдання підвищення прихованості та завадостійкості сигналів у складних умовах РЕБ. Таким чином, розділ 1 закладає науково-теоретичне підґрунтя для подальших досліджень, обґрунтовуючи актуальність і доцільність обраного напрямку.

У ***Розділі 2*** дисертант надав детальний аналіз статистичних характеристик та варіаційних можливостей генераторів хаосу для формування псевдовипадкових послідовностей, що застосовуються в системах захисту інформації. Особлива увага приділена властивостям динамічного хаосу, які забезпечують нерегулярність та аперіодичність процесів, необхідних для підвищення рівня захисту.

Проведено кореляційний аналіз різних моделей генераторів хаосу, що дозволяє виявити їхні переваги та обмеження для використання в криптографії та методах модуляції. Розглянуто метод формування початкових параметрів генераторів хаосу на основі символів пароля користувача з використанням геш-функцій, що забезпечує додатковий рівень захисту та персоналізації.

Таким чином, результати досліджень обґрунтовують доцільність

застосування генераторів хаосу для формування гама послідовностей в різних системах захисту інформації.

У ***Розділі 3*** Аль-Файюмі Халед досліджує підвищення завадозахищеності передавання інформації шляхом інтеграції статистичного шифрування, завадостійкого кодування та декореляції помилок. Визначено недоліки статистичного шифрування та запропоновано враховувати ентропію джерела для оптимізації кількості випадкових комбінацій для зменшення ризику успішності реалізації атаки на шифрограми. Алгоритм підвищення криптостійкості обґрунтовується використанням рівномірного розподілу випадкових комбінацій та інтеграції завадостійкого кодування для одночасної корекції помилок і розширення ансамблю комбінацій. Виконано статистичний аналіз розподілу символів в повідомленнях різного розміру, що дає змогу надати алгоритм спрощення вибору випадкових комбінацій для статистичного шифрування. Декореляція помилок забезпечує додаткове перемішування бітів у кодових блоках та мінімізацію групування помилок у шифрограмах передаваного повідомлення.

Обґрунтування інтегрованого захисту інформації від НСД та випадкових завад пояснюється можливістю підвищення криптостійкості системи статистичного шифрування за рахунок перевірочних елементів завадостійкого коду та додаткового перемішування біт у кодових блоках за рахунок декореляції помилок.

У ***Розділі 4*** досліджено методи формування шумоподібних сигналів на основі непозиційних сигналів. Надано аналіз властивостям таймерних сигнальних конструкцій для з’ясування переваг непозиційних сигналів перед позиційними по забезпеченню структурної прихованості. Обґрунтована доцільність використання таймерних сигналів в системах радіозв'язку для забезпечення підвищення структурної та енергетичної прихованості в умовах передавання повідомлень в умовах радіоелектронного конфлікту. Відзначено, що відомі методи розширення спектра для позиційних елементів не можуть бути поширені на позиційні сигнальні конструкцій. Розроблено методи розширення спектра таймерних сигналів з урахуванням структури їх побудови. Проведено імітаційне модулювання таймерних сигналів за допомогою лінійної частотної модуляції. Запропоновано кореляційний прийом таймерних шумоподібних сигналів для виділення фронтів імпульсів сигнальної конструкції.

У загальних висновках дисертації наведено основні, отримані автором наукові і практичні результати, що підкреслюють їх новизну і значимість.

За результатами досліджень автором опубліковано 16 друкованих праць, з яких: 6 статей у наукових фахових виданнях України, у тому числі одна стаття у журналі, який цитується у наукометричній базі даних Scopus; 9 тез доповідей в матеріалах наукових конференцій, у тому числі 2 тези доповіді у журналах, які цитуються у наукометричних базах даних Scopus. Одна наукова праця включена до складу монографії.

Структура дисертації логічна, її мета та завдання достатньою мірою відповідають обраній темою та певною проблематикою дослідження. Виклад матеріалу послідовний, аргументований і грамотний. Дисертація Аль-Файюмі Халеда є цілісним і завершеним дослідженням, вона оформлена згідно з вимогами Наказу МОН України від 12.01.2017 року № 40 (із змінами, внесеними

згідно з Наказом Міністерства освіти і науки №759 від 31.05.2019).

4. Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації

У дисертаційній роботі автором виконано комплекс теоретичних та експериментальних досліджень, результати яких прийнято за основу при науковому обґрунтуванні нових технічних рішень: можливість синтезу шумоподібних сигналів на основі непозиційних таймерних сигнальних конструкцій з використанням лінійної частотної модуляції та псевдовипадкового перескоку робочої частоти; застосування кореляційного прийому для звуження спектра шумоподібного таймерного сигналу та виділення фронтів сигнальної конструкції; забезпечення енергетичної прихованості за умови, що шум перевищує передаваний сигнал в каналі; доцільність багаторівневої системи захисту інформації на основі інтегрування статистичного шифрування, завадостійкого кодування та декореляції помилок; надано аналіз варіаційним можливостям дискретних генераторів хаосу по формуванню безлічі псевдовипадкових послідовностей із заданими взаємно-кореляційними властивостями для використання їх в різних системах безпеки захисту інформації.

Слід відзначити, що здобувач володіє широким спектром теоретичних знань, практичних навичок для проведення наукових досліджень. Основні положення та результати дисертації є науково обґрунтованими й достовірними, що підтверджено достатньою кількістю публікацій наукових праць у фахових виданнях України та журналах, які цитуються у наукометричній базі даних Scopus (3 праці).

5. Основні наукові результати, одержані автором, та їх новизна

Автором сформульовані наступні висновки**:**

– подальшого розвитку набула теорія динамічного хаосу для систем захисту та передавання конфіденційної інформації. Це дозволило оцінити потенціал дискретних генераторів хаосу у формуванні множини псевдовипадкових послідовностей із заданими кореляційними властивостями. Такі послідовності знайшли застосування в системах потокового шифрування, прямого розширення спектра таймерних сигналів і маніпуляцій, де хаотичні коливання використовуються для маскування процесу передавання непозиційних цифрових комбінацій;

– подальшого розвитку набули методи підвищення інформаційної прихованості та завадостійкості передавання інформації шляхом інтегрованих підходів до перетворення даних. Поєднання статистичного шифрування, завадостійкого кодування та декореляції помилок дозволило створити єдиний процес захисту інформації від несанкціонованого доступу та випадкових завад у каналі;

– розвинуто теорію синтезу шумоподібних сигналів, орієнтовану на розширення спектра непозиційних сигнально-кодових конструкцій. Це забезпечило можливість змінювати структуру таймерних комбінацій і підвищити їх здатність до виявлення та виправлення помилок;

– вперше розроблено метод синтезу шумоподібних сигналів, що базується на розширенні спектра непозиційних таймерних сигналів за допомогою лінійної частотної модуляції. Запропонований підхід забезпечує зростання

завадостійкості, а також енергетичної та структурної прихованості передавання сигнальних конструкцій.

6. Значення роботи для науки, практики та суспільства

Наукове значення роботи полягає в обґрунтуванні використання більш складних сигнально-кодових конструкцій для забезпечення захисту інформації від несанкціонованого доступу та перехоплення передаваного сигналу засобами радіотехнічної розвідки противника. Для цього в роботі запропоновано методи формування шумоподібних сигналів із застосуванням таймерних сигнальних конструкцій, які є непозиційними. Використання таймерних сигналів для завдання розширення спектра дає можливість змінювати структуру сигнальних конструкцій завдяки вибору початкових параметрів їх побудови. Такий підхід формування таймерних сигналів дозволяє обирати параметри побудови сигнальних конструкцій з урахуванням потокового стану каналу, що дозволяє забезпечувати задану завадостійкість каналу зв'язку. Також потрібно враховувати позитивний фактор використання таймерних сигналів, який полягає в можливості здійснювати контроль якості приймання сигнальних конструкцій з урахуванням використовуваних підмножин дозволених і заборонених комбінацій. Поєднання таймерних сигналів і методів розширення спектра дозволяє підвищити прихованість передаваних сигнальних конструкцій, що особливо важливо в умовах радіоелектронного конфлікту.

Автором запропоновано для підвищення криптостійкості передавання даних інтегрувати різні методи перетворення даних, до складу яких входить статистичне шифрування, завадостійке кодування і декореляції помилок. Характерним в цій схемі є те, що після статистичного шифрування на наступних кроках перетворення даних відбувається підвищення криптостійкості і завадостійкості передаваної інформації.

В роботі отримала подальший розвиток теорія динамічного хаосу, що дало змогу в результаті досліджень оцінити варіаційні можливості дискретних генераторів хаосу по формуванню безлічі псевдовипадкових послідовностей із заданими взаємно-кореляційними властивостями для використання їх в різних системах захисту інформації.

Практичне значення отриманих результатів відображено в розроблених автором рекомендаціях, а саме:

– надано аналіз сучасним методам розширення спектра та визначено їх ефективність по забезпеченню структурної та енергетичної прихованості передавання сигнальних конструкцій в умовах радіоелектронної боротьби;

– обґрунтована доцільність використання для захисту інформації непозиційних таймерних сигналів, які за своєю структурою є складними і за параметрами своєї побудови можуть змінювати структуру сигнальних конструкцій;

– розроблено нові методи розширення спектра з використанням таймерних сигналів на основі псевдовипадкового перескоку робочих частот і лінійної частотної модуляції, що забезпечило підвищення структурної та енергетичної прихованості сигнальних конструкцій;

– запропоновано кореляційний прийом таймерних шумоподібних сигналів, що сформовані на основі лінійної частотної модуляції, що дало змогу виділяти фронти імпульсних складових непозиційних сигналів, які відрізняються

тривалістю в межах сигнальної конструкції;

Практична значимість отриманих результатів визначається також використанням окремих положень і результатів дисертаційних досліджень у наукових дослідженнях ТОВ «АЙСАЙБЕРО» та у навчальному процесі Державного університету інтелектуальних технологій і зв'язку при підготовці бакалаврів спеціальності 125 Кібербезпека та захист інформації. Всі результати впровадження підтверджені відповідними документами, які представлені у додатках.

7. Оформлення дисертації та дотримання вимог академічної доброчесності

Дисертаційна робота написана правильною науково мовою із використанням сучасної термінології.

Тема, зміст та отримані наукові результати роботи відповідають спеціальності 125 – Кібербезпека галузі знань 12 – Інформаційні технології.

Аналіз наукових праць, що опубліковані здобувачем, змісту дисертації, дозволяє стверджувати, що усі наукові та практичні результати отримані автором особисто. В дисертаційній роботі не виявлено текстових запозичень та використання наукових результатів без посилань на відповідні джерела.

8. Дискусійні положення та зауваження до змісту дисертації

Відзначаючи високий теоретико-методологічний рівень дисертаційної роботи, наданої для рецензування, її практичну значимість та науково обґрунтовану новизну, хочу звернути увагу на деякі дискусійні моменти, які могли б доповнити дисертаційне дослідження або розставити певні акценти.

1. Слід відзначити, що перший розділ дещо перенавантажений теоретичними та навчальними відомостями щодо завдання дослідження. Вважаю, що для покращення вмісту першого розділу доцільно було б дати пояснення з приводу деяких показників з теорії прихованості та криптографії, які використовувалися у роботі для оцінки тих або інших методів захищеності інформації. В табл. 1.3 (с.59) автор наводить порівняння захищеності сигнальних конструкцій для різних видів модуляцій з криптографічною стійкістю відомих методів шифрування, використовуючи показники структурної прихованості та криптографічної стійкості відповідно. Слід відзначити, що ці показники дійсно за своїми розрахунками мають певну схожість, за виключенням того, що для визначення показника структурної прихованості використовується додатково двійковий логарифм. Проте фізична основа злому зашифрованого повідомлення та ідентифікації виду модуляції є різною. Тому вважаю, що таке порівняння не є коректним.

2. В п.1.5 для ускладнення засобам радіоелектронної розвідки ідентифікації системи модуляції пропонується періодично змінювати в неї кут розташування векторів у сузір'ї (рис. 1.11). Проте автор для цього алгоритму не наводить розрахунки збільшення показника структурної прихованості з урахуванням кількості обраних кутів зміни розташування векторів сузір'я системи модуляції, що було б корисним для покращення якості першого розділу дисертаційного дослідження.

3. В п. 1.3 розглядаються задача підвищення завадостійкості за рахунок використання завадостійких кодів, а також наводяться приклади в табл. 1.1 та 1.2 залежності мінімальної кодової відстані в залежності від довжини кодового

блока. При цьому акцентується увага на необхідність мінімізації часу передавання повідомлення (с. 41) для завдання зменшення його ймовірності виявлення засобами радіоелектронної розвідки противника. Проте автор не надав відповідних розрахунків для визначення оптимальної довжини кодового блока.

4. В п. 1.4 на основі експериментальних даних, що отримані за допомогою SDR радіочастотного сканера спектра (рис. 1.8, с.53), визначена можливість виявлення сеансу передавання сигнальних конструкцій методом псевдовипадкового перескоку робочої частоти (ППРЧ). Проте, в роботі автором не вказано наскільки потрібно зменшити тривалість передавання несної частоти методу ППРЧ, що могло б значно покращити якість дисертаційного дослідження.

5. В четвертому розділі запропоновано використовувати таймерні сигнальні конструкції (ТСК) для формування шумоподібних сигналів. При цьому автором не вказано які параметри побудови ТСК потрібно обирати для розширення спектра при використанні методів ППРЧ та лінійної частотної модуляції. З цього приводу, доцільно було б показати ефективність розширення спектра ТСК для різних параметрів розширення. Це що було б корисним для покращення четвертого розділу дисертаційного дослідження.

Ці зауваження й запитання є елементом наукової дискусії і не впливають на загальну високу оцінку дисертації Аль-Файюмі Халеда.

Загальні висновки щодо дисертаційної роботи

Аль-Файюмі Халед представив цілком самостійну й завершену кваліфікаційну наукову працю, ретельно виконавши усі завдання дослідження.

Актуальність і рівень розкриття поставлених проблем, новизна дисертації і ступінь обґрунтованості винесених на захист наукових положень, повнота їх апробації повністю відповідають вимогам пунктів 5–8 Постанови Кабінету Міністрів України № 44 від 12.01.2022 р. «Про затвердження порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», а також Наказу Міністерства освіти та науки від 12.07.2017 р. № 40 «Про затвердження вимог до оформлення дисертації».

Вважаю, що Аль-Файюмі Халед заслуговує на присудження наукового ступеня доктора філософії (Ph.D.) за спеціальністю 125 – «Кібербезпека».

Рецензент:
професор кафедри інженерії
програмного забезпечення
Державного університету
інтелектуальних технологій і зв’язку,

доктор технічних наук, професор Гаджиєв Матін Магсуд-огли