Голові
разової спеціалізованої вченої ради
Державного університету
інтелектуальних технологій і зв'язку
вул. Кузнечна, 1, м. Одеса

ВІДГУК

офіційного опонента, доктора технічних наук, професора, головного наукового співробітника Державного науково-дослідного інституту випробування і сертифікації озброєння та військової техніки Міністерства оборони України Рудницького Володимира Миколайовича на дисертацію Аль-Файюмі Халеда «Методи підвищення захищеності інформації на основі прихованості передавання сигнально-кодових конструкцій», яка подана на здобуття наукового ступеня доктора філософії з галузі знань 12 – Інформаційні технології за спеціальністю 125 – Кібербезпека.

Актуальність теми дослідження

В сучасних умовах існування України вкрай важливим є розвиток ефективних методів захисту передаваної інформації від перехоплення та несанкціонованого доступу (НСД). Рішення даної проблеми належить до завдань інформаційної безпеки і є найважливішою прерогативою будь-якої держави. Щоб гарантувати високий ступінь захисту інформації, необхідно постійно вирішувати складні науково-технічні завдання з розробки та вдосконалення засобів її захисту. Отже, актуальним є дослідження нових високонадійних технологій захисту інформації як від перехоплення, так і від несанкціонованого доступу до конфіденційної інформації. Високі властивості прихованості сигналу потенційно, у поєднанні з ефективними алгоритмами передавання, можуть забезпечувати суттєву протидію засобам радіорозвідки та НСД по виявленню сеансу передавання, перехопленню та порушенню цілісності повідомлень, розпізнаванню структури сигналу та розкриттю смислового вмісту інформації.

З цього приводу доцільним є створення більш ефективних методів підвищення прихованості передавання сигнальних конструкцій, які базуються на нестандартних процедурах перетворення даних. В роботі запропоновано нові підходи до захисту інформації на основі позиційних і непозиційних сигналів. Розроблено методи синтезу шумоподібних сигналів, в яких основою служать таймерні сигнальні конструкції. Такі сигнальні конструкції є непозиційними та більш складними у порівнянні з позиційними кодами. Структура таймерних сигналів може змінюватися завдяки початковим параметрам їх побудови. Це дозволяє створювати різні ансамблі сигнальних конструкцій, що є основою для підвищення структурної прихованості таймерних сигналів. Автор Аль-Файюмі Халед запропонував новий підхід з розширення спектра таймерних сигнальних конструкцій, а також метод кореляційного прийому таймерних шумоподібних сигналів. Отже, формування у такий спосіб шумоподібних сигналів дозволяє змінювати їх структуру за допомогою обраних параметрів таймерних сигналів. Також розроблено метод інтеграції статистичного шифрування із завадостійким кодуванням та декореляцією помилок, що дає переваги з можливістю підвищення криптостікості даних на кожному етапі їх перетворення.

Отже, науково-прикладна задача, яка була сформульована і вирішена в дисертаційній роботі Аль-Файюмі Халеда, є досить актуальною та полягає в розробці та дослідженні методів захисту інформації на основі позиційних і непозиційних сигналів, що дозволяє підвищити ефективність передавання конфіденційних даних в умовах радіоелектронної боротьби.

Зв'язок роботи з науковими програмами, планами, темами

Тема дисертаційної роботи пов'язана з пріоритетними напрямами наукових досліджень Державного університету інтелектуальних технологій і зв'язку такими як: інформаційно-комунікаційні та радіоелектронні системи та технології, засоби радіоелектронної боротьби для забезпечення національної безпеки і оборони, системи захисту інформації від несанкціонованого доступу. Напрями дисертаційного дослідження 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» (Розділ: «Інформаційні та комунікаційні технології», підрозділ: «Інформаційно-комунікаційні та радіоелектронні системи та технології, засоби радіоелектронної боротьби для забезпечення національної безпеки і оборони. Інформаційна безпека та кібербезпека»). Основою дисертаційної роботи є результати досліджень, які висвітлені у наукових статях та тезах до конференцій. Таким чином, вважаю, що тема дисертаційної роботи Аль-Файюмі Халеда, є актуальною і відповідає тематиці з галузі знань 12 – Інформаційні технології за спеціальністю 125 – Кібербезпека.

Наукова новизна одержаних результатів.

На підставі всебічного аналізу змісту дисертаційної роботи Аль-Файюмі Халеда та дотичних наукових публікацій автора встановлено, що здобувачем досягнуто основну мету, а саме: вирішено поставлену науково-прикладну задачу щодо розробки та дослідженню методів підвищення захищеності інформації на основі прихованості передавання сигнально-кодових конструкцій.

Наукова новизна дисертації визначається такими положеннями:

1. Отримав подальший розвиток напрямок застосування динамічного хаосу в системах захисту інформації від НСД. Проведено дослідження варіаційних можливостей дискретних генераторів хаосу для формування множини псевдовипадкових послідовностей із заданими взаємно-кореляційними характеристиками, що можуть бути використані в системах потокового шифрування та прямого розширення спектра таймерних сигналів. Це особливо важливо в умовах радіоелектронної боротьби, де необхідна висока стійкість до перехоплення та аналізу сигналів.

2. Отримали подальший розвиток технології інтегрованого захисту даних від НСД, які об'єднують різні процеси перетворення даних: статистичне шифрування, завадостійке кодування та декореляція помилок. Такий підхід забезпечує зростання криптостійкості шифрограми на кожному етапі її перетворення, що є особливо доцільним в умовах радіоелектронного конфлікту, де дані піддаються ризику НСД та навмисного спотворення.

3. Отримала подальший розвиток розділ з теорії шумоподібних

сигналів, який пов'язаний з методами розширення спектра сигнальних конструкцій. Розроблено та досліджено методи формування шумоподібних сигналів на основі непозиційних таймерних сигнальних конструкцій. Запропоновано методи розширення спектра дозволяють модифікувати структуру шумоподібних сигналів відповідно до заданих параметрів, підвищуючи їх енергетичну та структурну прихованість. Це особливо актуально для протидії засобам радіоелектронного придушення сигналів в умовах конфлікту.

4. Вперше запропоновано метод розширення спектра таймерних сигналів із використанням лінійної частотної модуляції, а також розроблено спосіб кореляційного прийому таких сигналів. Цей метод є відмінним від традиційних підходів до розширення спектра позиційних сигналів, що дозволяє суттєво підвищити завадостійкість, енергетичну та структурну прихованість передачі сигнальних конструкцій, зокрема в умовах радіоелектронної боротьби, де забезпечення прихованості передачі є критично важливим.

Констатую, що всі положення наукової новизни відповідають змісту роботи, є повністю обґрунтованими і доведеними в результаті проведеного дисертаційного дослідження.

Практична цінність та впровадження отриманих результатів

Практична цінність дисертаційної роботи Аль-Файюмі Халеда визначається розробленими методами та алгоритмами, які реалізують інтеграцію розширення спектра непозиційних сигналів, статистичного шифрування, завадостійкого кодування та декореляції помилок. Здобуті результати дослідження впроваджено у навчальний процес Державного університету інтелектуальних технологій і зв'язку для підготовки бакалаврів за спеціальністю 125 «Кібербезпека та захист інформації». Також результати роботи знайшли застосування в науково-дослідній діяльності ТОВ «АЙСАЙБЕРО».

Достовірність і обґрунтованість наукових положень, висновків і рекомендацій, які сформульовано та висвітлено в дисертації

Всі отримані та сформульовані положення наукової новизни та

практичної цінності, а також висновки й рекомендації дисертації відповідають чинним вимогам до наукових робіт. Зокрема про це свідчить:

– аналіз та узагальнення відомих науково-прикладних результатів у досліджуваній галузі;

– чітке обґрунтування науково-прикладної задачі, основної мети, об'єкта й предмета дослідження;

– використання сучасних методів математичного та комп'ютерного моделювання;

– коректність аналітичних і теоретичних припущень;

– збіжність результатів розрахунків, імітаційного моделювання та експериментальних досліджень;

– перспективність запропонованих методів синтезу шумоподібних сигналів на основі непозиційних сигнальних конструкцій та інтеграції статистичного шифрування із завадостійким кодуванням і декореляцією помилок.

Ці аспекти дозволяють зробити висновок про наукову та практичну обґрунтованість отриманих результатів і сформульованих висновків у дисертаційній роботі Аль-Файюмі Халеда.

Аналіз змісту, структури та обсягу роботи

Загальний обсяг роботи становить 167 сторінок, з яких основний текст викладено на 140 сторінках машинописного тексту.

У вступі представлено обґрунтування актуальності теми дослідження, сформульовано мету, об'єкт, предмет і основні завдання роботи, описано застосовані методи дослідження, викладено наукову новизну та практичну цінність отриманих результатів. Окремо зазначено особистий внесок автора, надано загальну характеристику та структуру дисертації, а також наведено інформацію про публікації та результати апробації (впровадження) дослідницької роботи.

У першому розділі дисертаційної роботи надано детальний аналіз актуального стану проблеми захисту передаваних даних в умовах радіоелектронного конфлікту. Запропоновано модель завадозахищеної системи зв'язку, яка стала основою для аналізу методів передачі, що

забезпечують ефективний захист інформації від перехоплення, несанкціонованого доступу та впливу випадкових завад. Розглянуто перспективні методи підвищення рівнів прихованості сигналів та завадостійкості із врахуванням обраних критеріїв ефективності. На основі проведеного аналізу сформульовано наукову проблему та визначено ключові завдання дослідження.

У другому розділі дисертації проведено дослідження статистичних характеристик програмних генераторів хаосу та оцінено їх варіаційні можливості для формування псевдовипадкових послідовностей, які можуть бути застосовані в різних системах захисту інформації. Особлива увага приділена вивченню властивостей динамічного хаосу, який характеризується нерегулярними та аперіодичними процесами, що робить його перспективним інструментом для створення ефективних методів захисту. Окремо потрібно відзначити значущість використання програмних генераторів хаосу для синтезу псевдовипадкових послідовностей у системах розширення спектра. Такі послідовності є ключовим елементом для формування шумоподібних сигналів, за допомогою яких є можливість забезпечити високий рівень завадостійкості та прихованості передавання даних. Це дає можливість забезпечити маскування передаваних сигнальних конструкцій, ускладнюючи їх перехоплення або спотворення в умовах радіоелектронної боротьби. Результати досліджень дозволяють не лише розкрити потенціал динамічного хаосу для задач криптографії, але й сприяють розвитку сучасних систем зв'язку з розширеним спектром, які є важливими для захисту в умовах сучасних загроз кібер- та радіоелектронної безпеки.

У третьому розділі досліджуються та аналізуються методи інтеграції шифрування та завадостійкого кодування. Доцільність такої інтеграції пояснюється можливістю об'єднання в єдиний процес шифрування і завадостійке кодування. В роботі розроблено метод інтеграції статистичного шифрування із завадостійким кодуванням та декореляцією помилок. Показано доцільність такої інтеграції, яка дозволяє на кожному етапі перетворення підвищувати криптостійкість статистичного шифрування. Це досягається завдяки збільшенню довжини випадкових кодових комбінацій

шляхом додавання до них перевірочних біт завадостійкого коду. Використання декореляції помилок, зокрема завдяки додатковому перемішуванню біт, дозволяє зменшити групування помилок, підвищуючи завадостійкість передачі та криптостійкість статистичного шифрування. Така комбінація процесів перетворення даних забезпечує не тільки зниження ймовірності помилок, але й підвищення загальної криптостійкості, що є критично важливим для реальних завадозахищених систем зв'язку, особливо в умовах радіоелектронної боротьби. Таким чином, вважаю, що метод комбінованого статистичного шифрування може бути застосований для розробки реальних завадозахищених систем зв'язку, в яких вирішується задача підвищення прихованості і завадостійкості передавання конфіденційної інформації.

У четвертому розділі надано обґрунтування доцільності застосування непозиційних сигналів, якими є таймерні сигнальні конструкції, для завдань формування шумоподібних сигналів. Пояснюється це властивостями побудови таймерних сигналів за певними параметрами, що дає можливість змінювати їх структуру з урахуванням вимог до структурної прихованості і завадостійкості передачі. Визначено, що ускладнення структури передаваного сигналу дозволяє розв'язати низку завдань щодо підвищення енергетичної та структурної прихованості сигнальних конструкцій. Це особливо важливо при перехопленні сеансу радіозв'язку засобами радіоелектронної розвідки супротивника. З цього приводу розроблено та досліджено методи синтезу шумоподібних сигналів на основі таймерних сигнальних конструкцій, що суттєво відрізняються від відомих методів розширення спектра, які були розроблені для позиційних сигналів. Важливість цього дослідження полягає в забезпеченні енергетичної та структурної прихованості шумоподібних сигналів, що робить їх більш стійкими до виявлення та перехоплення в умовах радіоелектронної боротьби. Окрім того, запропоновані методи включають використання псевдовипадкових послідовностей та псевдовипадкового перескоку робочої частоти для ефективного розширення спектра, а також метод лінійної частотної модуляції для підвищення рівня завадостійкості. Окремо

розроблено метод кореляційного прийому таймерного шумоподібного сигналу з виділенням імпульсів фронтів сигнальної конструкції, що сприяє покращенню якості прийому та зменшенню ймовірності виявлення сигналу в складних умовах.

У загальних висновках наведено основні кількісні та якісні результати дисертаційного дослідження.

У додатках наведено список публікацій здобувача за темою дисертації, акти впровадження та використання результатів дисертаційного дослідження.

У результаті аналізу змісту дисертаційної роботи Аль-Файюмі Халеда встановлено, що вона повністю відповідає Стандарту вищої освіти зі спеціальності 125 – «Кібербезпека» галузі знань 12 – «Інформаційні технології» для третього (освітньо-наукового) рівня вищої освіти та ОНП спеціальності 125 – «Кібербезпека» Державного університету інтелектуальних технологій і зв'язку.

На підставі перевірки дисертації на вимоги доброчесності встановлено, що дисертаційна робота Аль-Файюмі Халеда є результатом оригінальних і самостійних досліджень. Вона не містить елементів фальсифікації, фабрикації та текстових запозичень без посилань на відповідні джерела.

Отже, можна констатувати, що дисертація Аль-Файюмі Халеда є завершеним, оригінальним, змістовним, логічним і структурованим науково-прикладним дослідженням, що дозволяє йому в повному обсязі розкрити тему дослідження та досягти поставленої мети.

Мова та стиль викладання результатів

Дисертація Аль-Файюмі Халеда написана українською мовою. Стиль викладення матеріалів досліджень у цілому є лаконічним, структурованим, чітким і логічним.

Повнота викладу основних положень дисертації в опублікованих наукових працях

За темою дисертаційного дослідження здобувач Аль-Файюмі Халед опублікував 16 наукових праць, серед 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 доповідей у журналах, які цитуються у наукометричних базах даних Scopus. Одна наукова праця включена до складу монографії.

Загалом кількість і тип друкованих праць відповідає актуальним вимогам Міністерства освіти і науки України щодо публікацій основного змісту дисертації на здобуття ступеня доктора філософії. Змістовна наповненість та тематика опублікованих наукових праць дозволяє стверджувати, що наукові результати, які виносяться на захист, було повністю охоплено і висвітлено в публікаціях.

Зауваження та дискусійні положення

1. В описі актуальності роботи (с.22-24) та першому розділі (с.30-65) не в повній мірі охарактеризовані основні критерії ефективності, які призначені для оцінки запропонованих методів підвищення ефективності захисту інформації (наприклад, інформаційна прихованість, структурна прихованість енергетична прихованість, тощо).

2. У науковій новизні одержаних результатів вступу (с.26) та у другому розділі автор відзначив використання псевдовипадкових послідовностей (ПВП), що сформовані на основі програмних генераторів хаосу, для завдання розширення спектра сигнальних конструкцій. Проте далі приклади їх застосування в роботі відсутні.

3. У четвертому розділі п.4.3 (с.130) автор пропонує в інтегрованому методі розширення спектра таймерних сигналів використовувати спочатку пряме розширення спектра за допомогою ПВП, а потім задіяти один із видів псевдовипадкового перескоку робочої частоти. Проте при прямому розширенні спектра таймерних сигналів автор не акцентує уваги на доцільність використання для підвищення структурної прихованості послідовностей, що сформовані на основі програмного генератору хаосу.

4. На думку опонента, для покращення загальної структури роботи доцільно було б використати результати другого розділу з дослідженнями та методами розширення спектра таймерних сигналів четвертого розділу. Тобто, для інтегрованого методу розширення спектра таймерних сигналів потрібно було б використати двійкові послідовності, які були запропоновані у другому

розділі шляхом перетворення числової послідовності, сформовані за допомогою генератору хаосу.

5. Підрозділи пп.1.1-1.3 дещо перевантажені зайвими теоретичними відомостями загальнонаукового та навчально-методичного характеру. Те саме можна зазначити стосовно початку основних розділів 2 та 3.

6. У роботі недостатню увагу приділено питанням розробки рекомендацій щодо питань використання методів розширення спектра таймерних сигналів та результатам дослідження програмних генераторів хаосу.

7. При аналізі ефективності методу статистичного шифрування з інтеграцією завадостійкого кодування та декореляцією помилок доцільним було б показати, як збільшується криптостійкість на кожному кроці перетворення даних. Також не надано порівняльний аналіз запропонованої системи шифрування з іншими існуючими криптографічними протоколами, що бажано було б зробити для повноти дослідження.

8. У роботі також присутні: деякі неточності застосування спеціальної термінології (наприклад, «перешкоди» замість «завади», с.34, с.48, с.138), «русизми» («таким чином», с. 4, с.7, с.22, с.31, с.41, с.51, с.65, с.69, с.72, с.138 тощо), небажані застосування прийменника «по» (с.118-120, с.124, с.125, с.129, с.133, с.137, тощо).

9. У роботі присутні деякі орфографічні неточності та невластиві українській мові терміни, а також друкарські помилки.

Разом з цим зазначені зауваження істотно не впливають на загальний високий науковий рівень дисертаційної роботи та не знижують її науково-практичну цінність. Ці зауваження переважно носять уточнюючий характер та/або показують перспективу подальшого розвитку результатів досліджень автора у майбутньому.

Висновок

На підставі детального аналізу дисертації та наукових публікацій здобувача Аль-Файюмі Халеда, а також, приймаючи до уваги актуальність теми роботи, положення наукової новизни, практичну значущість, показники обґрунтованості та достовірності одержаних результатів і сформульованих

висновків по роботі, вважаю, що його дисертація «Методи підвищення захищеності інформації на основі прихованості передавання сигнально-кодових конструкцій» є завершеним і самостійним дослідженням, присвяченим вирішенню актуальної науково-прикладної задачі підвищення прихованості передавання інформації в інформаційно-комунікаційних системах на основі розробки методів інтеграції процесів таймерного кодування, статистичного шифрування та синтезу шумоподібних сигналів.

Зазначаю, що дисертація Аль-Файюмі Халеда відповідає 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».

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

Офіційний опонент
головний науковий співробітник
Державного науково-дослідного
інституту випробування і сертифікації
озброєння та військової техніки
Міністерства оборони України,
доктор технічних наук, професор

Володимир РУДНИЦЬКИЙ

Підпис Рудницького В.М. завіряю:
Вчений секретар науково-технічної ради
Кандидат технічних наук, с.н.с.

Олександр БУРСАЛА

03 02 2025 р.