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

ВІДГУК

офіційного опонента, кандидата технічних наук (спеціальність 05.13.21 – системи захисту інформації), доцента, декана факультету комп'ютерних наук та технологій Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут» Фесенка Андрія Олексійовича на дисертацію **Аль-Файюмі Халеда** на тему «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 та захист інформації»

Актуальність теми дисертації

Умови радіоелектронної боротьби (РЕБ) значно ускладнюють процес передавання даних через активне використання цілеспрямованих завад, перехоплення та інші види атак. Традиційні методи захисту інформації часто виявляються не ефективними, оскільки зловмисники розробляють нові технології атак, адаптуючи їх до специфіки РЕБ.

Переважна більшість існуючих систем захисту інформації орієнтована на використання позиційних сигналів. Зазвичай криптографічні методи, види модуляції та алгоритми розширення спектра базуються на сигнальних конструкціях, де тривалість імпульсів у кодових словах залишається постійною. Водночас ускладнені умови РЕБ вимагають створення нових підходів до формування сигнальних конструкцій. З цієї причини автором дисертації запропоновано використання непозиційних сигналів, таких як таймерні та хаотичні, параметри побудови яких можна адаптувати до змін середовища передавання інформації та забезпечувати більший рівень її захисту.

Представлені в дисертації методи таймерного кодування показують унікальні можливості по генеруванню різноманітних ансамблів сигналів. Ця властивість ускладнює структуру сигнально-кодових конструкцій, особливо таймерних шумоподібних сигналів. Розроблені методи розширення спектра таймерних сигналів значно підвищують рівень їх прихованості, навіть у разі

перехоплення.

Запропонований інтегрований метод захисту інформації на основі статистичного шифрування, завадостійкого кодування та декореляції помилок дозволяє поєднати функції захисту інформації від несанкціонованого доступу та завадостійкості, при цьому на кожному етапі перетворення даних забезпечується підвищення криптостійкості повідомлення.

Автором роботи проведено дослідження, засноване на методах системного та порівняльного аналізу, кореляційного аналізу, а також теорії ймовірності та завадостійкого кодування, теорії прихованості та криптографії.

Отже, науково-прикладна задача, яка була сформульована і вирішена в дисертації Аль-Файюмі Халедом, є актуальною. Вона полягає в розробці перспективних методів захисту інформації на основі таймерних широкосмугових сигналів та інтегрованих методів перетворення даних з поєднанням шифрування та завадостійкого кодування, що дозволяє підвищити рівень прихованості та завадостійкості, що особливо важливо для передавання інформації в умовах радіоелектронного конфлікту.

Зв'язок роботи з науковими програмами, планами, темами

Напрями дослідження в дисертаційної роботі безпосередньо пов'язані із науково-технічними завданнями, які сформульовано в Постанові Кабінету Міністрів України № 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 захисту передаваної інформації в інформаційно-комунікаційних системах на основі розробки методів інтеграції процесів розширення спектра таймерних сигналів, статистичного шифрування та завадостійкого кодування є актуальною і відповідає тематиці з галузі знань 12 – Інформаційні технології за спеціальністю 125 Кібербезпека та захист інформації.

Наукова новизна одержаних результатів

На підставі аналізу дисертаційної роботи Аль-Файюмі Халеда встановлено, що здобувачем вирішено поставлену науково-прикладну задачу щодо розробки та дослідженню інтеграції методів розширення спектра з використанням непозиційних таймерних сигналів, а також методів інтеграції статистичного шифрування та завадостійкого кодування з декореляцією помилок. Наукова новизна дисертації полягає в наступному:

1. Вперше на основі кореляційного аналізу обґрунтовано доцільність дослідження варіаційних можливостей дискретних генераторів хаосу по

формуванню безлічі псевдовипадкових послідовностей із заданими взаємно-кореляційними властивостями для систем потокового шифрування та прямого розширення спектра таймерних сигналів.

2. Вперше встановлено доцільність для підвищення рівня захисту передаваних повідомлень від несанкціонованого доступу інтеграції процесів статистичного шифрування, завадостійкого кодування та декореляції помилок, що дозволяє на кожному етапі перетворення даних підвищувати їх криптостійкість.

3. Вперше встановлено доцільність розширення спектра непозиційних таймерних сигналів, що дає можливість змінювати за заданими параметрами змінювати структуру шумоподібних сигналів, що збільшує їх рівень енергетичної та структурної прихованості.

4. Вперше запропоновано розширення спектра таймерних сигналів за допомогою лінійної частотної модуляції, а також розроблено метод кореляційного прийому таких сигналів, що відрізняється від відомих методів розширення спектра позиційних сигналів та їх прийому. Все це дало змогу підвищити завадостійкість, енергетичну та структурну прихованості передавання сигнальних конструкцій.

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

Практична цінність та впровадження отриманих результатів

Основу практичної цінності результатів дисертаційного дослідження Аль-Файюмі Халеда становлять методи та алгоритми, що реалізують запропоновані методи інтеграції розширення спектра непозиційних сигналів, статистичного шифрування, завадостійкого кодування та декореляції помилок. Отримані результати досліджень використано та впроваджено в навчальному процесі Державного університету інтелектуальних технологій і зв’язку при підготовці бакалаврів спеціальності 125 Кібербезпека та захист інформації. Результати дисертації мають впровадження у наукових дослідженнях ТОВ «АЙСАЙБЕРО».

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

Отримані та сформульовані положення наукової новизни та практичної цінності, а також основні висновки дисертації відповідають чинним вимогам до наукових робіт. Зокрема, про це свідчить:

– виконаний аналіз і узагальнення відомих науково-прикладних результатів у досліджуваній предметній галузі;

– обґрунтованість науково-прикладної задачі, основної мети, а також об’єкту й предмету досліджень; застосування сучасних методів математичного та комп’ютерного моделювання;

– коректність аналітичних і теоретичних припущень;

– збіжність результатів розрахунків та імітаційного моделювання експерименту;

– перспективність розробки нових методів синтезу шумоподібних сигналів на основі непозиційних сигнальних конструкцій, а також методу інтеграції статистичного шифрування із завадостійким кодуванням та декореляцією помилок.

Вказане дозволяє стверджувати про достовірність і обґрунтованість наукових положень і висновків, сформульованих 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 обґрунтовано актуальність теми досліджень, сформульовано мету, об’єкт, предмет і основні завдання досліджень, обґрунтовано методи досліджень, сформульовано наукову новизну й практичну значимість одержаних результатів, зазначено особистий внесок здобувача, представлено загальну характеристику та структуру дисертації, а також наведено відомості щодо публікацій і результатів апробації дисертаційної роботи.

У першому розділі дисертаційної роботи виконано аналіз актуального стану проблеми захисту передаваної інформації в умовах радіоелектронного конфлікту. Запропонована модель завадозахищеної системи зв’язку, на основі якої виконано аналіз методів передавання, що забезпечують захист інформації від перехоплення, несанкціонованого доступу та випадкових завад. Надано аналіз перспективним методом підвищення показників прихованості та завадостійкості на основі обраних критеріїв ефективності. Сформульовано наукову проблему та задачі дослідження.

У другому розділі виконано дослідження статистичних характеристик програмних генераторів хаосу та надана оцінка їх варіаційним можливостям по формуванню псевдовипадкових послідовностей для використання їх в різних системах захисту інформації. Обґрунтування цього дослідження пояснюється особливими властивостями динамічного хаосу, для якого характерним є деякий нерегулярний та аперіодичний процес.

У третьому розділі розроблено метод інтеграції статистичного шифрування із завадостійким кодованням та декореляцією помилок. Показано

як за допомогою багаторівневого перетворення даних на кожному кроці забезпечується підвищення криптостійкості статистичного шифрування, при якому перевірочні біти завадостійкого коду збільшують довжину випадкових комбінацій. Використання декореляції помилок забезпечує додаткове перемішування біт передаваних кодових блоків та зменшує групування помилок у дискретному каналі. Обґрунтовано, 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 розроблено та досліджено методи синтезу шумоподібних сигналів на основі таймерних сигнальних конструкцій. Запропоновано інтегровані методи розширення спектра таймерних сигналів на основі псевдовипадкових послідовностей та псевдовипадкового перескоку робочої частоти. Розроблено метод розширення спектра таймерного сигналу за допомогою лінійної частотної модуляції. Запропоновано кореляційний прийом таймерного шумоподібного сигналу з виділенням імпульсів фронтів сигнальної конструкції.

У загальних висновках наведено основні результати дисертаційного дослідження.

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

На підставі перевірки дисертації на вимоги доброчесності встановлено, що ця робота Аль-Файюмі Халеда є результатом оригінальних і самостійних досліджень, вона не містить текстових запозичень без посилань на відповідні джерела.

Дисертація Аль-Файюмі Халеда є завершеним, змістовним, логічним і структурованим науково-прикладним дослідженням, що дозволило 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 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 виданнях України (категорії Б), 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.

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

Зауваження та дискусійні положення

1. В підрозділі п.1.5 запропоновано метод підвищення структурної прихованості сигнальних конструкцій за допомогою різних видів модуляції шляхом періодичності зміни кута розташування векторів у сузір'ї системи модуляції КАМ-16 (рис. 1.11). При цьому, не представлені чисельні показники отриманої структурної прихованості у порівнянні з результатами табл. 1.3.

2. В розділі 3 для того, щоб охарактеризувати інтегрований метод перетворення даних на основі статистичного шифрування, завадостійкого кодування та декореляції помилок, в одному випадку використовується поняття «інформаційна прихованість» (стор. 95), а в іншому випадку «криптостійкість» (стор. 96). При цьому автором не надано пояснень з цього приводу.

3. Для покращення загальної структури розділу 2 бажано було надати більше прикладів застосування отриманих результатів, що стосується формування двійкових псевдовипадкових послідовностей на основі програмних генераторів хаосу.

4. В загальних висновках не в повній мірі охарактеризовані результати та чисельні показники, які були отримані у другому розділі дисертаційної роботи, насамперед, це стосується дослідження програмних генераторів хаосу.

5. З огляду на досить значну кількість наукових та прикладних результатів, отриманих автором, бажано було збільшити кількість загальних висновків в роботі.

6. У роботі присутні деякі орфографічні неточності та невластиві українській мові терміни.

Зазначені зауваження істотно не впливають на загальний високий науковий рівень дисертаційної роботи та не знижують її науково-практичну цінність. Ці зауваження переважно показують перспективу подальшого розвитку результатів досліджень автора у майбутньому.

Висновок

На підставі розгляду дисертації здобувача Аль-Файюмі Халеда, приймаючи до уваги актуальність теми роботи, положення наукової новизни, практичну значущість, показники обґрунтованості та достовірності одержаних результатів, вважаю, що представлена на захист 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.

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».

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

Офіційний опонент
декан факультету комп’ютерних наук
та технологій Державного некомерційного
підприємства «Державний університет
«Київський авіаційний інститут»,
доцент, кандидат технічних наук Андрій ФЕСЕНКО