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

Актуальність роботи

В сучасних умовах протистояння України загрозам у сфері інформаційної безпеки актуальним завданням є розробка ефективних методів захисту передавання даних від перехоплення та несанкціонованого доступу (НСД). Особливу складність цьому процесу додають умови радіоелектронної боротьби (РЕБ), коли застосовуються цілеспрямовані завади, перехоплення сигналів та інші види атак. Традиційні підходи до захисту інформації виявляються недостатньо ефективними через стрімкий розвиток нових технологій атак з боку зловмисників.

Більшість сучасних систем захисту орієнтована на використання позиційних сигналів із фіксованою тривалістю імпульсів у кодових словах. Проте ускладнені умови РЕБ вимагають інноваційних рішень для забезпечення захисту інформації. У дисертаційній роботі Аль-Файюмі Халеда запропоновано нові підходи до захисту даних, засновані на застосуванні непозиційних сигналів, таких як таймерні та хаотичні. Їх параметри можуть бути адаптовані до динамічних умов середовища, що підвищує рівень прихованості та захищеності даних.

Розроблені методи формування шумоподібних сигналів на основі таймерних конструкцій дозволяють генерувати різноманітні ансамблі сигналів зі змінною структурою. Завдяки цьому досягається суттєве ускладнення сигнально-кодових конструкцій, що підвищує їх стійкість до перехоплення та спроб аналізу. Запропоновані нові методи розширення спектра таймерних сигналів забезпечують їх високу ефективність навіть у складних умовах РЕБ.

Інтегрований метод захисту, що поєднує статистичне шифрування, завадостійке кодування та декореляцію помилок, створює додатковий рівень криптостійкості на кожному етапі перетворення даних. Такі методи забезпечують одночасно захист від НСД і завадостійкість, що є надзвичайно важливим для забезпечення конфіденційності даних у складних радіоелектронних умовах.

У роботі використано методи системного та порівняльного аналізу, кореляційного аналізу, теорії ймовірності, завадостійкого кодування, прихованості та криптографії. Науково-прикладна задача, сформульована та вирішена в дисертаційній роботі, полягає в розробці перспективних методів захисту інформації на основі таймерних широкосмугових сигналів і інтегрованого перетворення даних. Це дозволяє суттєво підвищити рівень прихованості, завадостійкості та ефективності передавання конфіденційних даних, що є критично важливим у сучасних умовах інформаційного протистояння.

Дисертаційна робота є складовою частиною досліджень, що проводяться в Державному університеті інтелектуальних технологій і зв’язку відповідно до Постанови Кабінету Міністрів України № 942 від 07.09.2011 р. із змінами, внесеними постановою КМ № 463 від 09.05.2023 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 конференцій.

Наукові результати та їх новизна

Вирішення поставлених завдань дисертаційної роботи виконано на основі нових наукових положень, які полягають у наступному:

1. Отримала подальший розвиток частина теорії динамічного хаосу, яка пов’язана з обґрунтуванням доцільності використання дискретних генераторів для формування множини псевдовипадкових послідовностей із заданими кореляційними властивостями. Ці послідовності знайшли застосування в системах потокового шифрування та розширення спектра таймерних сигналів, що особливо актуально для забезпечення прихованості інформації в умовах радіоелектронної боротьби.

2. Отримали подальший розвиток методи інтегрованого захисту інформації від несанкціонованого доступу, що дало змогу довести ефективність поєднання статистичного шифрування, завадостійкого кодування та декореляції помилок. Такий підхід створює єдиний процес захисту даних, забезпечуючи підвищену криптостійкість і завадостійкість до зовнішніх впливів на кожному етапі перетворення інформації.

3. Отримала подальший розвиток теорія сигналів, яка пов’язана з методикою формування синтезу шумоподібних сигнальних конструкцій на основі непозиційних таймерних сигналів, структуру яких можна змінювати за заданими параметрами їх побудови. Це сприяє підвищенню їх енергетичної та структурної прихованості, що є критично важливим для протидії перехопленню сигналів.

4. Вперше запропоновано розширення спектра таймерних сигналів із застосуванням лінійної частотної модуляції. Розроблено метод кореляційного прийому таких сигналів, що відрізняється від традиційних підходів. Це забезпечує зростання завадостійкості, прихованості та енергоефективності передачі даних.

Отримані результати дозволяють значно підвищити стійкість інформаційних систем до несанкціонованого доступу та навмисних завад, що підтверджується проведеним комплексним аналізом та дослідженнями.

Практичне значення та практична цінність отриманих результатів

Практичне значення результатів дослідження полягає у створенні та впровадженні нових методів і алгоритмів, які забезпечують інтеграцію технологій розширення спектра непозиційних сигналів, статистичного шифрування, завадостійкого кодування та декореляції помилок. Зокрема:

– проведено аналіз сучасних методів розширення спектра, визначено їх ефективність у забезпеченні структурної та енергетичної прихованості передачі інформації в умовах радіоелектронної боротьби;

– доведено доцільність застосування непозиційних таймерних сигналів, що мають складну структуру та здатні змінювати параметри сигнальних конструкцій;

– розроблено нові методи розширення спектра з використанням таймерних сигналів, побудовані на псевдовипадковому перескоку робочих частот і лінійній частотній модуляції, які значно підвищують прихованість інформації;

– запропоновано кореляційний метод прийому таймерних шумоподібних сигналів на основі лінійної частотної модуляції, що дозволяє виділяти фронти імпульсних складових із різною тривалістю в межах сигнальної конструкції.

Достовірність і обґрунтованість результатів підтверджуються:

– аналізом і узагальненням відомих науково-прикладних результатів у досліджуваній галузі;

– чітким обґрунтуванням науково-прикладної задачі, мети, об’єкта та предмета дослідження;

– використанням сучасних методів математичного та комп’ютерного моделювання;

– коректністю аналітичних і теоретичних припущень;

– збіжністю результатів розрахунків, імітаційного моделювання та експериментальних даних;

– перспективністю запропонованих методів синтезу шумоподібних сигналів і інтеграції статистичного шифрування із завадостійким кодуванням та декореляцією помилок.

Ці фактори свідчать про наукову новизну, практичну цінність та обґрунтованість результатів, сформульованих у дисертаційній роботі.

Отримані результати дослідження впроваджено в навчальний процес Державного університету інтелектуальних технологій і зв’язку для підготовки бакалаврів за спеціальністю 125 «Кібербезпека та захист інформації». Також вони знайшли застосування в наукових дослідженнях ТОВ «АЙСАЙБЕРО». Усі впровадження підтверджено відповідними документами, наведеними у додатках.

Оцінка змісту, ступеню завершеності та обґрунтованості положень дисертації

Повний обсяг дисертаційної роботи складає 167 сторінок, з яких 120 сторінок – основний текст. Список використаних джерел містить 113 найменувань.

У **вступі** обґрунтовано актуальність теми дослідження, сформульовано мету, об’єкт, предмет і основні завдання дисертаційної роботи. Описано застосовані методи дослідження, визначено наукову новизну, теоретичне та практичне значення отриманих результатів. Також зазначено особистий внесок здобувача, надано загальну характеристику й структуру дисертації, а також інформацію про публікації й результати апробації дослідницької роботи.

У **першому розділі** проведено аналіз сучасного стану проблеми захисту передаваної інформації в умовах радіоелектронного конфлікту. Визначено ключові напрями дослідження та сформульовано наукову проблему. Запропоновано модель завадозахищеної системи зв’язку, яка стала основою для

аналізу методів передачі, спрямованих на забезпечення захисту даних від перехоплення, несанкціонованого доступу й впливу випадкових завад. Особливу увагу приділено перспективним методам підвищення рівня прихованості та завадостійкості сигналів із урахуванням сучасних критеріїв ефективності, зокрема псевдовипадкового перескоку частоти, прямого розширення спектра та використання хаотичних коливань.

Спираючись на результати проведеного аналізу вибрано мету роботи та сформульовані задачі дисертаційного дослідження.

Другий розділ присвячено дослідженню статистичних характеристик програмних генераторів хаосу, які використовуються для формування псевдовипадкових послідовностей у системах захисту інформації. Вивчено варіаційні можливості таких генераторів і їхню здатність забезпечувати нерегулярний та аперіодичний характер сигналів. Зазначено, що ці особливості сприяють маскуванню передаваних сигнальних конструкцій і підвищенню завадостійкості в умовах радіоелектронної боротьби. Отримані результати підтверджують перспективність динамічного хаосу для криптографії та розвитку сучасних систем зв'язку.

У третьому розділі розглянуто методи інтеграції статистичного шифрування із завадостійким кодуванням та декореляцією помилок. Обґрунтовано доцільність такого підходу, який дозволяє об'єднати процеси шифрування й кодування для підвищення криптостійкості й завадозахищеності. Показано, що додавання перевірочних біт завадостійкого коду збільшує довжину випадкових кодових комбінацій, а використання декореляції помилок зменшує групування помилок у каналі. Така інтеграція є основою для створення реальних завадозахищених систем зв'язку, здатних забезпечити надійну передачу конфіденційної інформації.

Четвертий розділ присвячено методам формування шумоподібних сигналів на основі таймерних сигнальних конструкцій. Розроблено методи розширення спектра таких сигналів за допомогою псевдовипадкових послідовностей, псевдовипадкового перескоку частоти та лінійної частотної модуляції. Запропоновано кореляційний прийом таймерних сигналів для забезпечення енергетичної та структурної прихованості. Зазначено, що застосування таких методів підвищує стійкість сигналів до виявлення та перехоплення в умовах радіоелектронної боротьби.

У загальних висновках підсумовано основні кількісні та якісні результати дослідження. Окремо зазначено значущість запропонованих методів для підвищення завадостійкості та прихованості систем зв'язку в сучасних умовах.

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

Повнота викладення результатів дисертації у наукових виданнях

Ознайомлення з дисертаційною роботою та науковими працями дозволяє зробити висновок про дотримання здобувачем вимог щодо повноти викладення результатів дисертації у наукових виданнях. Основні результати досліджень викладено в 16 публікаціях. Серед них: 6 статей у фахових наукових виданнях

України (у тому числі 1 стаття в журналі, включеному до наукометричної бази Scopus) і 9 тез доповідей на Всеукраїнських і Міжнародних конференціях, у тому числі 2 тези доповіді у журналах, які цитуються у наукометричних базах даних Scopus. Одна наукова праця включена до складу монографії. Наведений перелік публікацій, їх зміст та обсяг у достатній мірі відображають особистий внесок автора і відповідають вимогам, що висуваються до дисертації на здобуття наукового ступеня доктора філософії.

Оформлення дисертації та дотримання вимог академічної доброчесності

Дисертаційна робота виконана із дотриманням вимог наукового стилю, із застосуванням сучасної термінології. Тема, зміст і здобуті наукові результати роботи повністю відповідають спеціальності 125 – Кібербезпека у галузі знань 12 – Інформаційні технології.

Аналіз опублікованих автором наукових праць та змісту дисертації свідчить, що всі наукові й практичні результати отримані особисто здобувачем. У дисертації не виявлено текстових запозичень чи використання результатів інших науковців без належного посилання на відповідні джерела.

Зауваження до дисертаційної роботи.

1. В роботі не в повній мірі обґрунтовано вибір критеріїв ефективності для оцінки запропонованих методів підвищення прихованості сигнально-кодових конструкцій на основі розширення спектра таймерних сигналів (п. 1.4, п. 1.5), а також методів захисту інформації на основі інтеграції статистичного шифрування, завадостійкого кодування з декореляцією помилок.
2. Роботу можна було б покращити, використавши порівняльний аналіз криптографічної стійкості на кожному кроці перетворення даних запропонованого методу інтеграції статистичного шифрування, завадостійкого кодування з декореляцією помилок. Це дало би змогу реально побачити, яка ефективність додаткових процедур перетворення даних на основі завадостійкого коду та декореляції помилок для підсилення криптостійкості запропонованого методу.
3. При імітаційному моделюванні методу розширення спектра таймерних сигналів за допомогою лінійної частотної модуляції (п. 4.6) доцільно було надати більше значень відношення сигнал до шуму (рис. 4.6, с. 138) для того, щоб отримати достатній ряд ймовірностей спотворення сигнальних конструкцій при кореляційному прийомі.
4. У запропонованих методах розширення спектра не надано інформації з приводу узгодження параметрів побудови таймерних сигналів з параметрами методів розширення спектра, що особливо важливо для забезпечення таких показників як завадостійкість, енергетична та структурна прихованість сигнальних конструкцій.
5. В роботі мають місце деякі граматичні та стилістичні помилки, а також невластиві українській мові терміни.

Вказані зауваження не знижують загального позитивного враження від дисертації, як з точки зору актуальності теми, так і наукової новизни та практичної цінності отриманих результатів.

Висновок про відповідність дисертації вимогам, які пред'являються до наукового ступеня доктора філософії

Дисертаційна робота Аль-Файюмі Халеда «Методи підвищення захищеності інформації на основі прихованості передавання сигнально-кодових конструкцій» є завершеною науково-дослідницькою роботою, яка містить нові науково обґрунтовані результати. У дисертації вирішено актуальну науково-прикладну задачу підвищення захищеності інформації на основі прихованості передавання сигнально-кодових конструкцій, що зумовлено зростаючими вимогами до забезпечення безпеки інформаційних систем в умовах постійного ускладнення загроз і методів несанкціонованого доступу до даних.

Тема і зміст дисертаційної роботи відповідають спеціальності 125 – Кібербезпека, а отримані наукові та практичні результати є значущими для галузі знань 12 – Інформаційні технології.

Зважаючи на актуальність теми дисертації, обґрунтованість наукових результатів, висновків та рекомендацій, їх наукову новизну та практичну цінність, повноту викладення матеріалу у наукових публікаціях, відсутність порушень академічної доброчесності, вважаю, що дисертація Аль-Файюмі Халеда відповідає вимогам «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого постановою Кабінету Міністрів України від 12 січня 2022 р. № 44 та вимогам наказу МОН України № 40 від 12.01.2017 р. «Про затвердження вимог до оформлення дисертації», а її автор, Аль-Файюмі Халед, заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 125 – «Кібербезпека».

Рецензент:
доцент кафедри кібербезпеки та
технічного захисту інформації
Державного університету інтелектуальних
технологій і зв'язку,
кандидат технічних наук, доцент Олексій ОНАЦЬКИЙ