

РЕЦЕНЗІЯ

на дисертаційну роботу Гавеля Сергія Миколайовича на тему «Підвищення прихованості передавання інформації на основі прямого розширення спектра таймерних сигнальних конструкцій», подану на здобуття наукового ступеня доктора філософії за галуззю знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека

1. Обґрунтування вибору теми дослідження

Забезпечення прихованості передавання інформації є важливою складовою захисту інформаційних ресурсів у безпроводових інформаційно-комунікаційних системах (ІКС). Особливого значення ця проблема набуває в умовах радіоелектронного протиборства (РЕП), застосування засобів радіоелектронної розвідки (РЕР) та зростання кіберзагроз, коли недостатньо забезпечити лише достовірність і завадостійкість передавання інформації. Важливим завданням є також ускладнення виявлення сигналу, визначення його параметрів та встановлення принципів формування сигнальної конструкції стороннім спостерігачем. Це зумовлює необхідність розроблення та вдосконалення методів формування сигналів із підвищеними властивостями енергетичної та структурної прихованості.

Одним із перспективних напрямів підвищення прихованості передавання інформації є використання таймерних сигнальних конструкцій (ТСК), у яких інформація передається параметрами часової структури сигналу. На відміну від традиційних позиційних сигнальних конструкцій, застосування ТСК забезпечує формування значної кількості структурно різних сигнальних реалізацій, що створює додаткові можливості для ускладнення їх розпізнавання та аналізу. Використання непозиційного принципу формування сигналу дозволяє розглядати ТСК як перспективну основу для підвищення структурної прихованості передавання інформації.

Водночас для підвищення енергетичної прихованості доцільним є поєднання таймерного кодування з методами прямого розширення спектра (ПРС). Розподіл енергії сигналу в широкій смузі частот знижує його спектральну щільність потужності та ускладнює виявлення на фоні шумів і завад. Застосування псевдовипадкових послідовностей (ПВП) для розширення спектра додатково змінює кореляційні та структурні властивості сигналу, що може підвищувати складність його аналізу засобами РЕР.

Актуальність дослідження визначається також необхідністю встановлення взаємозв'язку між параметрами таймерних сигналів, характеристиками ПВП, шириною спектра та видом модуляції і рівнем прихованості та завадостійкості передавання інформації. Важливим завданням є визначення оптимального співвідношення між енергетичною та структурною прихованістю, достовірністю передавання, пропускнуою здатністю та складністю технічної реалізації системи.

Дисертаційна робота Гавеля Сергія Миколайовича «Підвищення прихованості передавання інформації на основі прямого розширення спектра таймерних сигнальних конструкцій» присвячена розв'язанню актуального науково-прикладного завдання, пов'язаного з розробленням та дослідженням

методів формування широкосмугових шумоподібних таймерних сигналів. Поєднання непозиційного таймерного кодування з ПРС створює передумови для комплексного підвищення прихованості передавання інформації та розширює можливості застосування таких сигнальних конструкцій у захищених ІКС.

Отже, вибір теми дисертаційного дослідження є обґрунтованим, а сама тема відповідає сучасним завданням захисту інформації в ІКС і має як теоретичне, так і практичне значення.

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

Зміст дисертаційної роботи відповідає стандарту вищої освіти та освітньо-науковій програмі підготовки докторів філософії за спеціальністю 125 Кібербезпека Державного університету інтелектуальних технологій і зв'язку. Дослідження спрямоване на розв'язання науково-прикладного завдання підвищення прихованості передавання інформації шляхом використання таймерних сигнальних конструкцій, широкосмугових шумоподібних сигналів та методів прямого розширення спектра на основі псевдовипадкових послідовностей.

Тематика дисертаційної роботи відповідає науковому напрямку кафедри кібербезпеки та технічного захисту інформації, пов'язаному з розробленням і дослідженням методів підвищення захищеності інформації в інформаційно-комунікаційних системах, формуванням захищених сигнально-кодових конструкцій та забезпеченням прихованості передавання інформації в умовах впливу завад і засобів радіоелектронної розвідки.

Дисертаційне дослідження виконано в межах держбюджетної науково-дослідної роботи «Розроблення методів підвищення захищеності передавання інформації в інформаційно-комунікаційних системах на основі інтегрованих сигнально-кодових перетворень» (державний реєстраційний номер 0126U002946). Основні результати, отримані Гавелем Сергієм Миколайовичем, використано під час виконання зазначеної науково-дослідної роботи та включено до відповідного науково-технічного звіту.

Отже, тематика дисертаційного дослідження узгоджується з науковими напрямами кафедри, відповідає освітньо-науковій програмі за спеціальністю 125 Кібербезпека та має безпосередній зв'язок із виконанням зазначеної науково-дослідної роботи.

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

Дисертаційна робота Гавеля Сергія Миколайовича має логічну та послідовну структуру, яка відповідає меті й поставленим завданням дослідження. Робота складається зі вступу, чотирьох розділів, загальних висновків, двох додатків та списку використаних джерел. Загальний обсяг дисертації становить 181 сторінку, з яких 136 сторінок припадає на основний текст.

У **вступі** обґрунтовано актуальність теми дисертаційного дослідження, визначено мету, об'єкт, предмет і завдання роботи, наведено методи дослідження, сформульовано наукову новизну та практичне значення отриманих результатів.

Також наведено відомості про апробацію результатів дослідження, публікації здобувача та структуру дисертації.

Перший розділ присвячено аналізу теоретичних і методологічних засад підвищення прихованості передавання інформації. Розглянуто поняття енергетичної та структурної прихованості, особливості застосування таймерних сигнальних конструкцій, характеристики псевдовипадкових послідовностей та основні принципи розширення спектра сигналів. Проведений аналіз дозволив визначити основні проблемні питання та сформулювати напрям подальших досліджень.

Другий розділ присвячено дослідженню методів формування та оцінювання таймерних сигнальних конструкцій. Розглянуто особливості їх побудови, визначено показники структурної прихованості та досліджено вплив параметрів таймерних сигналів на їх характеристики. Окрему увагу приділено оцінюванню структурної прихованості таймерних сигналів та визначенню кількості можливих сигнальних реалізацій.

Третій розділ присвячено розробленню та дослідженню методів прямого розширення спектра таймерних сигнальних конструкцій. Обґрунтовано вибір псевдовипадкових послідовностей для розширення спектра позиційних і таймерних сигналів, проаналізовано їх кореляційні та структурні властивості. Досліджено вплив бази сигналу на його прихованість і завадостійкість, а також визначено особливості формування широкосмугових шумоподібних таймерних сигналів.

Четвертий розділ присвячено оцінюванню структурної прихованості широкосмугових таймерних сигналів та дослідженню впливу основних параметрів їх формування на рівень прихованості. Запропоновано інтегральний показник структурної прихованості, який враховує внесок таймерної сигнальної конструкції, псевдовипадкової послідовності та системи модуляції. Проведено порівняльне оцінювання сигналів із використанням послідовностей Уолша та псевдовипадкових послідовностей, сформованих на основі хаотичних коливань. Визначено залежності рівня структурної прихованості від параметрів таймерних сигнальних конструкцій і бази розширення спектра.

У загальних висновках систематизовано основні результати дисертаційного дослідження та сформульовано висновки відповідно до поставлених завдань. Наведені результати підтверджують досягнення мети роботи та розв'язання визначеного науково-прикладного завдання.

У додатках наведено матеріали, що доповнюють основний зміст дисертації та підтверджують результати проведених досліджень.

Зміст дисертації характеризується послідовністю викладення матеріалу, взаємозв'язком між теоретичними положеннями, розробленими методами та результатами їх дослідження. Основні положення роботи підтверджено математичними залежностями, розрахунками, таблицями та графічними матеріалами. Отримані результати узгоджуються з поставленими завданнями та положеннями наукової новизни.

Оформлення дисертаційної роботи загалом відповідає встановленим вимогам до дисертацій на здобуття ступеня доктора філософії. Матеріал викладено в науковому стилі, використано відповідну термінологію, формули, таблиці, рисунки та бібліографічні посилання. Структура та обсяг роботи

забезпечують достатнє розкриття змісту проведеного дослідження.

Загалом дисертаційна робота є завершеним самостійним науковим дослідженням, у якому послідовно розглянуто теоретичні засади, розроблено відповідні методи та проведено їх дослідження. Зміст роботи відповідає її темі, меті та поставленим завданням, а отримані результати мають наукову новизну та практичну цінність.

За результатами досліджень за темою дисертаційної роботи опубліковано 14 наукових праць, з яких 6 наукових статей у періодичних виданнях України, включених до Переліку наукових фахових видань України, та 8 тез доповідей у матеріалах наукових конференцій.

Серед опублікованих праць одна стаття опублікована у виданні, що індексується наукометричною базою даних Scopus. Крім того, одна теза доповіді також опублікована у виданні, що індексується в Scopus. Загалом кількість наукових праць здобувача у виданнях, що індексуються наукометричною базою даних Scopus, становить 2, з яких одна стаття та одна теза доповіді.

Одна з наукових праць здобувача включена до складу монографії. Опубліковані наукові праці відображають основні результати дисертаційного дослідження, зокрема результати розроблення та дослідження методів прямого розширення спектра таймерних сигнальних конструкцій, формування широкосмугових шумоподібних таймерних сигналів та оцінювання їх структурної прихованості.

Отже, результати дисертаційного дослідження достатньою мірою представлені в наукових публікаціях, що забезпечує їх апробацію та підтверджує повноту викладення основних положень дисертації у наукових виданнях.

Структура дисертації є логічною та послідовною, а її зміст, мета і завдання відповідають обраній темі та забезпечують розв'язання визначених у роботі науково-прикладних задач. Виклад матеріалу є послідовним, аргументованим і грамотним. Дисертація Гавеля Сергія Миколайовича є цілісним і завершеним науковим дослідженням. Роботу оформлено відповідно до вимог наказу Міністерства освіти і науки України від 12.01.2017 № 40 «Про затвердження вимог до оформлення дисертації» (зі змінами, внесеними згідно з наказом Міністерства освіти і науки України від 31.05.2019 № 759).

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

Обґрунтованість наукових положень, висновків і рекомендацій, сформульованих у дисертаційній роботі Гавеля Сергія Миколайовича, забезпечується коректною постановкою мети та завдань дослідження, використанням відповідного математичного апарату, застосуванням сучасних методів дослідження та проведенням розрахункових і порівняльних досліджень.

Основні наукові положення дисертації ґрунтуються на аналізі властивостей таймерних сигналів, методів ПРС, ПВП та хаотичних послідовностей, а також показників енергетичної та структурної прихованості. Обґрунтування запропонованих методів здійснюється шляхом математичного опису процесів формування сигналів, визначення їх параметрів та дослідження впливу окремих характеристик на рівень прихованості й завадостійкість передавання інформації.

Достовірність отриманих результатів підтверджується результатами розрахунків, моделювання та порівняльного аналізу характеристик таймерних і позиційних сигнальних конструкцій. Зокрема, досліджено залежність структурної прихованості від параметрів ТСК, бази розширення спектра, типу ПВП та виду модуляції. Проведені дослідження дозволили встановити переваги запропонованих підходів щодо підвищення прихованості передавання інформації.

Висновки дисертації відповідають отриманим результатам дослідження, сформульовані за окремими науковими положеннями та завданнями роботи і не виходять за межі проведеного дослідження. Практичні рекомендації щодо використання розроблених методів під час формування ширококутових шумоподібних таймерних сигналів є логічним наслідком отриманих теоретичних і розрахункових результатів.

Загалом ступінь обґрунтованості наукових положень, висновків і рекомендацій дисертаційної роботи можна оцінити як достатній, а отримані результати – як достовірні та належним чином підтверджені проведеними дослідженнями.

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

У дисертаційній роботі Гавеля Сергія Миколайовича отримано наукові результати, спрямовані на підвищення прихованості передавання інформації на основі прямого розширення спектра таймерних сигнальних конструкцій.

Основним науковим результатом є розроблення інтегрованого методу формування ширококутових шумоподібних таймерних сигналів із використанням ПВП, що забезпечує керування спектральними та кореляційними характеристиками сигналів і підвищує їх структурну прихованість.

Удосконалено методику оцінювання структурної прихованості ширококутових таймерних сигналів, яка враховує сукупний вплив ТСК, ПВП та системи модуляції.

Вперше запропоновано поняття інтерпретованої бази ширококутового таймерного сигналу, що враховує особливості розширення спектра всієї таймерної комбінації та може використовуватися для оцінювання її прихованості й завадостійкості.

Подальшого розвитку набули методи розширення спектра таймерних сигналів на основі системи залишкових класів, послідовностей Уолша та хаотичних ПВП, що дозволяє поєднати властивості завадостійкості та структурної прихованості.

Отримані результати підтверджено математичними розрахунками, моделюванням та порівняльним аналізом характеристик запропонованих сигнальних конструкцій. У цілому наукова новизна результатів полягає у розвитку методів підвищення прихованості передавання інформації шляхом поєднання непозиційної часової структури таймерних сигналів із методами прямого розширення спектра.

6. Значення роботи для науки, практики та суспільства

Наукове значення дисертаційної роботи полягає у розвитку теоретичних і методичних положень щодо підвищення прихованості передавання інформації на основі таймерних сигнальних конструкцій та прямого розширення спектра. Запропоновані методи й показники розширюють можливості дослідження структурної прихованості та можуть бути використані для подальшого розвитку захищених методів передавання інформації.

Практичне значення роботи полягає у можливості використання розроблених методів формування та розширення спектра широкосмугових шумоподібних таймерних сигналів під час проєктування і модернізації захищених ІКС та радіотехнічних систем, зокрема тих, що функціонують в умовах радіоелектронного протиборства та кіберзагроз. Результати роботи також впроваджено в навчальний процес кафедри кібербезпеки та технічного захисту інформації Державного університету інтелектуальних технологій і зв'язку.

Суспільне значення роботи визначається можливістю підвищення захищеності інформаційного обміну в сучасних інформаційно-комунікаційних системах, що сприяє забезпеченню конфіденційності та стійкості передавання інформації в умовах зростання рівня кіберзагроз і радіоелектронного впливу.

Практичне значення отриманих результатів дисертаційної роботи для захисту інформації полягає у розробленні методів формування та прямого розширення спектра широкосмугових шумоподібних таймерних сигналів, спрямованих на підвищення енергетичної та структурної прихованості передавання інформації.

Запропоновані методи формування таймерних сигналів із використанням послідовностей Уолша та хаотичних ПВП дають змогу керувати спектральними й кореляційними характеристиками сигналів та можуть бути використані під час створення і модернізації захищених ІКС та радіотехнічних систем.

Практичну цінність має також метод визначення інтерпретованої бази широкосмугового таймерного сигналу, який може застосовуватися для обґрунтованого вибору параметрів сигналів з урахуванням вимог до прихованості, завадостійкості та використання частотного ресурсу.

Розроблені методи можуть бути використані для побудови захищених каналів передавання інформації, що функціонують в умовах РЕП та кіберзагроз. Одержані результати також впроваджено в навчальний процес кафедри кібербезпеки та технічного захисту інформації Державного університету інтелектуальних технологій і зв'язку.

7. Оформлення дисертації та дотримання вимог академічної доброчесності

Дисертаційна робота Гавеля Сергія Миколайовича оформлена відповідно до встановлених вимог, виконана в науковому стилі із використанням відповідної наукової термінології. Структура, зміст та оформлення роботи відповідають вимогам до дисертацій на здобуття ступеня доктора філософії за спеціальністю 125 Кібербезпека.

Аналіз змісту дисертації та наукових публікацій здобувача свідчить про дотримання принципів академічної доброчесності. У роботі наведено посилання на використані джерела та результати досліджень інших авторів. Основні наукові результати, представлені в дисертації, отримані здобувачем самостійно.

Ознак академічного плагіату, некоректних запозичень або інших порушень академічної доброчесності під час аналізу дисертаційної роботи не виявлено. Загалом оформлення дисертації та представлення отриманих результатів відповідають установленим вимогам.

8. Дискусійні положення та зауваження до змісту дисертації

Разом із позитивною оцінкою дисертаційної роботи вважаю за доцільне висловити декілька зауважень і міркувань дискусійного характеру, які не знижують загальної наукової цінності отриманих результатів, але можуть бути враховані в подальших дослідженнях.

1. У першому розділі окремі теоретичні положення викладено досить детально, що дещо збільшує його обсяг. Доцільним могло б бути більш стисле представлення загальних відомостей з акцентуванням уваги на положеннях, безпосередньо пов'язаних із предметом дисертаційного дослідження.

2. У підрозділі 2.1 підвищення ентропії сигналу безпосередньо пов'язується зі зростанням рівня структурної прихованості, однак кількісний зв'язок між цими показниками не розкрито. Доцільним було б додатково обґрунтувати умови, за яких зростання ентропії дійсно забезпечує підвищення структурної прихованості сигнальних конструкцій.

3. У пункті 2.4 недостатньо розкрито вплив параметра s на достовірність передавання з урахуванням відношення сигнал/шум, оскільки його збільшення, з одного боку, підвищує структурну прихованість, а з іншого – може знижувати достовірність передавання.

4. У пункті 3.4 оцінювання хаотичних ПВП переважно ґрунтується на автокореляційному аналізі. Доцільно було б доповнити оцінювання іншими статистичними критеріями.

5. У пункті 4.5 оцінювання кореляційних властивостей виконано для трьох реалізацій ТСК та обмеженого набору ПВП Уолша. Доцільно було б розширити діапазон досліджуваних параметрів для більш повного обґрунтування отриманих закономірностей.

Загальні висновки щодо дисертаційної роботи

Дисертаційна робота Гавеля Сергія Миколайовича присвячена актуальному науково-прикладному завданню підвищення прихованості передавання інформації шляхом поєднання таймерних сигнальних конструкцій, прямого розширення спектра та псевдовипадкових послідовностей.

У роботі обґрунтовано доцільність використання таймерних сигнальних конструкцій для підвищення структурної прихованості, досліджено їх інформаційні, кореляційні та ентропійні характеристики, а також встановлено вплив параметрів ТСК, бази розширення спектра та виду модуляції на рівень прихованості й достовірність передавання інформації.

Отримані результати підтверджують перспективність застосування

широкосмугових таймерних сигналів для підвищення захищеності інформації в умовах радіоелектронного протиборства. Сукупність результатів роботи свідчить про досягнення поставленої мети та розв'язання визначених науково-прикладних завдань.

Висловлені зауваження мають дискусійний характер і не знижують загальної позитивної оцінки дисертаційної роботи. Дисертація є цілісним і завершеним науковим дослідженням, результати якого мають наукову новизну та практичне значення.

Офіційний рецензент
старший викладач кафедри інженерії
програмного забезпечення
Державного університету
інтелектуальних технологій і зв'язку
кандидат технічних наук

Юрій БАБІЧ