

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

ВІДГУК

офіційного опонента головного наукового співробітника Державного науково-дослідного інституту випробування і сертифікації озброєння та військової техніки, доктора технічних наук, професора, Рудницького Володимира Миколайовича на дисертаційну роботу Гавеля Сергія Миколайовича на тему «Підвищення прихованості передавання інформації на основі прямого розширення спектра таймерних сигнальних конструкцій», яка подана на здобуття наукового ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека.

Актуальність роботи

В умовах стрімкого розвитку інформаційно-комунікаційних технологій (ІКС), цифровізації суспільства та зростання кількості кіберзагроз особливої актуальності набуває проблема забезпечення захисту передаваної інформації каналами зв'язку. Сучасні ІКС функціонують в умовах постійного впливу засобів радіоелектронної розвідки (РЕР), навмисних завад, кібератак і несанкціонованого доступу (НСД), що висуває підвищені вимоги до забезпечення конфіденційності, цілісності та доступності інформаційних ресурсів.

Одним із перспективних напрямів підвищення рівня захисту інформації є використання методів фізичного рівня, які забезпечують прихованість передавання сигналів. Особливе місце серед них займають методи прямого розширення спектра (ПРС), що дозволяють зменшити спектральну щільність потужності сигналу, підвищити його завадостійкість та ускладнити виявлення засобами РЕР. Разом із тим відомі методи розширення спектра переважно орієнтовані на використання позиційних сигналів і не повною мірою враховують можливості непозиційних таймерних сигнальних конструкцій (ТСК) щодо забезпечення структурної та енергетичної прихованості.

У зв'язку з цим актуальним є розроблення нових методів захисту інформації, заснованих на інтеграції ТСК із методами ПРС, використанні псевдовипадкових та хаотичних послідовностей, а також удосконаленні методів оцінювання структурної прихованості широкосмугових сигналів. Запропонований у дисертаційній роботі комплексний підхід дозволяє підвищити ефективність захисту інформації від виявлення, перехоплення та аналізу в умовах сучасних кіберзагроз і радіоелектронного протистояння.

Отже, дисертаційна робота Гавеля Сергія Миколайовича, присвячена розробленню методів підвищення захищеності передавання інформації в ІКС на основі інтегрованих сигнально-кодових перетворень, є своєчасною, актуальною та спрямованою на вирішення важливого науково-прикладного завдання у галузі кібербезпеки та захисту інформації.

Зв'язок роботи з науковими програмами, планами, темами

Тема дисертаційної роботи безпосередньо пов'язана з пріоритетними напрямами розвитку науки і техніки України у сфері інформаційних технологій, кібербезпеки та захисту інформації, а також відповідає сучасним потребам забезпечення інформаційної безпеки держави в умовах зростання кіберзагроз і застосування засобів радіоелектронного протиборства.

Дисертаційне дослідження виконано відповідно до планів науково-дослідної роботи кафедри кібербезпеки та технічного захисту інформації Державного університету інтелектуальних технологій і зв'язку в межах науково-дослідної роботи «Розроблення методів підвищення захищеності передавання інформації в інформаційно-комунікаційних системах на основі інтегрованих сигнально-кодових перетворень» (державний реєстраційний номер 0126U002946), у якій здобувач брав безпосередню участь.

Результати дисертаційної роботи спрямовані на розроблення методів формування широкосмугових таймерних сигналів, інтегрованих методів прямого розширення спектра та оцінювання структурної й енергетичної прихованості сигнально-кодових конструкцій, що відповідає сучасним напрямкам розвитку інформаційно-комунікаційних технологій, кібербезпеки та технічного захисту інформації.

Отже, тема дисертаційної роботи Гавеля Сергія Миколайовича є актуальною, відповідає пріоритетним напрямкам наукових досліджень у галузі знань 12 «Інформаційні технології» (спеціальність 125 Кібербезпека) та безпосередньо пов'язана з виконанням державної науково-дослідної роботи.

Наукова новизна одержаних результатів

На підставі аналізу змісту дисертаційної роботи та опублікованих наукових праць Гавеля Сергія Миколайовича встановлено, що автором вирішено актуальне науково-прикладне завдання, яке полягає у розробленні методів підвищення захищеності передавання інформації в інформаційно-комунікаційних системах шляхом інтеграції таймерних сигнальних конструкцій із методами прямого розширення спектра. Запропоновані наукові рішення спрямовані на підвищення структурної та енергетичної прихованості сигналів, забезпечення стійкості до виявлення, перехоплення й аналізу в умовах кіберзагроз та радіоелектронного протиборства.

Наукова новизна дисертаційної роботи визначається такими основними положеннями:

1. Вперше розроблено інтегрований метод захисту інформації на основі формування широкосмугових шумоподібних таймерних сигналів із використанням псевдовипадкових послідовностей, який, на відміну від існуючих методів прямого розширення спектра, забезпечує підвищення структурної та енергетичної прихованості передавання інформації за рахунок керування спектральними та кореляційними властивостями сигнально-кодових конструкцій.

2. Вперше запропоновано інтегровану методику оцінювання структурної прихованості широкосмугових таймерних сигналів, яка враховує сумарний внесок структурної прихованості таймерних сигнальних конструкцій, псевдовипадкових послідовностей розширення спектра та використаної

системи модуляції, що дозволяє комплексно оцінювати внесок кожного із зазначених складників у забезпечення захисту інформації.

3. Вперше введено поняття інтерпретованої бази широкосмугового таймерного сигналу, яке, на відміну від класичного визначення бази позиційного сигналу, враховує особливості розширення спектра всієї таймерної сигнальної конструкції та створює наукове підґрунтя для оцінювання енергетичної прихованості непозиційних широкосмугових сигналів.

4. Набув подальшого розвитку метод розширення спектра таймерних сигналів, сформованих на основі системи залишкових класів, який поєднує функції завадостійкого кодування та структурної прихованості без використання додаткових перевірючих елементів, що сприяє підвищенню ефективності захисту інформації в інформаційно-комунікаційних системах.

5. Удосконалено метод розширення спектра таймерних сигналів із використанням послідовностей Уолша та хаотичних псевдовипадкових послідовностей, що забезпечує динамічну зміну кореляційних властивостей широкосмугових сигналів, підвищує рівень їх структурної прихованості та ускладнює їх виявлення й аналіз засобами радіоелектронної розвідки.

Констатую, що наведені положення наукової новизни є достатньо обґрунтованими, підтверджені результатами теоретичних досліджень, математичного моделювання та експериментальної перевірки, відповідають змісту дисертаційної роботи й свідчать про особистий внесок автора у розвиток методів захисту інформації та кібербезпеки інформаційно-комунікаційних систем.

Практична цінність та впровадження отриманих результатів

Практична цінність дисертаційної роботи Гавеля Сергія Миколайовича полягає у розробленні методів формування широкосмугових шумоподібних таймерних сигналів, методів прямого розширення спектра та методики оцінювання структурної прихованості, які можуть бути використані під час створення й модернізації захищених інформаційно-комунікаційних систем, систем спеціального призначення та засобів технічного захисту інформації.

Запропоновані в дисертації науково-технічні рішення дозволяють підвищити структурну та енергетичну прихованість передавання інформації, забезпечити ефективніше використання таймерних сигнальних конструкцій у системах із прямим розширенням спектра, а також удосконалити методи оцінювання рівня захищеності сигналів. Практичне значення мають також результати дослідження кореляційних властивостей широкосмугових таймерних сигналів, визначення інтерпретованої бази широкосмугового таймерного сигналу та використання різних типів псевдовипадкових послідовностей для реалізації єдиного методу розширення спектра.

Важливою перевагою роботи є те, що запропоновані методи підтверджені результатами математичного моделювання та експериментальних досліджень, а отримані кількісні оцінки структурної й енергетичної прихованості, кореляційних властивостей та завадостійкості свідчать про можливість їх практичного використання під час проєктування сучасних захищених інформаційно-комунікаційних систем.

Результати дисертаційної роботи впроваджено в освітній процес кафедри кібербезпеки та технічного захисту інформації Державного університету інтелектуальних технологій і зв'язку під час підготовки здобувачів вищої освіти за спеціальністю 125 Кібербезпека, що підтверджується відповідним актом впровадження.

Крім того, результати дисертаційного дослідження впроваджено у практичну діяльність ТОВ «КОБІ СС», де запропоновані методи використані під час виконання робіт із забезпечення захисту інформації та підвищення захищеності ІКС, що також підтверджується відповідним актом впровадження.

Отже, отримані результати мають вагоме практичне значення, характеризуються достатнім рівнем готовності до практичного застосування та можуть бути рекомендовані для використання під час розроблення перспективних інформаційно-комунікаційних систем із підвищеними вимогами до захисту інформації, прихованості передавання даних та забезпечення кібербезпеки.

Аналіз змісту, структури та обсягу роботи

Загальний обсяг дисертаційної роботи становить 181 сторінок, із яких основний текст викладено на 140 сторінках машинописного тексту. Робота складається зі вступу, чотирьох розділів, загальних висновків, списку використаних джерел та додатків. Дисертація містить рисунки, таблиці, формули та додатки, які доповнюють результати проведених досліджень і сприяють кращому сприйняттю викладеного матеріалу.

У вступі обґрунтовано актуальність теми дослідження, визначено мету, завдання, об'єкт і предмет дослідження, сформульовано наукову новизну та практичне значення одержаних результатів, наведено інформацію щодо їх апробації, публікацій, особистого внеску автора та впровадження результатів дисертаційної роботи.

У першому розділі надано аналіз сучасного стану проблеми забезпечення захисту інформації під час передавання в інформаційно-комунікаційних системах. Розглянуто сучасні методи підвищення захищеності інформації, зокрема методи розширення спектра, модуляції, завадостійкого кодування та криптографічного захисту. Особливу увагу приділено питанням структурної та енергетичної прихованості сигналів у контексті забезпечення кібербезпеки інформаційно-комунікаційних систем. За результатами проведеного аналізу сформульовано наукову проблему, визначено напрям досліджень та обґрунтовано необхідність розроблення нових методів прямого розширення спектра таймерних сигнальних конструкцій.

У другому розділі досліджено властивості таймерних сигнальних конструкцій як основи побудови захищених систем передавання інформації. Проведено аналіз інформаційних властивостей таймерних сигналів, досліджено вплив параметрів їх формування на структурну прихованість та завадостійкість, виконано оцінювання інформаційних характеристик із використанням положень теорії інформації. Значну увагу приділено використанню таймерного кодування для підвищення рівня захисту інформації від виявлення, аналізу та несанкціонованого доступу в умовах сучасних кіберзагроз.

У третьому розділі розроблено та досліджено метод прямого розширення спектра таймерних сигнальних конструкцій із використанням різних типів псевдовипадкових послідовностей. Проаналізовано особливості застосування М-послідовностей, кодів Голда, Касамі, Уолша та хаотичних псевдовипадкових послідовностей для формування широкосмугових шумоподібних сигналів. Досліджено вплив параметрів розширення спектра на енергетичну прихованість, кореляційні властивості, завадостійкість та ефективність захисту інформації в інформаційно-комунікаційних системах.

У четвертому розділі розроблено та досліджено метод прямого розширення спектра таймерних сигнальних конструкцій для підвищення прихованості передавання інформації. Запропоновано інтегрований метод формування широкосмугових шумоподібних таймерних сигналів, досліджено особливості їх кореляційного приймання, введено поняття інтерпретованої бази широкосмугового таймерного сигналу та розроблено інтегровану методику оцінювання структурної прихованості. Наведено результати математичного моделювання, які підтверджують ефективність запропонованих методів щодо підвищення структурної та енергетичної прихованості, завадостійкості й захищеності передавання інформації в умовах радіоелектронного протиборства та сучасних кіберзагроз.

У загальних висновках наведено основні результати дисертаційного дослідження, сформульовано наукові положення та практичні рекомендації, що випливають із виконаних досліджень.

У додатках подано акти впровадження результатів дисертаційної роботи, відомості про апробацію результатів дослідження, а також список наукових праць автора за темою дисертації.

Ознайомившись із змістом дисертаційної роботи можна зробити висновок, що робота виконана з дотриманням принципів академічної доброчесності. Результати наукових досліджень інших авторів супроводжуються посиланнями на їхні публікації і відокремлені від результатів здобувача. Наукові положення дисертації і висновки мають авторське обґрунтування. Ознак порушення академічної доброчесності не встановлено.

За результатами аналізу змісту дисертаційної роботи можна зробити висновок, що її структура є логічною та послідовною, матеріал викладено системно, а кожний наступний розділ ґрунтується на результатах попереднього. Робота відповідає вимогам, що висуваються до дисертацій на здобуття ступеня доктора філософії за спеціальністю 125 «Кібербезпека», а її зміст повністю узгоджується з поставленою метою та завданнями дослідження.

Мова та стиль викладання результатів

Дисертація Гавеля Сергія Миколайовича написана українською мовою. Стиль викладення матеріалу є науковим, логічним, послідовним та достатньо аргументованим. Основні положення, результати досліджень і висновки сформульовано чітко, із використанням сучасної термінології у галузі кібербезпеки, теорії сигналів та інформаційно-комунікаційних систем. Структура викладення матеріалу забезпечує цілісне сприйняття результатів дослідження та підтверджує належний рівень наукової підготовки автора.

Повнота викладу основних положень дисертації в опублікованих наукових працях

За темою дисертаційного дослідження здобувачем Гавелем Сергієм Миколайовичем опубліковано 14 наукових праць, серед яких:

- 6 статей у наукових фахових виданнях України, у тому числі 1 стаття у виданні, що індексується в міжнародній наукометричній базі Scopus;
- 8 публікацій, присвячених апробації результатів дослідження, серед яких 6 тез доповідей на міжнародних і всеукраїнських науково-практичних конференціях, 1 праця у виданні, що індексується в міжнародній наукометричній базі Scopus, та 1 наукову працю включено до колективної монографії.

Загалом кількість і характер наукових публікацій відповідають чинним вимогам Міністерства освіти і науки України щодо апробації та оприлюднення основних результатів дисертаційних досліджень на здобуття ступеня доктора філософії. Тематика опублікованих праць повністю відповідає предмету дисертаційного дослідження, а їх зміст відображає основні положення, наукову новизну та практичні результати, що виносяться на захист. Це дає підстави стверджувати, що результати дисертаційної роботи пройшли належну наукову апробацію та достатньою мірою висвітлені у відкритих наукових публікаціях.

Зауваження та дискусійні положення

1. У першому розділі на рис. 1.1 (с. 34) наведено узагальнену модель забезпечення захисту інформації від засобів радіоелектронної розвідки, у якій розглянуто енергетичну, структурну та інформаційну прихованість. Водночас доцільно було б коротко охарактеризувати й інші види прихованості, зокрема часову та просторову, а також обґрунтувати причини їх неврахування в межах проведеного дослідження. Це дозволило б повніше розкрити місце отриманих результатів у загальній теорії прихованості.

2. У першому розділі на рис. 1.2 (с. 41) наведено класифікацію методів забезпечення енергетичної прихованості сигналів у системах захищеного радіозв'язку. Разом із тим доцільно було б чіткіше визначити місце хаотичних сигнальних конструкцій у запропонованій класифікації та деталізувати їх взаємозв'язок із методами розширення спектра позиційних і таймерних сигналів. Зокрема, потребує уточнення, чи хаотичні генератори використовуються для формування псевдовипадкових послідовностей розширення спектра, чи безпосередньо як джерело несучих сигналів.

3. У підрозділі 2.5 запропоновано метод формування таймерних сигнальних конструкцій на основі системи залишкових класів та наведено приклад його реалізації для модулів $\{2, 3, 7\}$. Разом із тим доцільно було б детальніше обґрунтувати критерії вибору системи модулів та дослідити вплив різних їх комбінацій на кількість сформованих сигнальних конструкцій, структурну прихованість, часові параметри й складність синхронізації. Це дозволило б повніше оцінити можливості практичного застосування запропонованого методу.

4. У підрозділі 3.4 як базову модель генерації хаотичних псевдовипадкових послідовностей використано логістичне відображення. Разом із тим доцільно було б детальніше обґрунтувати вибір саме цього хаотичного

генератора та порівняти його характеристики з іншими відомими хаотичними відображеннями (наприклад, відображенням Тента, Чебишова або системою Лоренца) з позицій структурної прихованості, статистичних властивостей та складності практичної реалізації.

5. У підрозділі 4.1 обгрунтовано необхідність нової інтерпретації бази широкосмугових таймерних сигналів. Водночас доцільно було б більш детально показати, як запропонований підхід узгоджується з класичними характеристиками широкосмугових систем зв'язку та яким чином зміна трактування бази сигналу впливає на основні параметри системи передавання інформації.

6. У підрозділі 4.2 наведено метод формування широкосмугових таймерних сигналів на основі псевдовипадкових послідовностей. Водночас доцільно було б більш детально обгрунтувати критерії узгодження параметрів таймерної сигнальної конструкції та псевдовипадкової послідовності (співвідношення між m , s , та λ), оскільки саме від них залежить ефективність реалізації запропонованого способу розширення спектра.

7. У підрозділі 4.3 детально розглянуто процес кореляційного приймання широкосмугових таймерних сигналів та відновлення їх часової структури. Разом із тим доцільно було б більш детально проаналізувати вплив похибок синхронізації локальної псевдовипадкової послідовності та часових зсувів на точність визначення значущих моментів відновлення. Це дозволило б повніше оцінити практичну ефективність запропонованого методу в реальних умовах функціонування систем радіозв'язку.

8. 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 мають переважно уточнювальний характер та/або показують перспективу подальшого розвитку результатів досліджень автора у майбутньому.

Висновок

На підставі детального аналізу дисертації та наукових публікацій здобувача Гавеля Сергія Миколайовича, а також з урахуванням актуальності теми дослідження, наукової новизни, практичної значущості, обгрунтованості та достовірності отриманих результатів і сформульованих висновків вважаю, що дисертація на тему «Підвищення прихованості передавання інформації на основі прямого розширення спектра таймерних сигнальних конструкцій» є завершеним, самостійно виконаним науковим дослідженням, у якому вирішено актуальне науково-прикладне завдання підвищення прихованості передавання інформації в інформаційно-комунікаційних системах шляхом розроблення методів прямого розширення спектра таймерних сигнальних конструкцій, удосконалення способів формування та приймання широкосмугових таймерних сигналів, а також розвитку підходів до забезпечення енергетичної і структурної прихованості в умовах радіоелектронної протидії.

Окремі зауваження, висловлені під час рецензування, мають переважно

рекомендаційний характер, стосуються поглиблення теоретичного обґрунтування окремих положень, деталізації результатів досліджень та не впливають на загальну наукову цінність, достовірність отриманих результатів і практичну значущість дисертаційної роботи.

Вважаю, що дисертація Гавеля Сергія Миколайовича відповідає вимогам пунктів 5–8 Постанови Кабінету Міністрів України № 44 від 12 січня 2022 року «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 вимогам щодо оформлення дисертацій.

Отже, вважаю, що Гавель Сергій Миколайович заслуговує на присудження наукового ступеня доктора філософії (PhD) за спеціальністю 125 Кібербезпека.

Офіційний опонент

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

 Володимир РУДНИЦЬКИЙ

Підпис Рудницького В.М. 
Вчений секретар науково-технічної ради,
кандидат технічних наук

 Олександр БУРСАЛА

17

08

2025