

Голові разової спеціалізованої вченої
ради Державного університету
інтелектуальних технологій і зв'язку
МОН України, доктору технічних наук,
доценту кафедри інформаційних та
комп'ютерних систем
Віктору ТІХОНОВУ,
вул. Кузнечна, 1, м. Одеса, 66000

ВІДГУК

офіційного опонента, доктора технічних наук (спеціальність 05.13.21 – системи захисту інформації), професора, професора кафедри комп'ютерних інформаційних технологій, проректора з наукових досліджень та трансферу технологій Національного університету «Київський авіаційний інститут» Гнатюка Сергія Олександровича на дисертацію 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 теми дисертації

Сучасний розвиток інформаційно-комунікаційних систем супроводжується постійним зростанням вимог до забезпечення захищеного передавання інформації в умовах активної радіоелектронної протидії. Особливої ваги набуває проблема підвищення прихованості сигналів, оскільки сучасні засоби радіоелектронної розвідки здатні ефективно виявляти, аналізувати та класифікувати сигнали навіть за умов застосування методів розширення спектра. Тому актуальним науковим завданням є розроблення нових методів формування широкосмугових сигналів, які поєднували б високу завадостійкість, енергетичну та структурну прихованість.

Перспективним напрямом вирішення цієї задачі є використання таймерних сигнальних конструкцій у поєднанні з методами прямого розширення спектра. Використання непозиційного принципу кодування дозволяє суттєво ускладнити часову структуру сигналу, а застосування псевдовипадкових послідовностей

забезпечує зменшення спектральної щільності потужності та підвищення енергетичної прихованості. Водночас питання інтеграції таймерного кодування з технологіями прямого розширення спектра, інтерпретації бази широкосмугових таймерних сигналів, а також розроблення методів їх формування та кореляційного приймання залишаються недостатньо дослідженими.

З огляду на це тема дисертації Гавеля Сергія Миколайовича, присвячена підвищенню прихованості передавання інформації на основі прямого розширення спектра таймерних сигнальних конструкцій є актуальною, має важливе наукове та практичне значення і спрямована на вирішення актуальної науково-прикладної задачі у сфері кібербезпеки та захисту інформації.

Зв'язок роботи з науковими програмами, планами, темами

Дисертаційна робота виконана відповідно до основних положень Закону України «Про основні засади забезпечення кібербезпеки України», Закону України «Про захист інформації в інформаційно-комунікаційних системах» та Стратегії кібербезпеки України, що визначають пріоритетні напрями розвитку систем захисту інформації та забезпечення кібербезпеки держави.

Тематика дослідження узгоджується з основними науковими напрямами фундаментальних досліджень Національної академії наук України на 2024–2028 роки, затвердженими постановою Президії НАН України від 10.01.2024 № 8, зокрема з напрямами 1.2.9 та 1.2.9.5 – теорія та комп'ютерні технології інформаційної безпеки. Крім того, дисертаційна робота відповідає змісту освітньо-наукової програми підготовки докторів філософії зі спеціальності 125 Кібербезпека Державного університету інтелектуальних технологій і зв'язку та спрямована на розвиток теоретичних і прикладних засад підвищення захищеності передавання інформації в інформаційно-комунікаційних системах.

Практичне значення отриманих результатів підтверджується їх використанням під час виконання держбюджетної науково-дослідної роботи «Розроблення методів підвищення захищеності передавання інформації в інформаційно-комунікаційних системах на основі інтегрованих сигнально-кодкових перетворень» (державний реєстраційний номер 0126U002946), до звіту за якою включено результати дисертаційного дослідження.

Дисертаційна робота Гавеля С. М. має безпосередній зв'язок із державними пріоритетами у сфері кібербезпеки та виконується в межах актуальних наукових програм і тематик, що підтверджує її наукову та практичну значущість.

Наукова новизна одержаних результатів

Наукова новизна дисертаційної роботи полягає у розробленні нових та вдосконаленні існуючих методів підвищення прихованості передавання інформації в інформаційно-комунікаційних системах на основі інтеграції таймерного кодування, методів прямого розширення спектра та псевдовипадкових послідовностей.

Найбільш вагомими науковими результатами дисертаційного дослідження є такі:

- вперше розроблено інтегрований метод захисту інформації, що поєднує таймерні сигнальні конструкції, широкосмугові шумоподібні сигнали та псевдовипадкові послідовності. На відміну від відомих методів прямого розширення спектра, запропонований метод забезпечує формування сигналів із керованими кореляційними та спектральними властивостями, що сприяє підвищенню прихованості передавання інформації та стійкості до навмисних завад;

- вперше запропоновано поняття інтерпретованої бази широкосмугового таймерного сигналу, яке, на відміну від класичного визначення бази сигналу, враховує розширення спектра на інтервалі формування всієї таймерної сигнальної конструкції. Це створює теоретичне підґрунтя для оцінювання характеристик широкосмугових таймерних сигналів та вибору їх параметрів;

- удосконалено методику оцінювання структурної прихованості широкосмугових таймерних сигналів, яка, на відміну від існуючих підходів, комплексно враховує внесок таймерних сигнально-кодових конструкцій, псевдовипадкових послідовностей і способу модуляції, що дозволяє більш повно оцінювати рівень захищеності інформації;

- удосконалено метод розширення спектра таймерних сигналів із використанням послідовностей Уолша та псевдовипадкових послідовностей, сформованих на основі хаотичних процесів, що забезпечує динамічну зміну кореляційних властивостей широкосмугових сигналів та підвищує рівень їх структурної прихованості порівняно з класичними методами DSSS;

- набув подальшого розвитку метод формування та розширення спектра таймерних сигналів, сформованих на основі системи залишкових класів, який забезпечує поєднання функцій структурної прихованості та завадостійкого кодування без використання додаткових перевірочних елементів.

Наведені результати дослідження характеризуються достатнім рівнем наукової новизни, є логічно взаємопов'язаними та становлять вагомий внесок у розвиток методів захисту інформації в інформаційно-комунікаційних системах за рахунок підвищення прихованості передавання даних.

Практична цінність та впровадження отриманих результатів

Практична цінність дисертаційної роботи Гавеля С. М. мають важливе прикладне значення і можуть бути використані під час проєктування та модернізації захищених інформаційно-комунікаційних систем, які функціонують в умовах радіоелектронного протидіювання та кіберзагроз.

Практичне значення роботи визначається насамперед розробленням інтегрованого методу формування широкосмугових шумоподібних таймерних сигналів із використанням псевдовипадкових послідовностей, який забезпечує керування спектральними та кореляційними характеристиками сигналів, підвищуючи рівень їх енергетичної та структурної прихованості.

Заслужує на увагу, запропонований автором метод визначення інтерпретованої бази широкосмугового таймерного сигналу, який створює можливість обґрунтованого вибору параметрів сигналів під час проєктування систем із прямим розширенням спектра залежно від вимог щодо прихованості, завадостійкості та ефективного використання частотного ресурсу.

Практичний інтерес становить метод розширення спектра таймерних сигналів, сформованих на основі системи залишкових класів, який поєднує функції завадостійкого кодування та структурної прихованості без використання додаткових перевірочних елементів, забезпечуючи збільшення кількості допустимих сигнальних комбінацій порівняно з класичними позиційними кодами, а також розроблена інтегрована методика оцінювання структурної прихованості широкосмугових таймерних сигналів, яка дозволяє комплексно оцінювати рівень прихованості з урахуванням властивостей таймерних сигнальних конструкцій, псевдовипадкових послідовностей та використаного способу модуляції.

Практична цінність роботи підтверджується результатами моделювання, які демонструють підвищення структурної прихованості та ефективності використання сигнального простору, а також можливість застосування запропонованих методів під час створення захищених каналів зв'язку та інформаційно-комунікаційних систем.

Достовірність і практична значущість отриманих результатів підтверджуються їх впровадженням у навчальний процес кафедри кібербезпеки та технічного захисту інформації Державного університету інтелектуальних технологій і зв'язку, а також використанням у діяльності ТОВ «КОБІ СС», що підтверджено відповідними актами впровадження.

Загалом практична цінність дисертаційної роботи не викликає сумнівів, а отримані результати можуть бути використані під час розроблення перспективних систем захищеного радіозв'язку та інформаційно-комунікаційних систем, орієнтованих на забезпечення високого рівня прихованості передавання інформації в умовах радіоелектронної протидії.

Аналіз змісту, структури та обсягу роботи

Дисертаційна робота Гавеля С. М. складається зі вступу, чотирьох розділів, висновків, списку використаних джерел і додатків. Структура дисертації є логічною та послідовною, а виклад матеріалу забезпечує повне розкриття поставленої мети та завдань дослідження. Загальний обсяг роботи становить 181 сторінок, з яких 136 сторінок — основний текст.

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** проведено аналіз сучасного стану проблеми захисту інформації в інформаційно-комунікаційних системах, що функціонують в умовах радіоелектронного протиборства. Розглянуто особливості застосування таймерних сигнальних конструкцій, методів прямого розширення спектра, псевдовипадкових послідовностей та сучасних підходів до забезпечення енергетичної і структурної прихованості передавання інформації. На основі проведеного аналізу сформульовано мету та основні завдання дисертаційного дослідження.

У **другому розділі** досліджено методи підвищення захищеності таймерних сигнальних конструкцій. Запропоновано метод захисту інформації на основі системи залишкових класів, виконано порівняльний аналіз із класичними завадостійкими кодами, а також обґрунтовано можливість підвищення

структурної прихованості сигнально-кодових конструкцій за рахунок використання непозиційного принципу кодування.

У **третьому розділі** розроблено методи підвищення прихованості таймерних сигнальних конструкцій із використанням послідовностей Уолша та псевдовипадкових послідовностей, сформованих на основі генераторів хаосу. Досліджено кореляційні та статистичні властивості сформованих послідовностей, а також обґрунтовано можливість їх використання для формування шумоподібних сигналів із покращеними характеристиками прихованості.

У **четвертому розділі** запропоновано метод формування широкосмугових таймерних сигналів на основі прямого розширення спектра, введено поняття інтерпретованої бази широкосмугового таймерного сигналу, розроблено метод кореляційного приймання та відновлення структури таймерних сигнальних конструкцій, а також інтегровану методику оцінювання їх структурної прихованості. Наведено результати моделювання, які підтверджують ефективність запропонованих методів.

У **висновках** наведено основні результати дисертаційного дослідження, що відповідають поставленим завданням та підтверджують досягнення визначеної мети роботи.

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

На підставі аналізу дисертаційної роботи можна зробити висновок, що вона виконана з дотриманням принципів академічної доброчесності. Ознак текстових запозичень без належних посилань на використані джерела не виявлено.

Загалом дисертація Гавеля Сергія Миколайовича є завершеним, логічно побудованим, змістовним і цілісним науковим дослідженням, у якому послідовно вирішено поставлені наукові завдання та повною мірою досягнуто мету дослідження.

Мова та стиль викладання результатів

Дисертація Гавеля Сергія Миколайовича 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 Гавель Сергій Миколайович опублікував 14 наукових праць, серед яких 6 статей у наукових фахових виданнях України (категорія Б), у тому числі одна стаття у виданні, що індексується в наукометричній базі даних Scopus; 8 тез доповідей у матеріалах наукових конференцій, у тому числі одні тези доповіді, опубліковані у виданні, що індексується в наукометричній базі даних Scopus та одна наукова праця опублікована у складі монографії.

Кількість і тип друкованих праць відповідають чинним вимогам Міністерства освіти і науки України щодо апробації та опублікування основних результатів дисертації на здобуття ступеня доктора філософії. Зміст опублікованих наукових праць свідчить про те, що основні наукові результати дисертаційного дослідження, які виносяться на захист, повною мірою висвітлено в публікаціях автора.

Зуваження та дискусійні положення

З огляду на високу теоретичну та практичну значущість, безперечну наукову новизну і загалом позитивне враження від змісту дисертаційного дослідження варто зупинитись на деяких дискусійних питаннях, а саме:

1. У підрозділі 1.2 наведено узагальнену модель забезпечення прихованості передавання інформації та розглянуто енергетичну, структурну й інформаційну прихованість. Водночас доцільно було б більш чітко обґрунтувати взаємозв'язок між цими складовими та показати, яким чином їх комплексне використання впливає на загальний рівень захищеності інформаційно-комунікаційної системи.

2. У підрозділі 1.3 доцільно було б більш чітко показати принципові відмінності між класичним прямим розширенням спектра позиційних сигналів та розширенням спектра таймерних сигнальних конструкцій. Такий порівняльний аналіз дозволив би краще обґрунтувати необхідність розроблення запропонованого методу формування широкосмугових таймерних сигналів.

3. У підрозділі 1.6 детально проаналізовано переваги та недоліки класичного методу прямого розширення спектра на основі псевдовипадкових послідовностей. Водночас доцільно було б більш чітко показати, які саме обмеження цього методу при використанні позиційних сигналів зумовлюють необхідність переходу до таймерних сигнальних конструкцій. Таке порівняння

дозволило б більш аргументовано обґрунтувати переваги запропонованого в дисертації методу інтеграції ПРС-ПВП із таймерним кодуванням.

4. У підрозділі 2.1 доцільно було б більш детально обґрунтувати взаємозв'язок між інформаційними характеристиками сигналів (кількістю інформації та ентропією), рівнем структурної прихованості та ефективністю захисту інформації в інформаційно-комунікаційних системах. Це дозволило б повніше розкрити практичне значення наведених теоретичних положень для вирішення основної задачі дисертаційного дослідження.

5. У підрозділі 2.2 основну увагу приділено класичному ентропійному оцінюванню сигнальних конструкцій. Водночас доцільно було б окремо обґрунтувати, чи є ентропія достатнім критерієм оцінювання структурної прихованості таймерних сигнальних конструкцій, або ж її необхідно використовувати спільно з іншими показниками, що характеризують часову та кореляційну структуру сигналів.

6. У підрозділі 3.4 доцільно було б доповнити результати автокореляційного аналізу порівнянням із класичними псевдовипадковими послідовностями (*m*-послідовностями, кодами Голда), що дозволило б наочно підтвердити переваги запропонованого методу формування хаотичних ПВП щодо забезпечення структурної прихованості.

7. У підрозділі 3.5 наведено результати дослідження впливу бази сигналу на характеристики широкосмугових таймерних сигналів. Водночас роботу можна було б посилити шляхом формування узагальнених рекомендацій щодо вибору бази сигналу залежно від вимог до рівня структурної прихованості, завадостійкості та допустимих витрат частотного ресурсу.

8. У підрозділі 4.3 доцільно було б більш чітко показати, що кореляційний прийом широкосмугових таймерних сигналів виконує не лише функцію відновлення часової структури сигналу, але й є додатковим рівнем захисту інформації, оскільки без знання параметрів псевдовипадкової послідовності, правил формування таймерної сигнальної конструкції та синхронізації сигнал практично неможливо коректно відновити.

Проте, зазначені зауваження не впливають на загальну позитивну оцінку дисертаційної роботи Гавеля Сергія Миколайовича та не знижують її науково-практичну цінність. Висловлені зауваження мають переважно рекомендаційний характер і можуть бути враховані автором у подальших наукових дослідженнях.

Висновки

На підставі аналізу дисертаційної роботи Гавеля Сергія Миколайовича, з урахуванням актуальності обраної теми, наукової новизни, практичного значення одержаних результатів, їх обґрунтованості та достовірності, вважаю, що дисертація на тему «Підвищення прихованості передавання інформації на основі прямого розширення спектра таймерних сигнальних конструкцій» є завершеним, самостійним і цілісним науковим дослідженням, у якому розв'язано актуальне науково-прикладне завдання підвищення захищеності інформації в інформаційно-комунікаційних системах шляхом розроблення методів прямого розширення спектра таймерних сигнальних конструкцій, що забезпечують підвищення енергетичної та структурної прихованості передавання інформації.

Дисертаційна робота Гавеля Сергія Миколайовича 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 року № 44 (зі змінами), а також Вимогам до оформлення дисертації, затвердженим наказом Міністерства освіти і науки України від 12.01.2017 № 40 (зі змінами), а її автор Гавель Сергій Миколайович заслуговує на присудження ступеня доктора філософії за спеціальністю 125 Кібербезпека.

Офіційний опонент

проректор з наукових досліджень та трансферу технологій,
професор кафедри комп'ютерних інформаційних технологій
Національного університету «Київський авіаційний інститут»,
доктор технічних наук, професор

Сергій ГНАТЮК