

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.

Актуальність роботи

Сучасний розвиток інформаційно-комунікаційних систем (ІКС) супроводжується широким застосуванням безпроводових технологій передавання інформації, що, своєю чергою, підвищує вимоги до захисту інформації в радіоканалах зв'язку. Особливої актуальності ця проблема набуває в умовах розвитку засобів радіоелектронної розвідки, радіомоніторингу та радіоелектронної боротьби, здатних здійснювати виявлення, класифікацію та аналіз параметрів сигналів.

Одним із перспективних напрямів протидії таким загрозам є підвищення прихованості передавання інформації за рахунок одночасного забезпечення енергетичної та структурної прихованості сигнально-кодових конструкцій. Актуальність дослідження зумовлена тим, що класичні методи розширення спектра, хоча й забезпечують зниження спектральної щільності потужності сигналів та підвищення їх завадостійкості, не завжди достатньою мірою забезпечують приховування структури сигналу та ускладнення її розпізнавання засобами радіоелектронної розвідки (РЕР).

У дисертаційній роботі розглядається актуальне науково-технічне завдання підвищення прихованості передавання інформації шляхом формування широкосмугових шумоподібних сигналів на основі таймерних сигнальних конструкцій (ТСК) та псевдовипадкових послідовностей (ПВП). Особливість запропонованого підходу полягає у поєднанні переваг прямого розширення спектра (ПРС), яке забезпечує енергетичну прихованість, із непозиційним принципом формування ТСК, що створює додаткові передумови для підвищення структурної прихованості.

З огляду на зазначене, тема дисертаційної роботи Гавеля Сергія Миколайовича є актуальною, має важливе науково-прикладне значення для розвитку методів захисту інформації в ІКС та системах захищеного радіозв'язку.

Наукові результати та їх новизна

Наукова новизна дисертаційної роботи визначається розробленням та удосконаленням методів підвищення прихованості передавання інформації на основі прямого розширення спектра таймерних сигналів. Отримані результати спрямовані на підвищення структурної та енергетичної прихованості сигнально-кодових конструкцій, їх завадостійкості та рівня захисту інформації в інформаційно-комунікаційних системах.

До основних наукових результатів дисертаційної роботи належать:

- вперше розроблено інтегрований метод формування широкосмугових

шумоподібних таймерних сигналів із використанням псевдовипадкових послідовностей, що забезпечує керовані кореляційні та спектральні властивості сигналів;

- удосконалено методику оцінювання структурної прихованості шумоподібних таймерних сигналів з урахуванням внеску таймерних сигнально-кодкових конструкцій, псевдовипадкових послідовностей прямого розширення спектра та системи модуляції;

- вперше запропоновано поняття інтерпретованої бази широкосмугового таймерного сигналу, що враховує розширення спектра на інтервалі формування всієї таймерної комбінації;

- набув подальшого розвитку метод розширення спектра таймерних сигналів, сформованих на основі системи залишкових класів, шляхом поєднання завадостійкого кодування та структурної прихованості;

- удосконалено метод розширення спектра таймерних сигналів із використанням послідовностей Уолша та псевдовипадкових послідовностей на основі хаотичних коливань, що забезпечує динамічну зміну їх кореляційних властивостей.

У цілому наведені результати характеризуються науковою новизною та спрямовані на комплексне підвищення енергетичної і структурної прихованості, завадостійкості та захищеності передавання інформації в інформаційно-комунікаційних системах.

Практичне значення та практична цінність отриманих результатів

Практичне значення дисертаційної роботи полягає у розробленні методів формування та прямого розширення спектра широкосмугових шумоподібних таймерних сигналів, які можуть бути використані під час проєктування та модернізації захищених ІКС, що функціонують в умовах радіоелектронного протистояння та кіберзагроз.

Запропоновані методи забезпечують можливість керування спектральними та кореляційними характеристиками сигналів, підвищення їх енергетичної та структурної прихованості, а також завадостійкості. Практичний інтерес становлять метод визначення інтерпретованої бази широкосмугового таймерного сигналу та інтегрована методика оцінювання його структурної прихованості, які можуть застосовуватися під час обґрунтування параметрів сигнально-кодкових конструкцій.

Практичну цінність також має запропонований комбінований метод прямого розширення спектра із використанням таймерних сигналів, послідовностей Уолша та хаотичних ПВП, що створює можливість підвищення прихованості передавання інформації без суттєвого ускладнення структури сигналу.

Результати дисертаційної роботи впроваджено в навчальний процес кафедри кібербезпеки та технічного захисту інформації Державного університету інтелектуальних технологій і зв'язку, що підтверджено відповідним актом впровадження.

Отже, отримані результати мають практичну цінність та можуть бути використані під час створення і вдосконалення захищених радіотехнічних та

телекомунікаційних систем для підвищення прихованості, завадостійкості та захищеності передавання інформації.

Оцінка змісту, ступеню завершеності та обґрунтованості положень дисертації

Повний обсяг дисертаційної роботи становить 181 сторінку, з яких 136 сторінок – основний текст. Дисертація складається зі вступу, чотирьох розділів, висновків, двох додатків та списку використаних джерел.

У вступі обґрунтовано актуальність теми дисертаційного дослідження, визначено мету, об'єкт, предмет і завдання роботи. Сформульовано основні положення наукової новизни, визначено методи дослідження, розкрито теоретичне та практичне значення отриманих результатів. Наведено відомості про особистий внесок здобувача, апробацію результатів дослідження, публікації та структуру дисертаційної роботи.

Перший розділ присвячено аналізу сучасного стану проблеми забезпечення прихованості передавання інформації в інформаційно-комунікаційних системах. Розглянуто основні інформаційні характеристики сигналів, ентропійні підходи до оцінювання сигнальних конструкцій, особливості структурної прихованості, а також методи її кількісного оцінювання. Проаналізовано властивості псевдовипадкових послідовностей, зокрема М-послідовностей, послідовностей Голда, Касамі, Уолша та хаотичних послідовностей. Розглянуто вплив бази сигналу на його прихованість і завадостійкість. Проведений аналіз дав змогу визначити напрями подальших досліджень та обґрунтувати постановку завдань дисертаційної роботи.

Другий розділ присвячено дослідженню та розвитку теоретичних положень щодо формування псевдовипадкових послідовностей і підвищення їх структурної прихованості. Розглянуто методи формування ПВП на основі лінійних та нелінійних генераторів, проведено порівняльний аналіз їхніх характеристик. Досліджено можливості використання генераторів хаосу для формування ПВП із підвищеними статистичними та кореляційними характеристиками. Розглянуто методи адаптивного квантування та додаткової модифікації сформованих послідовностей. Проведено аналіз впливу бази сигналу на прихованість, завадостійкість та ефективність передавання інформації.

Третій розділ присвячено розробленню методів підвищення прихованості передавання інформації на основі прямого розширення спектра таймерних сигнальних конструкцій. Запропоновано метод формування широкосмугових шумоподібних таймерних сигналів із використанням псевдовипадкових послідовностей. Досліджено можливості застосування послідовностей Уолша та хаотичних ПВП для формування шумоподібних сигналів. Запропоновано підходи до кількісного оцінювання структурної прихованості та визначення бази широкосмугового таймерного сигналу. Проведено порівняльний аналіз отриманих характеристик та досліджено залежність прихованості й завадостійкості від параметрів сформованих сигнальних конструкцій.

Четвертий розділ присвячено дослідженню процесів передавання та

приймання ширококутових таймерних сигналів. Розглянуто структурну схему формування шумоподібних таймерних сигналів із ПРС та математичну модель їх передавання каналом зв'язку. Розроблено підхід до кореляційного приймання ширококутових таймерних сигналів, який враховує їхню непозиційну часову структуру та забезпечує відновлення значущих моментів і тривалостей елементів таймерної комбінації. Досліджено вплив параметрів сигналу та каналу зв'язку на достовірність відновлення його структури. Показано можливість одночасного забезпечення енергетичної та структурної прихованості під час передавання інформації.

У загальних висновках систематизовано основні результати дисертаційного дослідження, сформульовано висновки щодо розроблених методів формування, розширення спектра, приймання та оцінювання ширококутових таймерних сигнальних конструкцій, а також визначено їх значення для підвищення прихованості передавання інформації.

У додатках наведено матеріали, що доповнюють основний зміст дисертації та підтверджують результати проведених досліджень і практичне використання отриманих результатів.

Загалом зміст дисертаційної роботи відповідає поставленій меті та визначеним завданням. Структура роботи є логічною та послідовною, а основні положення підтверджено математичними моделями, аналітичними залежностями, розрахунками та результатами досліджень. Отримані результати взаємопов'язані між собою та послідовно розкривають поставлену науково-прикладну задачу підвищення прихованості передавання інформації на основі прямого розширення спектра таймерних сигнальних конструкцій. Це дає підстави вважати дисертаційну роботу завершеним самостійним науковим дослідженням, результати якого мають наукову новизну та практичну цінність.

Повнота викладення результатів дисертації у наукових виданнях

Основні результати дисертаційного дослідження достатньо повно висвітлено у наукових працях здобувача. За темою дисертації опубліковано 14 наукових праць, з яких 6 статей у наукових фахових виданнях України, одна з яких опублікована у виданні, що індексується наукометричною базою Scopus, та 8 тез доповідей у матеріалах наукових конференцій.

Окремо слід зазначити, що одна наукова праця включена до складу монографії. Загалом у виданнях, що індексуються наукометричними базами даних Scopus, представлено 2 наукові праці, з яких одна є науковою статтею, а одна – тезами конференційної доповіді.

Зміст опублікованих праць охоплює основні положення та результати дисертаційного дослідження, зокрема питання підвищення прихованості передавання інформації, формування та розширення спектра таймерних сигнальних конструкцій, використання псевдовипадкових послідовностей, оцінювання структурної прихованості та забезпечення завадостійкості інформаційно-комунікаційних систем.

Отже, результати дисертаційної роботи в достатньому обсязі апробовані та оприлюднені в наукових виданнях і матеріалах наукових конференцій, що підтверджує повноту їх викладення та належний рівень апробації основних

положень дисертаційного дослідження.

Оформлення дисертації та дотримання вимог академічної доброчесності

Дисертаційна робота Гавеля Сергія Миколайовича оформлена відповідно до встановлених вимог, має послідовну структуру та виконана з дотриманням наукового стилю й використанням відповідної наукової термінології. Тема, зміст, мета, завдання та отримані наукові результати відповідають спеціальності 125 Кібербезпека галузі знань 12 Інформаційні технології.

Аналіз змісту дисертації та опублікованих за її результатами наукових праць свідчить про дотримання основних принципів академічної доброчесності. У роботі наведено посилання на використані наукові джерела та результати досліджень інших авторів. Наукові положення, методи та результати, що становлять особистий внесок здобувача, належним чином представлені в дисертації та його наукових публікаціях.

Ознак порушення академічної доброчесності, неправомірних запозичень або використання результатів інших авторів без відповідного посилання не виявлено. Загалом оформлення дисертації та представлення результатів дослідження відповідають встановленим вимогам до дисертаційних робіт.

Зауваження до дисертаційної роботи.

1. У першому розділі дисертації окремі теоретичні положення викладено досить детально. Зокрема, це стосується загальних питань теорії інформації, ентропійного оцінювання та характеристик псевдовипадкових послідовностей. Доцільним напрямом удосконалення структури роботи могло б бути скорочення загальновідомих теоретичних відомостей та більш концентроване представлення матеріалу, безпосередньо пов'язаного із завданнями оцінювання структурної прихованості таймерних сигналів.

2. У підрозділі 2.4 структурна прихованість оцінюється переважно за кількістю можливих реалізацій сигнальних конструкцій. Доцільним було б ширше врахувати практичні характеристики засобів радіоелектронної розвідки та умови їх спостереження.

3. У підрозділі 3.2 наведено детальний аналіз різних типів ПВП, проте критерії їх вибору для методу прямого розширення спектра можна було б сформулювати більш чітко з урахуванням взаємозв'язку кореляційних, ансамблевих та структурних характеристик.

4. У підрозділі 3.5 доцільно було б сформулювати узагальнений критерій ефективності, який би дозволяв оцінювати компроміс між підвищенням енергетичної та структурної прихованості, завадостійкістю і витратами частотного ресурсу зі збільшенням бази сигналу. Це дозволило б більш обґрунтовано визначати оптимальні значення бази ширококутових таймерних сигналів залежно від вимог до захищеності передавання інформації.

5. У п. 4.4 запропоновано інтегральний показник структурної прихованості, який визначається як сума внесків таймерних сигналів, ПВП та системи модуляції. Водночас доцільним було б додатково обґрунтувати незалежність зазначених складових та адитивність їх внесків до загального

показника структурної прихованості.

6. У дисертаційній роботі наявні окремі орфографічні, стилістичні та технічні неточності (формули 1.2, 1.39, 3.27), а також поодинокі друкарські помилки й недоліки в оформленні окремих матеріалів. Зазначені зауваження мають переважно редакційний характер і не впливають на загальну наукову цінність та практичну значущість отриманих результатів.

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

Дисертаційна робота Гавеля Сергія Миколайовича на тему «Підвищення прихованості передавання інформації на основі прямого розширення спектра таймерних сигнальних конструкцій» є завершеним, самостійним науковим дослідженням, у якому розв'язано актуальне науково-прикладне завдання підвищення прихованості передавання інформації в інформаційно-комунікаційних системах шляхом розроблення та вдосконалення методів формування і прямого розширення спектра таймерних сигнальних конструкцій.

Отримані в дисертації результати характеризуються науковою новизною, теоретичною обґрунтованістю та практичною значущістю. Запропоновані методи забезпечують підвищення енергетичної та структурної прихованості сигнальних конструкцій і можуть бути використані під час створення та модернізації захищених інформаційно-комунікаційних систем, що функціонують в умовах радіоелектронного протистояння та кіберзагроз.

Результати дисертаційного дослідження достатньо повно висвітлені у наукових публікаціях здобувача, зокрема у фахових виданнях України та виданнях, що індексуються наукометричною базою даних Scopus. Оформлення дисертації відповідає встановленим вимогам, а аналіз її змісту та опублікованих праць свідчить про дотримання принципів академічної доброчесності.

З урахуванням актуальності теми, обґрунтованості наукових положень, достовірності отриманих результатів, їх наукової новизни та практичної цінності вважаю, що дисертаційна робота Гавеля Сергія Миколайовича відповідає вимогам, що висуваються до дисертацій на здобуття наукового ступеня доктора філософії.

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

Офіційний рецензент
кандидат технічних наук, доцент
кафедри кібербезпеки та технічного
захисту інформації Державного
університету інтелектуальних
технологій і зв'язку

Олексій ОНАЦЬКИЙ