Голові спеціалізованої вченої ради Д 41.113.03
Державного університету
інтелектуальних технологій і зв'язку
вул. Кузнечна, 1, м. Одеса

ВІДГУК

офіційного опонента – член-кореспондента НАН України,
Заслуженого діяча науки і техніки України,
лауреата Державної премії України в галузі науки і техніки,
першого проректора Державного університету
інформаційно-комунікаційних технологій,
доктора технічних наук, професора
Корченка Олександра Григоровича
на дисертаційну роботу
Кільдішева Віталія Йосиповича
«Моделі та методи захисту інформації на основі параметричного перетворення передаваних сигнально-кодових конструкцій»,
подану на здобуття наукового ступеня доктора технічних наук
за спеціальністю 05.13.21 – системи захисту інформації

1. Актуальність теми. Зростання загроз інформаційній безпеці, зумовлене розвитком засобів несанкціонованого доступу (НСД) та радіоелектронної розвідки (РЕР), визначає високу актуальність проведеного дисертаційного дослідження. Особливої ваги набуває проблема забезпечення захищеності інформаційно-комунікаційних систем із безпроводовим передаванням, які є найбільш вразливими до перехоплення та спотворення даних у середовищі радіоелектронного протиборства.

У сучасних умовах спостерігається фундаментальне протиріччя між необхідністю забезпечення високого рівня прихованості передавання інформації та обмеженими можливостями традиційних методів розширення спектра на основі псевдовипадкових послідовностей (ПВП), структура яких є передбачуваною і піддається відновленню засобами кореляційного та спектрального аналізу.

Подолання цього протиріччя можливе за рахунок створення нових сигнально-кодових конструкцій із нестабільною, непередбачуваною структурою та низькою спектральною щільністю, що ускладнює їх виявлення засобами РЕР навіть за умови використання високочутливих приймачів. У цьому контексті

перспективним є застосування таймерних сигнальних конструкцій, які завдяки своїй непозиційній природі та можливості параметричного керування дозволяють ефективно поєднувати властивості завадостійкого кодування, статистичного шифрування та спектрального розширення.

Отже, актуальність теми дисертаційної роботи Кільдішева Віталія Йосиповича полягає у необхідності розробки інтегрованих методів формування та перетворення сигнально-кодових конструкцій, здатних забезпечити одночасно високу прихованість, завадостійкість і криптостійкість передавання інформації в умовах радіоелектронного впливу.

2. Ступінь обґрунтованості наукових положень дисертації, їх достовірність і новизна. Основні наукові результати дослідження, висновки та практичні рекомендації чітко сформульовані, логічно обґрунтовані та не викликають сумнівів щодо їх достовірності. Коректність наукових положень дисертації забезпечується системним застосуванням теорії прихованості, криптографії, завадостійкого кодування, методів радіоелектронних систем і комплексів, теорії ймовірностей та підходів до моделювання складних систем. Для перевірки висунутих гіпотез і оцінювання ефективності запропонованих методів використано комплекс аналітичного та імітаційного моделювання.

Основні наукові результати дисертації, на мій погляд, полягають у наступному:

вперше

– запропоновано модель оцінювання захищеності передавання сигнально-кодових конструкцій на основі обсягу сигналу (тривалість сигналу, ширина спектра та динамічний діапазон), яка дозволяє оцінювати енергетичну, структурну та інформаційну прихованість. Завдяки цьому стає можливим комплексне оцінювання рівня прихованості та виявлення критичних вразливостей систем зв'язку в умовах радіоелектронного впливу.

– вперше розроблена узагальнена модель удосконалення методів прихованого передавання інформації, що забезпечує можливість формалізованого порівняльного аналізу відомих та нових методів захисту. Запропонований підхід дозволяє визначати найбільш ефективні рішення за критеріями завадостійкості та прихованості, що сприяє підвищенню адаптивності систем зв'язку.

– запропоновано метод взаємного обміну між якістю та швидкістю передавання даних шляхом комбінованого використання таймерних і позиційних кодів у нестаціонарних каналах. Такий підхід відкриває можливість гнучкого

балансування між надійністю і пропускною здатністю, що є важливим у сучасних системах захищеного зв'язку.

– розроблено метод одночасного захисту інформації від несанкціонованого доступу та випадкових завад, у якому визначено залежність рівня прихованості від мінімальної кодової відстані сигнальних конструкцій. Це забезпечує підвищення стійкості каналів до атак радіоелектронної розвідки та випадкових перешкод у складних умовах функціонування.

– створено багаторівневу модель захисту інформації, що інтегрує статистичне шифрування, завадостійке та таймерне кодування, а також процедури декореляції помилок. Така інтеграція дозволила досягти синергетичного ефекту, що значно підвищує криптостійкість та надійність функціонування інформаційно-комунікаційних систем.

– встановлено закономірності впливу параметрів таймерних сигнальних конструкцій на структурну прихованість і завадостійкість шумоподібних сигналів. На основі проведених досліджень визначено критерії вибору оптимальних параметрів, що дозволяють адаптивно налаштовувати системи до конкретних умов застосування.

– розвинуто теорію систем зв'язку з шумоподібними сигналами шляхом створення нових алгоритмів розширення спектра непозиційних сигналів (ППРЧ, ПРС-ПВП, ЛЧМ). При цьому визначено умови забезпечення енергетичної прихованості, що розширює можливості використання даних методів у завадозахищених системах передаванні інформації;

удосконалено:

– алгоритми розширення спектра для таймерних сигналів, які враховують структуру побудови непозиційних сигнальних конструкцій. На відміну від відомих методів для позиційних кодів, запропоновані алгоритми забезпечують розширення спектра на всьому інтервалі формування таймерної комбінації з урахуванням бази елемента та кількості імпульсів розширення, що визначаються параметрами сигнальної конструкції;

– алгоритми кореляційного прийому непозиційних таймерних сигналів для різних способів розширення спектра, які відрізняються від відомих підходів тим, що прийом сигнальних конструкцій здійснюється на інтервалі всієї комбінації із використанням опорної послідовності та визначенням значущих моментів відтворення за екстремумами напруги на виході інтегратора кореляційного приймача.

Сукупність указаних вище принципів і методів формують методологію підвищення захищеності інформаційно-комунікаційних систем на основі інтеграції параметричних перетворень сигнально-кодових конструкцій, яка завдяки узгодженому використанню таймерного та завадостійкого кодування, статистичного шифрування, декореляції помилок і методів розширення спектра забезпечує створення багаторівневих систем захисту інформації, стійких до випадкових завад, несанкціонованого доступу та радіоелектронного впливу, із гарантованим рівнем енергетичної, структурної та інформаційної прихованості.

3. Практична цінність результатів полягає у розробленні структурних схем і алгоритмів роботи пристроїв розширення спектра для непозиційних і таймерних сигналів, створенні інтегрованої системи захисту інформації, у якій на кожному рівні забезпечується завадостійкість і криптографічна стійкість, а також у сформованих критеріях і методиках перевірки ефективності функціонування таких систем.

Додатково практична цінність дисертаційного дослідження підтверджується актами впровадження КП «Обласний інформаційно-аналітичний центр» Одеської обласної ради, ПП «АРДО», а також у навчальному процесі кафедри кібербезпеки та технічного захисту інформації Державного університету інтелектуальних технологій і зв'язку в процесі викладання дисциплін для підготовки бакалаврів та магістрів за напрямом 125 «Кібербезпека та захист інформації».

4. Оцінка змісту та структури дисертаційної роботи. Дисертаційна робота складається зі вступу, шести розділів, висновків, додатків і списку використаних джерел (154 найменувань). Повний об'єм дисертації складає 340 сторінок, у тому числі 291 сторінка основного тексту.

У вступі обґрунтовано актуальність дослідження, наведено зв'язок роботи з науковими програмами, планами та темами, визначено мету та задачі роботи, визначено об'єкт та предмет дослідження. Наведено наукову новизну та практичну цінність отриманих результатів, визначено особистий внесок здобувача в роботах, опублікованих у співавторстві, представлено відомості про апробацію та публікації результатів дослідження.

У першому розділі здійснено аналіз наукових джерел щодо забезпечення захищеності інформаційно-комунікаційних систем, що дозволило сформувати концепцію багаторівневого захисту на основі поєднання енергетичної, структурної та інформаційної прихованості. Обґрунтовано доцільність інтеграції засобів маскування й криптографічного захисту, визначено ключові параметри сигналів, що впливають на завадозахищеність, та запропоновано модель оцінювання

ефективності методів захисту за критеріями прихованості, завадостійкості й використання канальних ресурсів.

У другому розділі досліджено теоретичні та прикладні аспекти підвищення завадостійкості передавання інформації в умовах радіоелектронної боротьби на основі сумісного використання блокових кодів і таймерних сигналів. Обґрунтовано доцільність моделювання нестаціонарних каналів зв'язку з урахуванням корельованих завад та використання моделей Гільберта й Маркова для оцінювання достовірності передачі. Показано, що таймерні сигнали дають змогу компенсувати надлишковість блокових кодів і забезпечують адаптивний обмін між швидкістю та якістю передавання. Запропоновано метод оцінювання кодів Слєпяна з урахуванням часових властивостей сигналів, що дозволяє зменшити часові витрати й підвищити ефективність використання каналу. Отримані результати створюють основу для побудови адаптивних методів захисту інформації в умовах дії завад.

У третьому розділі розроблено принципи та методи підвищення захищеності інформації шляхом використання непозиційних таймерних сигнально-кодових конструкцій, які забезпечують структурну прихованість і завадостійкість передавання. Обґрунтовано доцільність поєднання таймерного, позиційного та стохастичного кодування для компенсації надлишковості та підвищення рівня захисту. Встановлено закономірності взаємозв'язку між структурною прихованістю та коригувальною здатністю сигналів, а також показано можливість їх керованого балансування за допомогою рівняння якості Захарченка. Розроблено підхід до формування множин таймерних сигналів із контрольованою надлишковістю, що дозволяє створювати багаторівневі захищені канали зв'язку в умовах дії завад.

У четвертому розділі обґрунтовано інтегрований підхід підвищення захищеності передавання інформації шляхом поєднання стохастичного шифрування, завадостійкого та таймерного кодування. Запропоновано багаторівневу структуру захисту, у якій кожен рівень виконує власну функцію – від забезпечення криптографічної стійкості до компенсації надлишковості та підвищення структурної прихованості сигналів. Розроблено методи формування шифрограм із варіативними комбінаціями кодових слів, що підвищують ентропію та ускладнюють криптоаналіз. Доведено, що поєднання статистичного шифрування з таймерним і завадостійким кодуванням забезпечує синергетичний ефект, підвищуючи надійність і стійкість системи до завад та несанкціонованого доступу в умовах дії засобів РЕБ.

У п'ятому розділі виконано комплексний аналіз параметрів таймерних сигналів для формування шумоподібних сигнально-кодових конструкцій у системах захисту інформації. Обґрунтовано критерії вибору параметрів ТСК з урахуванням вимог до завадостійкості, прихованості та складності реалізації. Показано, що керування параметрами таймерних сигналів дозволяє досягати оптимального балансу між пропускною здатністю, надійністю передачі та структурною прихованістю. Проведено оцінку застосування хаотичних генераторів для синтезу псевдовипадкових послідовностей і доведено ефективність їх комбінування з таймерним кодуванням. Запропоновані методи забезпечують формування багаторівневих шумоподібних сигналів із високим рівнем криптографічної стійкості, що створює основу для побудови сучасних завадостійких і прихованих каналів зв'язку.

У шостому розділі дисертації узагальнено результати дослідження та представлено методологію побудови систем захисту інформації на основі синтезу шумоподібних таймерних сигналів, орієнтованих на забезпечення високого рівня енергетичної та структурної прихованості в умовах активних радіоелектронних впливів. Проведений аналіз дозволив довести ефективність комбінованого застосування таймерного кодування з методами розширення спектра — ППРЧ, ЛЧМ, ПРС-ПВП, а також хаотичними та мультиплексними структурами сигналів. Такий підхід забезпечує формування широкого класу сигнально-кодових конструкцій із підвищеною завадостійкістю та криптографічною складністю. Результати розрахунків і моделювання підтвердили, що адаптивне керування параметрами таймерного кодування дозволяє зберігати прихованість передачі навіть за умов низького відношення сигнал/шум, а також зменшувати кількість піднесучих частот без втрати енергетичної ефективності. Таким чином, у розділі обґрунтовано, що інтеграція таймерного кодування з методами розширення спектра та хаотичними процесами формує основу для створення адаптивних, енергетично прихованих і структурно стійких каналів зв'язку, здатних ефективно функціонувати в умовах радіоелектронної боротьби.

Додатки містять допоміжний матеріал з результатів досліджень, а також 3 акти впровадження результатів роботи.

5. Повнота викладу наукових положень, висновків, рекомендацій в опублікованих працях здобувача. Основні наукові результати, що отримані в дисертації, у повній мірі викладені здобувачем у 44 наукових працях, зокрема: 1 монографія, 22 статті, з яких 20 статей у фахових наукових журналах, що входять до переліку МОН України, зокрема 1 стаття в журналі, який цитується в

наукометричній базі даних Scopus та 1 стаття – у наукометричній базі даних Web of Science. Дві статті опубліковано в іноземних фахових виданнях, які цитуються в наукометричній базі даних Scopus.

Апробація досліджень дисертації: 21 публікація опубліковано в матеріалах міжнародних та всеукраїнських симпозіумів, науково-практичних та науково-технічних конференцій, з яких 5 наукових праць – у виданнях, які цитуються у наукометричній базі даних Scopus.

Загальна кількість наукових праць у виданнях, які цитуються у наукометричних базах даних Scopus та Web of Science складає 9, з яких – 4 статті та 5 тез до конференцій. Крім зазначених робіт, складено 6 звітів з НДР за спеціальною тематикою.

Апробацію результатів досліджень на міжнародних та всеукраїнських науково-технічних конференціях слід визнати достатньою.

6. Відповідність дисертації встановленим вимогам. Дисертація написана сучасною науково-технічною мовою, її оформлення відповідає вимогам МОН України, що пред'являються до дисертаційних робіт. Зміст автореферату достатньо повно розкриває зміст дисертації, об'єктивно відображає основні положення дисертаційної роботи.

У цілому можна позитивно оцінити дисертаційне дослідження, відзначити його наукову новизну та практичне значення, високий теоретичний рівень.

7. Відповідність паспорту спеціальності. Основні результати роботи спрямовані на створення систем захисту інформації від помилок у каналі зв'язку та несанкціонованого доступу й відповідають паспорту спеціальності 05.13.21 – системи захисту інформації, зокрема, п. 1 «Теоретичні, методологічні, технічні, технологічні й організаційні основи створення комплексних систем захисту інформації (СЗІ), зокрема інформації, що зберігається, оброблюється і передається в комп'ютерних системах і мережах», п. 2 «Організація, архітектура, методологія проектування, технологія функціонування СЗІ» і п. 3 «Математичні моделі інформаційних структур, що потребують захисту, шифрів, шифросистем та криптографічних протоколів».

8. Зауваження щодо змісту дисертації:

1. У першому розділі (п.1.4) запропоновано модель оцінювання захищеності передачі інформації на основі обсягу сигналу (рис. 1.9). Водночас доцільно було б подати структуру моделі для кожного із запропонованих методів розширення спектра, що дозволило б наочно оцінити відповідність сформованих шумоподібних сигналів параметрам каналу зв'язку.

2. У другому розділі при використанні моделей дискретного каналу Пуртова та Елліота–Гільберта (п. 2.1) для моделювання процесів передавання сигнальних конструкцій в умовах радіоелектронної боротьби не подано обґрунтованого вибору та діапазону їх параметрів, що обмежує можливість кількісної оцінки адекватності моделювання реальним умовам.
3. У третьому розділі (п. 3.5) подано результати дослідження ефективності J-кратного повторення таймерних сигналів для підвищення завадостійкості, однак не розглянуто аспект структурної прихованості, який суттєво впливає на рівень захисту інформації від несанкціонованого доступу.
4. У четвертому розділі розроблено концепцію багаторівневого захисту інформації від випадкових завад і несанкціонованого доступу. Водночас оцінка криптостійкості виконана лише для статистичного шифрування (п. 4.8) і не охоплює інші рівні перетворення даних, що ускладнює формування цілісного уявлення про рівень захищеності всієї багаторівневої системи.
5. У п'ятому розділі проведено аналіз параметричного перетворення даних на основі таймерних сигналів у задачі розширення спектра та визначено вплив основних параметрів на завадостійкість системи. Водночас обмеження параметрів побудови сигналів наведено лише для елемента Δ з метою забезпечення потрібного рівня стійкості до завад. Для інших характеристик, зокрема максимальної кількості найквістових інтервалів m, такі межі не визначено, що ускладнює повну оцінку ефективності побудови таймерних сигналів.
6. У шостому розділі під час розгляду алгоритмів розширення спектра непозиційних таймерних сигналів не наведено обґрунтування вибору або опису методів синхронізації, які доцільно застосовувати в інформаційно-комунікаційних системах для забезпечення захисту передаваної інформації.
7. У 3-му, 4-му, 5-му та 6-му пунктах наукової новизни не зазначено ступінь новизни; у її 3-му і 5-му пунктах не зазначено за рахунок чого досягається ефект, а у 6-му не визначений ефект від запропонованого рішення.
8. Формулювання 2-го, 3-го та 4-го пункту практичного значення носить більш теоретичний характер і не відображає прикладну (практичну) спрямованість рішення.
9. У тексті дисертації виявлено неповну уніфікацію термінології, зокрема у вживанні понять, що стосуються параметрів сигнально-кодових конструкцій та методів їх перетворення, а також окремі стилістичні та орфографічні

неточності, наприклад, після формул (1.20), (1.42), (1.47), (2.29) відсутні коми, після формули (1.36) зайва двокрапка тощо.

Висновок. Дисертаційна робота Кільдішева Віталія Йосиповича є завершеним науковим дослідженням, присвяченим актуальній науково-технічній проблемі підвищення захищеності інформації в інформаційно-комунікаційних системах. У роботі вирішено важливе наукове завдання розроблення теоретичних засад і методів захисту інформації на основі шифрування, таймерного кодування та спектрального розширення сигналу. Запропоновані алгоритми забезпечують формування шумоподібних сигнально-кодових конструкцій з підвищеними властивостями завадостійкості, структурної прихованості та стійкості до несанкціонованого доступу, що створює науково обґрунтовану основу для побудови ефективних комплексних систем захисту інформації в умовах радіоелектронного впливу.

Дисертаційна робота відповідає вимогам "Порядку присудження та позбавлення наукового ступеня доктора наук", затвердженого постановою Кабінету Міністрів України від 17 листопада 2021 р. № 1197, а її автор – Кільдішев Віталій Йосипович – заслуговує на присудження наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – системи захисту інформації.

Офіційний опонент:
Перший проректор Державного університету
інформаційно-комунікаційних технологій,
член-кореспондент НАН України,
доктор технічних наук, професор,
лауреат Державної премії України
в галузі науки і техніки,
Заслужений діяч
науки і техніки України Олександр КОРЧЕНКО