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

ВІДГУК

офіційного опонента – завідувача кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету доктора технічних наук, професора Смірнова Олексія Анатолійовича 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

Актуальність теми дисертації.

Сучасні досягнення науки і техніки визначають нові напрямки розвитку методів і засобів захисту інформації в умовах зростаючих кібернетичних та радіоелектронних загроз.

Тема дисертаційної роботи Кільдішева В.Й. пов'язана з процесами забезпечення захищеності передавання інформації в інформаційно-комунікаційних системах, особливо в умовах використання безпроводових каналів, які є найбільш уразливими до несанкціонованого доступу та перехоплення.

В роботі сформульовано науково-прикладну проблему розробки методології підвищення захищеності переданої інформації на основі інтеграції методів шифрування, завадостійкого кодування та спектрального розширення сигналів. Проблема породжена протиріччям між необхідністю забезпечення високого рівня конфіденційності, цілісності та доступності даних і недостатньою ефективністю існуючих методів прихованого передавання інформації, що базуються переважно на передбачуваних псевдовипадкових послідовностях. У роботі досягається забезпечення конфіденційності інформації шляхом параметричного перетворення нових сигнально-кодових конструкцій, які мають низьку спектральну щільність та підвищену стійкість до кореляційного аналізу й статистичного моніторингу.

ДУІТЗ
вх 01-33/445
04 11 2025

Таким чином, тема дисертаційної роботи є актуальною, оскільки вона спрямована на розв'язання важливої науково-прикладної задачі захисту інформації в умовах сучасних радіоелектронних загроз і має вагоме значення як для розвитку теорії захищених систем зв'язку, так і для практики побудови сучасних засобів інформаційної безпеки.

Зв'язок дисертації з науковими програмами, планами, темами.

Результати дисертації пов'язані з наступними НДР: "Розробка мобільної системи захищеного інформаційного обміну для військових і цивільних підрозділів державних структур" (№ 0120U102607), "Інформаційна технологія психолінгвістичного аналізу тексту для стеганографічних систем" (№ 0123U102085), "Методи та засоби синтеза груп симетричних двухоперандних операцій криптографічного кодування для малоресурсних криптоалгоритмів" (№ 0121U114390), "Дослідження шляхів розвитку потокового шифрування на основі криптографічного кодування" (№ 0121U114389), "Розробка комплексних технологій інтелектуального керування складними організаційно-технологічними об'єктами в кризових умовах" (№ 0120U104341), "Інтелектуальне управління оцінюванням ефективності цифрової трансформації бізнесу" (№ 0120U104442).

Робота відповідає актуальному пріоритетному напряму наукових досліджень "Інформаційно-комунікаційні та радіоелектронні системи та технології, засоби радіоелектронної боротьби для забезпечення національної безпеки і оборони. Інформаційна безпека та кібербезпека" та положенням "Стратегії інформаційної безпеки", введеної в дію Указом Президента України від 28.12.2021 № 685/2021.

Достовірність та обґрунтованість одержаних наукових результатів.

Достовірність та обґрунтованість отриманих у дисертації наукових результатів підтверджується коректністю застосованого методологічного апарату, повнотою проведених теоретичних узагальнень і результатами моделювання. Використані аналітичні та числові методи базуються на фундаментальних положеннях теорії інформації, теорії сигналів, теорії ймовірностей та математичної статистики.

Обґрунтованість запропонованих положень забезпечено порівнянням результатів моделювання таймерних сигналів і шумоподібних сигнально-кодових конструкцій з відомими методами розширення спектра (псевдовипадковий перескок робочої частоти (ППРЧ), пряме розширення спектра псевдовипадковими послідовностями (ПРС-ПВП), лінійна частотна модуляція (ЛЧМ) та інші), що підтвердило адекватність розроблених моделей.

Висновки про ефективність запропонованих рішень зроблено на основі комплексного аналізу показників завадостійкості, структурної прихованості та пропускної здатності каналів.

Достовірність отриманих результатів підкріплена узгодженістю теоретичних висновків із результатами числового експерименту, а також відповідністю моделей і алгоритмів фізичним принципам побудови інформаційно-комунікаційних систем. Запропоновані залежності та критерії вибору параметрів таймерних сигнальних конструкцій перевірено шляхом імітаційного моделювання в середовищі C++ і підтверджено аналітичними розрахунками.

Отримані висновки та рекомендації є логічним наслідком поставлених завдань і мають внутрішню узгодженість між теоретичними, методичними та практичними результатами.

Положення в достатній і необхідній мірі опубліковані та обговорені науковою спільнотою при апробації на наукових конференціях та семінарах. Достовірність сформованих у роботі висновків та рекомендацій додатково підтверджується актами впровадження, копії яких представлено в додатку Б.

Наукова новизна отриманих результатів дисертаційної роботи, на мою думку, перш за все, полягає у наступному:

1. Розвинуто теорію систем передавання інформації з шумоподібними сигналами шляхом побудови нових методів спектрального розширення таймерних сигналів (ППРЧ, ПРС-ПВП, ЛЧМ) та визначення оптимальних параметрів сигнально-кодових конструкцій з урахуванням умов радіоелектронного впливу.

2. Вперше запропоновано багаторівневу модель захисту інформації, яка поєднує статистичне шифрування, завадостійке та таймерне кодування, декореляцію помилок з функціями шифрування й захисту від несанкціонованого доступу.

3. Удосконалено методи формування таймерних сигналів шляхом розроблення критеріїв вибору їх параметрів для забезпечення необхідного рівня завадостійкості, структурної прихованості та пропускної здатності інформаційно-комунікаційного каналу.

4. Вперше розроблено алгоритми розширення спектра таймерних сигналів і кореляційного прийому широкосмугових непозиційних сигналів, у яких враховано структуру сигнальної конструкції та особливості екстремального визначення значущих моментів відновлення інформації.

5. Обґрунтовано доцільність використання таймерних сигналів у системах спеціального зв'язку, що забезпечують підвищену енергетичну та структурну прихованість передавання конфіденційної інформації в умовах радіоелектронного конфлікту.

Значення результатів роботи для практики.

Практичне значення полягає у створенні нових методів і алгоритмів захисту інформації в інформаційно-комунікаційних системах, які поєднують статистичне шифрування, таймерне кодування та методи спектрального розширення сигналу. Реалізація таких підходів дозволяє формувати шумоподібні сигнали з підвищеними властивостями прихованості та завадостійкості, що є особливо важливим для систем передавання конфіденційних даних в умовах радіоелектронного впливу.

Розроблені алгоритми розширення спектра таймерних сигналів і кореляційного прийому можуть бути використані при побудові радіоканалів спеціального призначення, де висуваються підвищені вимоги до енергетичної ефективності та структурної прихованості сигналів.

Практична цінність роботи полягає у можливості застосування отриманих результатів для проектування та удосконалення комплексних систем технічного і криптографічного захисту інформації. Запропоновані підходи можуть бути інтегровані у сучасні засоби безпечного зв'язку, системи управління військового призначення, а також у захищені корпоративні мережі з адаптивним вибором параметрів передавання даних.

Оцінка структури та змісту дисертації, її завершеності, змісту реферату.

Дисертаційна робота Кільдішева В.Й. є завершеною науковою працею, в якій викладено нові науково обґрунтовані результати, отримані автором особисто. Перелік публікацій здобувача за темою дисертації, його особистий внесок у публікаціях зі співавторами, а також науково-практичне значення роботи ідентичні в дисертації та рефераті. Зміст реферату достатньо повно відображає основні положення, що викладені у дисертаційній роботі.

Робота складається зі вступу, шести розділів, висновків і двох додатків. Повний обсяг дисертації – 340 сторінок, з яких 291 сторінка основного тексту.

Перший розділ присвячено аналізу сучасного стану проблеми захисту інформації в інформаційно-комунікаційних системах, а також розгляду теоретичних основ побудови шумоподібних сигналів і методів розширення спектра. Узагальнено підходи до формування сигнально-кодових конструкцій, що забезпечують завадостійкість і структурну прихованість переданих даних.

Проведено критичний огляд існуючих рішень у сфері таймерного та завадостійкого кодування, що дозволило обґрунтувати вибір напрямів подальших досліджень і сформулювати наукову задачу підвищення захищеності каналів зв'язку в умовах радіоелектронного впливу.

У другому розділі здобувач запропонував математичні моделі процесів передавання інформації в умовах дії навмисних і випадкових завад, побудовані на основі моделей дискретних каналів Пуртова та Елліота–Гільберта. Виконано моделювання умов передавання сигнальних конструкцій при різних співвідношеннях сигнал/шум і ймовірностях помилки. Розроблено підхід до оцінювання параметрів завадостійкості, структурної прихованості та пропускної здатності системи. Запропоновано узагальнену модель таймерного каналу, яка враховує часову структуру сигналу та динаміку завад.

У третьому розділі здобувач описує дослідження процесів формування, передачі та прийому таймерних сигналів, а також впливу їх параметрів на якість передавання інформації. Розглянуто механізм J-кратного повторення сигнальних конструкцій для підвищення завадостійкості та достовірності прийому. Проведено аналіз ефективності такого підходу з позиції балансу між швидкодією системи та рівнем помилок. Наведено результати моделювання, що підтверджують доцільність використання таймерних сигналів у системах з розширеним спектром.

Четвертий розділ присвячено розробці багаторівневої моделі захисту інформації, у якій об'єднано статистичне шифрування, завадостійке кодування з функцією шифрування та таймерне кодування з функцією захисту від несанкціонованого доступу. Додатково реалізовано процедуру декореляції помилок для зменшення групування похибок при передачі сигналів. Проведено аналітичну оцінку криптостійкості системи та визначено умови, за яких багаторівневий підхід забезпечує необхідний рівень захисту в умовах радіоелектронного впливу.

У п'ятому розділі представлено результати дослідження параметричного перетворення даних на основі таймерних сигналів у задачі розширення спектра. Розглянуто вплив основних параметрів — інтервалу побудови сигналу, кількості найквістових інтервалів та бази елемента — на завадостійкість, структурну прихованість і пропускну здатність системи. Визначено оптимальні співвідношення параметрів для досягнення максимального рівня прихованості при допустимих втрат ах енергетичної ефективності. Наведено рекомендації щодо вибору параметрів таймерних сигналів для практичних застосувань.

Шостий розділ присвячений практичній реалізації запропонованих теоретичних і методичних рішень у системах зв'язку для передавання конфіденційної інформації. Розроблено структурні схеми передавача та приймача, описано алгоритми розширення спектра таймерних сигналів і кореляційного прийому. Запропоновано підходи до адаптивного налаштування параметрів системи залежно від рівня завад і пропускної здатності каналу. Наведено приклади практичного використання розроблених методів у реальних інформаційно-комунікаційних системах спеціального призначення.

Відповідність технічного та стильового оформлення встановленим вимогам.

Дисертаційна робота та реферат відповідають вимогам наукового стилю та загальноприйнятим нормам української мови. Текст роботи написано зрозуміло, коректно та з дотриманням вимог доцільності використання технічної і наукової термінології.

Дисертація та реферат написано з дотриманням вимог ДСТУ3008-2015 "Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлення", а також "Вимог до оформлення дисертації", затверджених наказом Міністерства освіти і науки України від 12.01.2017 р. № 40 та з урахуванням змін від 31.05.2019 р. №759.

Відповідність дисертації спеціальності.

Дисертаційна робота Кільдішева В.Й. за змістом повною мірою відповідає паспорту спеціальності 05.13.21 – Системи захисту інформації, формулі спеціальності та напрямкам досліджень за пунктами 1, 2 та 3.

Повнота оприлюднення результатів роботи в публікаціях та ступінь апробованості.

Основні результати дисертації Кільдішева В.Й. достатньо повно викладені у 44 наукових працях, до яких відносяться одна монографія, 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, а також 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.

Зауваження та дискусійні питання.

1. У запропонованій узагальненій моделі вдосконалення методів прихованого передавання інформації (п. 1.6, рис. 1.12) чітко простежується структура алгоритмів формування сигнально-кодових конструкцій. Водночас не зовсім зрозуміло, яким саме чином дана модель забезпечує можливість проведення порівняльного аналізу різних методів або визначення їх ефективності за узагальненими критеріями.

2. У другому розділі доцільно було б доповнити аналіз каналів Пуртова та Елліота–Гільберта кусково-стаціонарною моделлю, що дозволила б врахувати більшу кількість станів і підвищити точність моделювання в умовах радіоелектронного впливу.

3. У третьому розділі, де розглянуто застосування непозиційних таймерних сигнальних конструкцій для забезпечення структурної прихованості, відсутня кількісна оцінка впливу вибору значущих моментів модуляції на ймовірність виявлення сигналу засобами радіоелектронної розвідки.

4. У четвертому розділі, присвяченому побудові багаторівневої системи захисту інформації, доцільно було б подати порівняльний аналіз ефективності інтегрованого підходу (шифрування – кодування – таймерне перетворення) з традиційними схемами криптографічного захисту для оцінювання досягнутого рівня підвищення стійкості системи.

5. У п'ятому розділі під час дослідження параметрів таймерних сигналів у задачі розширення спектра подано обґрунтовані межі зміни параметрів m, s та i, які визначають компроміс між рівнем прихованості та завадостійкості системи. Водночас не наведено аналізу, який би дозволяв встановити граничні значення параметрів, за яких доцільно застосовувати той чи інший метод розширення спектра.

6. У пункті 6.2.2 дисертації не в повній мірі проаналізовано вплив параметрів m, s та i таймерних сигналів на автокореляційні та спектральні характеристики розширених сигнальних конструкцій. Доцільним було б доповнити дослідження оцінкою цих залежностей для повнішого обґрунтування ефективності методу.

Висновки.

Високо оцінюючи дисертаційну роботу Кільдішева В.Й. можна вважати її завершеною науковою працею на актуальну тему, що виконана автором самостійно та вирішує важливу науково-прикладну проблему. Робота має чітку

структуру, вагоме наукове та практичне значення, результати в достатній мірі опубліковані. Робота відповідає паспорту спеціальності 05.13.21 – "Системи захисту інформації" і вимогам, що висуваються до дисертаційних робіт, які подаються на здобуття наукового ступеня доктора наук. Зміст реферату відповідає змісту дисертації. Мета роботи досягнута, усі поставлені задачі виконано.

Вважаю, що дисертаційна робота Кільдішева Віталія Йосиповича на тему «Моделі та методи захисту інформації на основі параметричного перетворення передаваних сигнально-кодових конструкцій" відповідає вимогам пунктів 7, 8, 9 "Порядку присудження та позбавлення наукового ступеня доктора наук", а її автор, заслуговує присудження наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – "Системи захисту інформації".

Офіційний опонент
завідувач кафедри
кібербезпеки та програмного
забезпечення Центральноукраїнського
національного технічного університету
доктор технічних наук, професор Олексій СМІРНОВ

Підпис професора Смірнова О.А. засвідчую:
Проректор з наукової роботи та міжнародних зв'язків
Центральноукраїнського національного технічного університету,
кандидат технічних наук, доцент Андрій ТИХИЙ

"____" _____ 2025 року