ЗАТВЕРДЖЕНО

Ректор Державного університету
інтелектуальних технологій і зв'язку

_____ Олександр НАЗАРЕНКО

«06» 06 2025 р

ВИСНОВОК
про наукову новизну, теоретичне та практичне значення результатів докторської дисертації доцента кафедри кібербезпеки та технічного захисту інформації кандидата технічних наук, доцента Кільдішева Віталія Йосиповича на тему: «Моделі та методи захисту інформації на основі параметричного перетворення передаваних сигнально-кодових конструкцій» за спеціальністю 05.13.21 – системи захисту інформації

1. Призначені рішенням Вченої ради Державного університету інтелектуальних технологій і зв'язку (протокол № 3 від 29.05.2025 року) рецензенти, а саме:

– Василіу Євген Вікторович д.т.н., проф., декан факультету ІТК (д.т.н. зі спеціальності 05.13.21 – системи захисту інформації, професор за кафедрою Інформаційної безпеки та передачі даних);

– Гаджиєв Матін Магсуд огли д.т.н., проф. в.о. зав. кафедри ІПЗ (д.т.н. зі спеціальності 05.12.13 – радіотехнічні пристрої та засоби телекомунікацій, професор за кафедрою Кібербезпеки та технічного захисту інформації);

– Панченко Борис Євгенович д.ф-м.н., проф. професор кафедри ІПЗ (д.т.н. зі спеціальності 01.05.03 – програмне забезпечення обчислювальних машин та систем, професор за кафедрою Інженерії програмного забезпечення).

2. Розглянули:

Наукову новизну, теоретичне та практичне значення результатів докторської дисертації на тему «Моделі та методи захисту інформації на основі параметричного перетворення передаваних сигнально-кодових конструкцій» на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – Системи захисту інформації. Роботу виконано в Державному університеті інтелектуальних технологій і зв'язку Міністерства освіти і науки України. Науковий консультант – д.т.н., проф. Корчинський Володимир Викторович.

Тему дисертації «Моделі та методи захисту інформації на основі параметричного перетворення передаваних сигнально-кодових конструкцій» перезатверджено на засідані Вченої ради ДУІТЗ протокол № 4 від 01.07.2025 р.

3. Ухвалили:

Затвердити подальший текст висновку про наукову новизну докторської дисертації Кільдішева Віталія Йосиповича на тему: «Моделі та методи захисту інформації на основі параметричного перетворення передаваних сигнально-кодових конструкцій».

3.1 Актуальність теми

Розвиток системи захисту даних обумовлено зростаючими загрозами інформаційній безпеці, що пов'язано з розвитком засобів несанкціонованого доступу, методів радіотехнічної розвідки та соціальної інженерії. Це побуджає удосконалення методів захисту телекомунікаційних систем практично на всіх рівнях моделі OSI. Враховуючи сучасний стан

технічних можливостей засобів радіоелектронної протидії, особливу увагу потрібно зосередити на методах захисту інформації як на канальному, так і фізичному рівні, що важливо для систем безпроводового зв'язку, які є найбільш уразливими та вимагає використання шумоподібних сигналів.

Проблематикою використання шумоподібних сигналів (ШПС) для забезпечення захисту інформації на основі прихованості сигнально-кодових конструкцій були закладені такими науковцями, як Д. Агеєв, О. Котельников, К. Шеннон, З. Каневський, В. Литвиненко, М. Захарченко, Б. Радзимовський, М. Мазурков, В. Чечельницький, В. Гордійчук, А. Зюко, В. Банкет, В. Корчинський, О. Скопа, Н. Казакова та інші. Зазначені вище науковці внесли значний здобуток у питання розвитку забезпечення захисту інформації від НСД, проте існуючі методи формування ШПС, зокрема на основі псевдовипадкових послідовностей (Уолша, Голда, Касамі), не забезпечують достатнього рівня структурної прихованості, оскільки їхня структура є передбачуваною. Це знижує ефективність протидії засобам радіоелектронної розвідки та НСД, особливо у випадках застосування сучасних методів спектрального аналізу для виявлення та ідентифікації сигналів. З цього приводу доцільним є дослідження в напряму розробки таймерних шумоподібних сигналів, структура яких є більш складною. Крім того, на основі таймерних сигнальних конструкцій (ТСК) є можливість сумісно з розрядно-цифровим кодуванням вирішувати завдання по контролю достовірності передавання інформації, а також створювати алгоритми захисту повідомлень від НСД.

Таким чином, можна констатувати актуальність дисертаційної роботи, яке полягає у необхідності розробки та дослідження нових методів підвищення захищеності інформаційно-комунікаційних систем шляхом інтеграції методів кодування, шифрування та розширення спектра.

3.2 Ступінь обґрунтованості наукових положень, висновків та рекомендацій, сформульованих у дисертації:

Обґрунтованість і достовірність наукових положень, висновків та рекомендацій, сформульованих у дисертаційній роботі Кільдішева В. Й. «Моделі та методи захисту інформації на основі параметричного перетворення передаваних сигнально-кодових конструкцій» визначені наступним:

– аналітичні розрахунки базуються на фундаментальних положеннях теорій прихованості, криптографії, радіоелектронних систем і комплексів, моделювання складних систем, ймовірності;

– ефективність нових, одержаних автором роботи результатів дослідження підтверджуються розрахунками та результатами імітаційного моделювання.

3.3 Наукова новизна результатів отриманих автором дисертації

1) Уперше запропоновано модель оцінювання захищеності передачі інформації на основі обсягу сигналу, яка дозволяє наочно оцінювати відповідність характеристик сигналу можливостям каналу та приймати рішення щодо методів узгодження або параметричного перетворення сигналу. Це дозволяє здійснювати оцінку рівня захищеності за критеріями енергетичної, структурної та інформаційної прихованості відповідно до умов функціонування ІКС.

Уперше запропоновано узагальнену модель вдосконалення методів прихованого передавання інформації, яка дозволяє здійснювати порівняльний аналіз методів захисту за критеріями прихованості та завадостійкості.

2) Уперше запропоновано метод взаємного обміну якості та швидкості передавання інформації шляхом комбінованого застосування таймерних і позиційних кодів у нестаціонарних каналах зв'язку, що дозволяє підвищити захищеність та ефективність систем зв'язку в умовах радіоелектронного конфлікту.

3) Уперше запропоновано метод одночасного захисту інформації від НСД та випадкових завад у каналі зв'язку, що дозволило встановити залежність рівня структурної

прихованості ТСК та завадостійкості від мінімальної кодової відстані дозволених комбінацій, які визначаються як за рівнянням якості, так і шляхом повного перебору всіх можливих сигнальних конструкцій.

4) Уперше розроблено багаторівневу модель захисту інформації, яка забезпечує синергетичне поєднання статистичного шифрування, завадостійкого та таймерного кодування, а також процедури декореляції помилок. Такий підхід дозволяє одночасно на кожному рівні моделі підвищити криптостійкість, завадостійкість та захист від НСД. Обґрунтовано доцільність використання таймерних сигналів для компенсації надлишкових елементів, які виникають у процесі статистичного шифрування та завадостійкого кодування.

5) Уперше встановлено закономірності впливу параметрів ТСК на рівень структурної прихованості та завадостійкості шумоподібних сигналів. Розроблено критерії вибору параметрів, які забезпечують баланс між складністю реалізації, пропускною здатністю та прихованістю передавання даних. Виявлено протиріччя між прагненням до підвищення структурної прихованості шляхом збільшення параметра s та необхідністю його обмеження до оптимального значення $s_{опт}$, що визначається співвідношенням сигнал/шум у каналі.

6) Розвинуто теорію систем зв'язку з шумоподібними сигналами шляхом створення нових методів розширення спектра непозиційних сигналів на основі псевдовипадкового перескоку робочої частоти (ППРЧ), прямого розширення спектра псевдовипадковими послідовностями (ПРС-ПВП) та лінійної частотної модуляції (ЛЧМ) з визначенням оптимальних параметрів таймерних сигналів. Запропоновано умови забезпечення енергетичної прихованості для методів розширення спектра на основі критеріїв частотної та енергетичної ефективності використання каналу.

3.4 Апробація результатів

21 публікація опубліковані 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.

3.5 Практична значущість отриманих результатів

Практична значущість одержаних в дисертації результатів полягає в наступному:

– Розроблено алгоритм адаптивного обміну між завадостійкістю та швидкістю передавання залежно від стану нестаціонарного каналу зв'язку. Встановлено, що сумісне використання ТСК і РЦК дозволяє підвищити завадостійкість в 1,59 рази при зростанні відносної швидкості передавання від $R_{РЦК} = 0{,}55$ до $R_{РЦК\text{-}ТСК} = 1{,}05$, що водночас забезпечує зменшення часу передавання заданого обсягу інформації у два рази.

– Розроблено алгоритм підвищення структурної прихованості та завадостійкості шляхом формування ТСК із варіативним використанням параметрів n, i та s, що забезпечує збільшення кількості можливих реалізацій у 10 і більше разів порівняно з позиційними кодами. Встановлено залежність зменшення кількості реалізацій ТСК приблизно у 2, 7, 12 та 22 рази при збільшенні мінімальної кодової відстані $d_0 - 2,3,4,5$ відповідно. Виявлено зворотну залежність між показниками структурної прихованості та завадостійкості, що зумовлена зменшенням значення базового елемента побудови таймерного сигналу Δ.

– Розроблено багаторівневу модель системи захисту інформації на основі інтеграції стохастичного шифрування із завадостійким кодуванням, декореляцією помилок і таймерним кодуванням, у які додатково вбудовані механізми захисту від НСД. У межах реалізації стохастичного шифрування запропоновано алгоритм формування шифрограми шляхом добору випадкових кодових комбінацій з урахуванням імовірності появи символів у відкритому тексті. Показано, що при довжині випадкових комбінацій n=9, 10, …, 17 досягається зменшення дисперсії розподілу ймовірностей символів ($D_{x\gamma}$) до нуля, зокрема у 28, 47, … , 57269 разів, залежно від довжини комбінації. Це унеможливлює ефективне застосування частотного криптоаналізу при перехопленні повідомлень. Для компенсації надлишковості шифрограми, що виникає внаслідок стохастичного шифрування та блокового

кодування, запропоновано використовувати таймерні сигнали, які дозволяють оптимізувати тривалість передавання без втрати стійкості до атак.

– На основі встановлених закономірностей розроблено методику вибору параметрів таймерних сигналів для формування шумоподібних сигналів. Проведено аналіз впливу фіксованої кількості значущих моментів відновлення (ЗММ) у ТСК, який показав, що максимальна кількість реалізацій досягається при значенні параметра i, зазвичай на 2–4 одиниці меншим за m. Визначено, що зі зростанням інтервалу побудови сигналів (m = 6, 7, … , 19) структурна прихованість зростає (для прикладу при s = 7, i = 4 вона становить від 12 до 22 умовних одиниць). Показано можливість подвоєння структурної прихованості шляхом використання комбінацій з різними значеннями ЗММ i. Обґрунтовано вибір оптимального значення параметра s_o, який залежить від співвідношення сигнал/шум h у каналі й при якому забезпечується максимальна пропускна здатність $C_{\text{тск}}$ при одночасному досягненні заданого рівня прихованості. Встановлено, що надмірне зменшення часового інтервалу Δ при $s > s_{\text{опт}}$ призводить до збільшення показника втрат H_s, який характеризує рівень спотворених сигнальних конструкцій. Виявлено протиріччя між прагненням до підвищення структурної прихованості через збільшення s та необхідністю його обмеження до $s \le s_{\text{опт}}$ при фіксованому m і h.

– Розроблено нові алгоритми розширення спектра для таймерних сигналів (ППРЧ, ПРС-ПВП, ЛЧМ), які враховують структуру непозиційних сигнальних конструкцій. На відміну від відомих методів для позиційних кодів, запропоновані алгоритми забезпечують: розширення спектра на інтервалі всієї комбінації таймерних сигналів, що передбачає визначення кількості імпульсів розширення $N_{\text{тТСК}} = B_{t_o} \times m$ з урахуванням бази елемента Найквіста B_{t_o}; вибір параметрів (m, s, i) з урахуванням співвідношення сигнал/шум у каналі; формування широкосмугових сигналів зі спектральними характеристиками, придатними для застосування в реальних ІКС з підвищеними вимогами до завадостійкості та прихованості. Запропоновано комбінований метод розширення спектра таймерних сигналів на основі поєднання ПРС-ПВП та ППРЧ. Використання двох баз розширення спектра таймерного сигналу дозволяє істотно підвищити структурну прихованість сигнально-кодових конструкцій, рівень якої за криптостійкістю є співставним з протоколами шифрування DES та AES.

– Розроблено нові алгоритми кореляційного прийому широкосмугових таймерних сигналів (для ПРС-ПВП та ЛЧМ), які враховують структуру побудови непозиційних сигналів. Вони забезпечують прийняття рішень щодо значущих моментів відновлення фронтів в межах усієї сигнальної конструкції та передбачають використання кореляційного приймача з пристроєм визначення екстремумів напруги на виході інтегратора.

– Розроблено умови забезпечення енергетичної прихованості для методів розширення спектра – ППРЧ, ПРС-ПВП та ЛЧМ. Ці умови базуються на трьох критеріях: база сигналу $B = \Delta f T >> 1$; частотна ефективність $\gamma = R/\Delta f_{\text{еф}}$; енергетична ефективність і $\beta - R/h_0^2$. Аналіз показав, що методи ППРЧ та ЛЧМ задовольняють лише першу та другу умови, тоді як метод ПРС-ПВП – усі три, що свідчить про його перевагу з пог енергетичної прихованості. З урахуванням особливостей непозиційного характеру ТСК запропоновано принцип розширення спектра на інтервалі побудови сигнальної конструкції T_c, що забезпечує підвищену структурну прихованість у порівнянні з позиційними кодами (РЦК). Проведено кількісний аналіз впливу параметрів ТСК на структурну прихованість. Наприклад, при $m = 8$, $s = 5$, $i = 3$, базова структурна прихованість дорівнює $S_{\text{тск}} - 12$ дв.вим. Розширення спектра методом ПРС-ПВП із базою $B_{t_o} = 8$ і $N_{\text{пвп}} = 64$, а також застосування модуляції ФМ-2, дозволяє збільшити прихованість до $S_{\text{тск пвп}} = 77$ дв.вим. Подальше збільшення бази до $B_{t_o} = 16$ і $N_{\text{пвп}} = 128$ дозволяє досягти значення $S_{\text{тск пвп}} = 141$ дв.вим. Отже, структура ПВП після розширення спектра кожної ТСК стає унікальною, що значно ускладнює аналіз та ідентифікацію сигнальних конструкцій у каналі зв'язку.

3.6 Зв'язок з науковими програмами, планами й темами

Результати досліджень дисертаційної роботи увійшли до складу науково-технічних звітів з держбюджетних науково-дослідних робіт за темами: «Підвищення ефективності використання нестаціонарних каналів з базою ΔFt_0=1» (державний реєстраційний номер 0111U005680); «Ефективність систем інформаційної безпеки» державний реєстраційний номер 0111U007643); «Ефективність систем інформаційної безпеки» державний реєстраційний номер 0112U006815); «Підвищення ефективності використання нестаціонарних каналів з базою ΔFt_0=1» (державний реєстраційний номер 0112U006814); «Підвищення ефективності використання нестаціонарних каналів з базою ΔFt_0=1» (державний реєстраційний номер 0113U004750); «Ефективність систем інформаційної безпеки» (державний реєстраційний номер 0113U004749).

Методи дослідження

Для вирішення поставлених в дисертаційній роботі задач використано сукупність методів, прийомів та принципів наукового пізнання. Зокрема, були задіяні методи досліджень з теорій прихованості, криптографії, радіоелектронних систем і комплексів, моделювання складних систем, ймовірності, а також – застосовано методи математичного та імітаційного моделювання.

3.7 Особистий внесок автора

Всі дослідження з тематики дисертаційної роботи, автор виконав самостійно або спільно зі співавторами.

В [1, 7] автору належить розробка алгоритму розширення спектра таймерних сигналів, який полягає у використанні двох несучих частот ЛЧМ для позитивних та негативних імпульсів сигнальних конструкцій. В [2, 6, 8] автору належать спільні зі співавторами розробка та аналіз ефективності комбінованих методів захисту даних за допомогою стохастичного шифрування та таймерного кодування. В [3, 26, 29] автору належить аналіз ефективності застосування гомоморфних криптосистем у рекомендаційних системах веб-сервісів. В [4, 30] автору належить розробка алгоритму двійкової псевдовипадкової послідовності з підвищеною криптографічною стійкістю на основі програмних генераторів хаосу. В [5, 37, 42] автору належить статистичні дослідження генераторів хаосу та обґрунтування застосування їх у криптографічних системах. В [9, 13, 36, 39, 40] автору належать спільні із співавторами алгоритми розширення спектра таймерних сигналів на основі ППРЧ та формулювання висновків. В [10] автором надана оцінка енергетичної прихованості функціонування радіотехнічних систем на основі прямого розширення спектра таймерних сигналів. В [11, 12, 28] автору належать розрахунок енергетичної та структурної прихованості таймерних сигналів з урахуванням забезпечення заданої достовірності передавання даних. В [14] автору належать спільні із співавторами розробка системи оцінок для порівняльного аналізу методів підвищення енергетичної та структурної прихованості шумоподібних сигналів з урахуванням зміни частотної та енергетичної ефективності каналу. В [15] автору належать спільні із співавторами аналіз ефективності використання двосимвольних ансамблів у симплексних системах на базі коригувальних ТСК. В [16, 38, 41] автору належать спільні зі співавторами розробки алгоритмів мультиплексування імпульсів таймерних сигналів. В [16] автору належать розрахунки інформаційних параметрів кодів Сліпяна з компенсацією надлишковості таймерними сигналами. В [17, 27] автору належать спільні із співавторами розробка та аналіз методів підвищення прихованості передавання на основі розширення спектра непозиційних ТСК з використанням технологій FHSS і DSSS, а також розглядаються особливості використання кореляційного прийому шумоподібних таймерних сигналів. В [18] автору належать розрахунки та формулювання висновків, щодо ідентичності об'єктів інформаційної мережі як елементу моделі кібербезпеки. В [19] автору належать спільні із співавторами розробка методу підвищення прихованості сигнальних конструкцій передавання на основі

сумісного використання хаотичних та таймерних сигналів. В [20] автору належить розрахунок завадостійкості передавання даних при *j*-кратному повторенні надлишкових ТСК. В [21] автору належать спільні із співавторами аналіз та розрахунок завадостійкості в умовах впливу корельованих завад та аналіз пропускної здатності безперервного каналу зв'язку. В [22] автору належить аналіз завадостійкості і розрахунок компенсації надлишковості в блокових коректуючих кодах за рахунок ТСК та формулювання висновків. В [23] автору належать спільні із співавторами розробка моделі спільного використання системи виявлення й обробки атак із системою постійного аудиту інформаційної безпеки. В [24] автору належить розробка адаптивного алгоритму синтезу шумоподібних сигналів шляхом зміни параметрів ТСК у залежності від поточного стану каналу зв'язку. В [25] автором запропоновано систему оцінок захищеності методів захисту передаваної інформації в умовах РЕБ. В [28] автором запропонована методика підвищення структурної прихованості сигнальних конструкцій на основі сумісного використання ТСК і методів маніпуляції. В [31, 36, 43] автору належать спільні із співавторами розробка алгоритму підвищення прихованості передавання даних для системи з кодовим розділенням каналів на основі послідовностей динамічного хаосу. В [32] автору належать спільні із співавторами розробка методів підвищення структурної прихованості на основі шумоподібних таймерних сигналів. В [33] автором запропонована методика підвищення структурної прихованості даних на основі випадкового таймерного кодування. В [34] автору належать спільні із співавторами методика розробки комбінованого методу захисту інформації на основі сумісного використання завадостійкого кодування, таймерних сигналів і хаотичних реалізацій. В [35] автором надано аналіз умови забезпечення захищеності систем зв'язку спеціального призначення. В [44] автору належить аналіз доцільності застосування зворотного зв'язку в системах передачі даних та формування висновків дослідження.

3.8 Висновок про повноту опублікованих результатів.

За результатами дисертаційних досліджень було опубліковано 44 наукових праць, зокрема: 1 монографія [1], 22 статті [2-23], з яких 20 статей у фахових наукових журналах, що входять до переліку МОН України [2-4, 7-23], зокрема 1 стаття [2] в журналі, який цитується в наукометричній базі даних Scopus та 1 стаття [8] – у наукометричній базі даних Web of Science. Дві статті [5, 6] 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 [24-44], з яких 5 наукових праць [24, 27, 27, 28, 34] – 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.

СПИСОК ОСНОВНИХ РОБІТ АВТОРА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Сталий розвиток і цифрові інновації : монографія / за заг. ред. Буркинського Б. В. та ін.; НАН України, МОН України, ДУ «Ін-т ринку та екон.-екол. дослідж.», Держ. ун-т інтелект. технологій і зв'язку. Одеса : ДУ «ІРЕЕД НАНУ», 2024. 543 с.

2. Korchynskyi V., Hordiichuk V., Kildishev V., Riabukha O., Staikutsa S., Alfaiomi Kh. Method of information protection based on the integration of probabilistic encryption and noise immune coding. *Radioelectronic and Computer Systems*. 2023. Vol. 4, No. 13. P. 184-196.

3. Корчинський В. В., Кільдішев В. Й., Онищук В. В., Аль-Файюми Халед. Дослідження ефективності застосування гомоморфних криптосистем у рекомендаційних системах веб-сервісів. *Інфокомунікаційні та комп'ютерні технології*. 2021. № 2 (02). С. 195–201.

4. Korchynskyi V. V., Kildishev V. I., Alfaion K. та інші. A method for formation parameters of chaos generators based on hash functions. *Наукові праці ОНАЗ*. 2020. № 2. P. 65-69.

5. Korchynskyi V., Kildishev V., Riabukha O., Berdnikov O. The generating random sequences with the increased cryptographic strength. *Informatics, Automatics and Control Systems*. 2020. No. 1. P. 20-23. – DOI: 10.35784/iapgos.916 (Scopus).

6. Hordiichuk V., Shyshatskyi A., Korchynskyi V., Kildishev V. Timing pulse code modulation as a tool for quantization noise reduction in special-purpose IT systems. *Journal of Physics: Conference Series*. 2021. Vol. 1839. P. 1-10. DOI: https://doi.org/10.1088/1742-6596/1839/1/012005 (Scopus).

7. Korchynskyi V. V., Kildishev V. I., Berdnikov A. M., Smazhenko K. O. Increase of stealth transmission based on timer signals and linear frequency modulation. *Наукові праці ОНАЗ ім. О. С. Попова*. 2020. № 1. P. 53-57.

8. Korchynskyi V. V., Kildishev V. I., Holev D. V., Berdnikov O. M. Increasing the secrecy of transmission information based on combined random coding. *Radio Electronics, Computer Science, Control*. 2019. No. 3 (50). P. 108-116. (Web of Science).

9. Korchynskyi V. V., Kildishev V. I., Berdnikov A. M., Bielova I. V. Methods for generating noise-like timer signals based on pseudo-random tuning of the operating frequency. *Наукові праці ОНАЗ ім. О. С. Попова*. 2019. № 2. С. 98-103.

10. Korchynskii V. V., Kildishev V. I., Osadchuk E. A. The increase of transmission protection based on multiplexing of timer signal constructions. *Наукові праці ОНАЗ*. 2018. № 1. P. 93-97.

11. Корчинський В. В., Кільдішев В. Й., Осадчук К. О., Бердніков О. М. Дослідження енергетичної прихованості шумоподібних таймерних сигнальних конструкцій. *Вісник НТУ «ХПІ». Серія : Нові рішення в сучасних технологіях*. 2018. № 42 (1214). С. 126-130. DOI: https://doi.org/10.20998/2413-4295.2018.12.01.

12. Korchynskyi V. V., Kildishev V. I., Holev D. V., Berdnikov A. M. Research methods of increasing the security of information transfer based on timer signals. *Наукові праці ОНАЗ ім. О. С. Попова*. 2018. № 2. С. 109-115.

13. Корчинський В. В., Кільдішев В. Й., Бердніков О. М., Осадчук К. О. Підвищення захищеності системи зв'язку з таймерними сигнальними конструкціями та псевдовипадковою перебудовою робочої частоти. *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2017. № 2. С. 179-182.

14. Korchynskii V. V., Kildishev V. I., Berdnikov A. M. Methods for assessing the security of communication systems for special purposes. *Наукові праці ОНАЗ ім. О. С. Попова*. 2017. № 2. P. 101-107.

15. Захарченко М. В., Кільдішев В. Й., Голев Д. В., Толкачов А. В. Ефективність двосимвольних ансамблів у симплексних системах на базі коригувальних таймерних сигнальних конструкцій. *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2017. № 1. С. 215-218.

16. Захарченко М. В., Кільдішев В. Й., Голев Д. В., Осадчук К. О. Інформаційні параметри кодів Сліпяна з компенсацією надмірності таймерними сигналами. *Наукові праці ОНАЗ ім. О. С. Попова*. 2017. № 1. С. 14-20.

17. Korchynskii V. V., Osadchuk E. A., Kildishev V. I. Method of multiplexing of timer signal structures based on OFDM technology. *Вісник Національного університету «Львівська політехніка»*. 2017. № 2. P. 41-44.

18. Стайкуца С. В., Кільдішев В. Й. Ідентичність об'єктів інформаційної мережі як елемент моделі кібербезпеки. *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2016. № 2. С. 185-189.

19. Захарченко М. В., Корчинський В. В., Радзімовський Б. К., Кільдішев В. Й. Підвищення скритності передачі конфіденційної інформації на базі хаотичних сигналів та таймерних сигнальних конструкцій. *Східноєвропейський журнал передових технологій*. 2012. № 3/9 (57). С. 45-49. DOI: https://doi.org/10.15587/1729-4061.2012.4168.

20. Корчинський В. В., Кільдішев В. Й., Хомич С. В., Бєлова Ю. В. Ефективність *j*-кратного повторення надлишкових таймерних сигнальних конструкцій. *Вісник НТУ «ХПІ»*. 2012. Вип. 26. С. 88-95.

21. Захарченко М. В., Кільдішев В. Й., Бєлова Ю. В., Хомич С. В. Вплив корельованих завад на пропускну здатність безперервного каналу зв'язку. *Вісник НТУ «ХПІ». Серія : Нові рішення у сучасних технологіях.* 2012. Вип. 33. С. 62-68.

22. Захарченко М. В., Кільдішев В. Й., Хомич С. В., Пришляк О. Г. Компенсація надлишковості в блокових коректуючих кодах за рахунок таймерних сигналів. *Вісник Хмельницького національного університету*. 2011. Вип. 2. С. 175-181.

23. Шевцов Ю. С., Кононович В. Г., Кільдішев В. Й. Модель спільного використання системи виявлення і обробки атак із системою постійного аудиту інформаційної безпеки. *Вісник Східноукраїнського національного університету ім. В. Даля*. 2010. № 9 (151), ч. 1. С. 52-58.

Наукові праці, які засвідчують апробацію матеріалів дисертації

24. Hordiichuk V., Korchynskyi V., Kildishev V., Molodetskyi B., Staikutsa S., Alfaiomi K. Adaptive Synthesis of Wideband Timer Signals in the Conditions of Radio-Electronic Warfare. *2024 IEEE 17th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*. Lviv, Ukraine, 2024. P. 1–4. doi:10.1109/TCSET64720.2024.10755658. (Scopus).

25. Кільдішев В.Й. Система оцінок захищеності методів захисту інформації в умовах РЕБ. *Забезпечення кібероборони держави : збірник матеріалів IV наук.-практ. вебінару* (м. Київ, 10 листопада 2023 р.). Київ: НУОУ, 2023. С. 65-68.

26. Onyshchuk V., Kildishev V., Korchynskyi V., Alfaiomi K. Productivity of Modern Homomorphous Cryptosystems in Recommendation Systems of Web Services. *Proc. 16th Int. Conf. on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*. Lviv-Slavske, Ukraine, 22–26 Feb. 2022. P. 331-334. (Scopus).

27. Hordiichuk V., Korchynskyi V., Kildishev V., Zakharchenko M. Timer Signals Transmission Security Increase Based on Spectrum Spreading Methods. *2022 IEEE 2nd Ukrainian Microwave Week (UkrMW)*. Kyiv, 14-18 Nov. 2022. P. 331-334. (Scopus).

28. Корчинський В.В., Кільдішев В.Й., Аль-Файюми Х., Валігурський Ю.П. Підвищення прихованості передавання на основі таймерних сигнальних конструкцій і методів модуляції. *Перспективні напрямки захисту інформації: матеріали VII міжнар. наук.-практ. конф.* (м. Одеса, 30 серпня – 3 вересня 2021 р.). Одеса–Тернопіль: Крок, 2021. С. 31-33.

29. Korchynskyi V., Kildishev V., Golev D. Increase of Transmission Security Based on Timer Signal Construction. *2018 Int. Conf. on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo)*. Odessa, 10–14 Sept. 2018. P. 1-4. doi:10.1109/UkrMiCo43733.2018.9047554. (Scopus).

30. Корчинський В.В., Кільдішев В.Й., Онищук В.В., Аль-Файюми Х. Підвищення захищеності користувацьких даних веб-серверів шляхом впровадження гомоморфного шифрування. *Матеріали 75-ї наук.-техн. конф. професорсько-викладацького складу, науковців, аспірантів та студентів :* тези доповідей. Одеса: ОНАЗ, 2020. С. 132–133.

31. Korchynskyi V., Kildishev V., Berdnikov O., Valihurskyi Y., Polyshchuk K. The Methods of Forming Random Sequences Based on the Dynamic Chaos. *VIII Міжнародна наук.-практ. конф. «Фізико-технологічні проблеми передавання, оброблення та зберігання інформації в інфокомунікаційних системах»* (м. Чернівці, 3–5 жовтня 2019 р.). Чернівці, 2019. С. 26-29.

32. Корчинський В.В., Кільдішев В.Й., Бердніков О.М., Губін А.В. Системи радіозв'язку із шумоподібними таймерними сигналами. *Матеріали 73-ї наук.-техн. конф. професорсько-викладацького складу, науковців, аспірантів та студентів*, тези доповідей. Одеса: ОНАЗ, 2018. С. 134-136.

33. Корчинський В.В., Кільдішев В.Й., Голев Д.В. Прихованість та завадостійкість передачі інформації на основі випадкового таймерного кодування. *Матеріали 73-ї наук.-техн. конф. професорсько-викладацького складу, науковців, аспірантів та студентів :* тези доповідей. Одеса: ОНАЗ, 2018. С. 133-134.

34. Zakharchenko M., Korchynskyi V., Kildishev V. Integrated Methods of Information Security in Telecommunication Systems. *2017 Int. Conf. on Information and Telecommunication*

Technologies and Radio Electronics (UkrMiCo'2017). Odessa, 11–15 Sept. 2017. V.1. P. 78-81. (Scopus).

35. Корчинський В.В., Кільдішев В.Й. Захищеність систем зв'язку спеціального призначення. *П'ята міжнар. наук.-техн. конф. «Проблеми інформатизації»* (13-15 листопада 2017 р.). Черкаси: ЧДТУ, 2017. С. 18-19.

36. Корчинський В.В., Кільдішев В.Й. Підвищення прихованості передачі в системі зв'язку з кодовим розділенням каналів на основі динамічного хаосу. *XIX Міжнар. наук.-практ. конф. «Безпека інформації у інформаційно-телекомунікаційних системах»* (м. Буча, 25–26 травня 2017 р.). Буча: Держспецзв'язок, 2017. С. 48.

37. Корчинський В. В., Кільдішев В. Й., Бердніков О. М. Методи розширення спектру таймерних сигналів на основі псевдовипадкової перебудови робочої частоти. *Перспективні напрями захисту інформації : матеріали IV Всеукр. наук.-практ. конф.* (м. Одеса, 2–6 вересня 2017 р.). Одеса: ОНАЗ, 2017. С. 57-59.

38. Корчинський В.В., Кільдішев В.Й., Бердніков О.М., Валігурський Ю.П. Метод порівняльного аналізу генераторів псевдовипадкових чисел. *Перспективні напрями захисту інформації: матеріали IV Всеукр. наук.-практ. конф.* (м. Одеса, 2–6 вересня 2017 р.). Одеса: ОНАЗ, 2017. С. 46-48.

39. Корчинський В.В., Кільдішев В.Й., Осадчук К.О., Русаловська О.А. Підвищення захищеності передачі інформації на основі таймерних сигнальних конструкцій та технології OFDM. *Перспективні напрями захисту інформації : матеріали III Всеукр. наук.-практ. конф.* (м. Одеса, 2–6 вересня 2017 р.). Одеса: ОНАЗ, 2017. С. 39-42.

40. Кільдішев В.Й., Бердніков О.М., Степанов В.О. Підвищення захищеності системи зв'язку з ППРЧ на основі таймерних сигнальних конструкцій. *П'ята міжнар. наук.-техн. конф. «Проблеми інформатизації»* (м. Черкаси, 13–15 листопада 2017 р.). Черкаси: ЧДТУ, 2017. С. 17-18.

41. Корчинський В.В., Кільдішев В.Й., Бердніков О.М., Русаловська О.А. Спектральні методи захисту інформації на основі таймерних сигналів та псевдовипадкової перебудови робочої частоти. *Перспективні напрями захисту інформації : матеріали III Всеукр. наук.-практ. конф.* (м. Одеса, 2–6 вересня 2017 р.). Одеса: ОНАЗ, 2017. С. 36–39.

42. Корчинський В.В., Кільдішев В.Й., Бердніков О.М. Методи підвищення захищеності систем зв'язку на основі таймерних сигналів. *Матеріали 72-ї наук.-техн. конф. професорсько-викладацького складу, науковців, аспірантів та студентів :* тези доповідей. Одеса: ОНАЗ, 2017. С. 114-117.

43. Корчинський В.В., Кільдішев В.Й., Валігурський Ю.П., Поліщук К.В. Підвищення ефективності потокового шифрування в радіомережах на основі динамічного хаосу. *Матеріали 72-ї наук.-техн. конф. професорсько-викладацького складу, науковців, аспірантів та студентів :* тези доповідей. Одеса: ОНАЗ, 2017. С. 117-118.

44. Захарченко М.В., Корчинський В.В., Кільдішев В.Й. Про доцільність застосування зворотного зв'язку в системах передачі даних. *Матеріали 64-ї наук.-техн. конф. професорсько-викладацького складу, науковців, аспірантів та студентів* (м. Одеса, 1–4 грудня 2009 р.). Одеса: ОНАЗ, 2009. С. 78-80.

3.9 Відповідність змісту дисертації спеціальності, за якою вона подається до захисту

Зміст дисертаційної роботи Кільдішева В. Й. «Моделі та методи захисту інформації на основі параметричного перетворення передаваних сигнально-кодових конструкцій» відповідає паспорту спеціальності 05.13.21 – системи захисту інформації, за якою вона подається до захисту. Поставлені задачі, наукові положення, висновки, рекомендації, які наведені в роботі, в повному обсязі обґрунтовані та аргументовані.

3.10 Рекомендація дисертації до захисту

1. Дисертаційна робота Кільдішева В. Й. на тему: «Моделі та методи захисту інформації на основі параметричного перетворення передаваних сигнально-кодових конструкцій» за науковим рівнем, актуальністю та за практичною цінністю, обсягом і

оформленням відповідає вимогам які ставляться до робіт на здобуття наукового ступеня доктора наук, п.7 та п.9 Порядку присудження та позбавлення наукового ступеня доктора наук, затвердженого постановою Кабінету Міністрів України від 17 листопада 2021 р. № 1197.

2. Реферат дисертації повністю відповідає змісту дисертації.

Основні результати дисертації опубліковано у 44 наукових працях, у тому числі: 1 – монографія, 22 статті, з яких 20 статей у фахових наукових журналах, що входять до переліку МОН України, у тому числі 1 стаття у журналі, який цитується у наукометричній базі даних Scopus та 1 стаття [9] – у наукометричній базі даних Web of Science. Дві статті опубліковані в іноземних фахових виданнях, які цитуються у наукометричній базі даних Scopus. Апробація досліджень дисертації: 21 публікація опубліковані 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, 6 – звітів з НДР за спеціальною тематикою.

Дисертація відповідає паспорту спеціальності 05.13.21 – системи захисту інформації.

3. З урахуванням вищезазначеного рекомендувати дисертаційну роботу Кільдішева В. Й. на тему: «Моделі та методи захисту інформації на основі параметричного перетворення передаваних сигнально-кодових конструкцій» для подання до захисту у спеціалізовану Вчену раду за обраною спеціальністю.

4. Дисертація є закінченою науковою працею, у якій одержані нові наукові результати.

Рекомендацію ухвалено *одноголосно*.

Декан факультету ІТК:
д.т.н., проф. Євген ВАСІЛІУ

В.о. зав. кафедри ІПЗ:
д.т.н., проф. Матін ГАДЖИЄВ

Професор кафедри ІПЗ
д.ф-м.н., проф. Борис ПАНЧЕНКО