МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ І ЗВ'ЯЗКУ

Кільдішев Віталій Йосипович

УДК 004.056.53

МОДЕЛІ ТА МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ ПАРАМЕТРИЧНОГО ПЕРЕТВОРЕННЯ ПЕРЕДАВАНИХ СИГНАЛЬНО-КОДОВИХ КОНСТРУКЦІЙ

05.13.21 – системи захисту інформації

РЕФЕРАТ

дисертації на здобуття наукового ступеня
доктора технічних наук

Одеса – 2025

Дисертацією є рукопис

Робота виконана в Державному університеті інтелектуальних технологій і зв'язку

Науковий консультант – доктор технічних наук, професор
Корчинський Володимир Вікторович,
Державний університет інтелектуальних технологій і зв'язку, завідувач кафедри кібербезпеки та технічного захисту інформації

Офіційні опоненти:

член-кореспондент НАН України, Заслужений діяч науки і техніки України, лауреат Державної премії України в галузі науки і техніки,
доктор технічних наук, професор
Корченко Олександр Григорович,
Державний університет інформаційно-комунікаційних технологій, перший проректор

доктор технічних наук, професор
Смірнов Олексій Анатолійович,
Центральноукраїнський національний технічний університет, завідувач кафедри кібербезпеки та програмного забезпечення

доктор технічних наук, професор
Лахно Валерій Анатолійович,
Національний університет біоресурсів і природокористування України, професор кафедри комп'ютерних систем, мереж та кібербезпеки

Захист дисертації відбудеться 20 листопада 2025 р. о 12.00 год. на засіданні спеціалізованої вченої ради Д 41.113.03 в Державному університеті інтелектуальних технологій і зв'язку за адресою: 65023, м. Одеса, вул. Кузнечна, 1.

З дисертацією можна ознайомитись у науково-технічній бібліотеці Державного університету інтелектуальних технологій і зв'язку за адресою: 65023, м. Одеса, вул. Кузнечна, 1.

Реферат розісланий 17 жовтня 2025 р.

В.о. вченого секретаря
спеціалізованої вченої ради Матін ГАДЖИЄВ

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Актуальність теми дослідження зумовлена щораз більшими загрозами інформаційній безпеці, які пов’язані з розвитком засобів несанкціонованого доступу (НСД) та радіоелектронної розвідки (РЕР). Це створює потребу в удосконаленні методів захисту інформації на канальному та фізичному рівнях моделі OSI, особливо в інформаційно-комунікаційних системах (ІКС) із безпроводовим передаванням, які є найбільш вразливими до перехоплення та спотворення даних у середовищі радіоелектронного протиборства. Одним із перспективних напрямів захисту переданої інформації є застосування спектральних методів, зокрема розширення спектра вузькосмугового сигналу для підвищення прихованості передачі. Водночас для ефективного протистояння сучасним загрозам доцільним є використання комплексного підходу до захисту інтеграції, який передбачає інтеграцію різних методів перетворення сигнальних конструкцій – таких як шифрування, завадостійке кодування та спектральне розширення.

Теоретичні основи використання шумоподібних сигналів (ШПС) для забезпечення прихованості передавання сигнальних конструкцій були закладені провідними науковцями – Г. Найквістом, К. Шенноном, Р. Калманом, Е. Вітербі, І. Джейкобсом, Д. Купером та іншими. Разом із дослідженнями українських учених (В. Литвиненко, М. Захарченко, Б. Радзімовський, В. Гордійчук, А. Зюко, В. Банкет та інших) це створило підґрунтя для розвитку методів спектрального маскування переданої інформації. Однак наявні методи формування ШПС, зокрема на основі псевдовипадкових послідовностей (ПВП) (наприклад, Уолша, Голда, Касамі), не забезпечують достатнього рівня захисту, оскільки їхня структура є передбачуваною і піддається відновленню за допомогою кореляційного аналізу або статистичного спектрального моніторингу.

У цьому випадку утворюється протиріччя між забезпеченням ефективності протидії засобам РЕР та НСД і наявними методами розширення спектра. У зв’язку з цим виникає потреба в розробці нових методів генерації ШПС з більш складною та нестабільною структурою, низькою спектральною щільністю, що дозволить ускладнити їх виявлення навіть при використанні сучасних систем радіомоніторингу.

Перспективним підходом до забезпечення цілісності інформації є використання таких методів завадостійкого кодування, які можуть гарантувати як достовірність передавання, так і сприяти підвищенню захисту від НСД в складі комбінованих систем захисту. У цьому контексті доцільним є дослідження властивостей непозиційних сигналів, зокрема таймерних сигнальних конструкцій (ТСК), які були запропоновані М. Захарченком. Використання ТСК у поєднанні з розрядно-цифровим кодуванням (РЦК) дозволяє не лише здійснювати контроль достовірності передавання, але й розробляти алгоритми захисту інформації від НСД. Подальший розвиток технологій захисту інформації в умовах впливу завад і НСД можливий завдяки інтеграції різних методів перетворення даних: стохастичного шифрування, завадостійкого кодування та алгоритмів зменшення групування помилок у кодових блоках. Важливим напрямом дослідження для підвищення прихованості є розробка методів формування шумоподібних таймерних сигналів. Складність реалізації таких методів пояснюється непозиційністю імпульсних

складових ТСК, для яких непридатні класичні підходи до спектрального розширення, розроблені для позиційних кодів.

Отже, актуальність теми дослідження полягає в потребі створення та аналізу нових методів підвищення захищеності ІКС шляхом інтеграції методів кодування, шифрування та розширення спектра. Реалізація таких підходів сприятиме формуванню ефективних механізмів протидії сучасним загрозам інформаційній безпеці та забезпечить високий рівень конфіденційності, цілісності й доступності інформації в умовах дії радіоелектронних загроз.

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

Дисертаційна робота підготовлена у відповідності до основних положень Закону України «Про основні засади забезпечення кібербезпеки України», Закону України «Про захист інформації в інформаційно-комунікаційних системах», Стратегії кібербезпеки України. Тема дослідження пов’язана з науковими напрямами, сформульованими в п. 1.2.9 та п. 1.2.9.5 – теорія та комп’ютерні технології інформаційної безпеки "Основні наукові напрями та найважливіші проблеми фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук національної академії наук України на 2024–2028 роки", затверджених постановою Президії НАН України від 10.01.2024 №8, а також з напрямами, які корелюють із науково-технічними завданнями Постанови Кабінету Міністрів України № 942 від 7.09.2011 р. із змінами, внесеними постановою КМ № 463 від 9.05.2023 р. «Про затвердження переліку пріоритетних тематичних напрямів наукових досліджень і науково-технічних розробок на період до 2023 року» (Розділ «Інформаційні та комунікаційні технології», підрозділ «Інформаційно-комунікаційні та радіоелектронні системи та технології, засоби РЕБ для забезпечення національної безпеки і оборони. Інформаційна безпека та кібербезпека»). Тема роботи пов’язана з такими пріоритетними напрямами наукових досліджень у ДУІТЗ, як: теоретичні дослідження та розробка методів захисту інформації від НСД в ІКС і мережах; методи захисту передаваної інформації з використанням розширення спектра непозиційних сигналів; розробка методів захисту інформації на основі комбінованих методів перетворення даних з використанням стохастичного шифрування, завадостійкого кодування та хаотичних сигнальних конструкцій.

Результати досліджень дисертаційної роботи увійшли до складу науково-технічних звітів з держбюджетних науково-дослідних робіт за темами: «Підвищення ефективності використання нестаціонарних каналів з базою $\Delta Ft_0=1$» (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 $\Delta Ft_0=1$» (державний реєстраційний номер 0112U006814); «Підвищення ефективності використання нестаціонарних каналів з базою $\Delta Ft_0=1$» (державний реєстраційний номер 0113U004750); «Ефективність систем інформаційної безпеки» (державний реєстраційний номер 0113U004749).

Мета та завдання дослідження.

Метою дисертаційної роботи є розв’язання науково-технічної проблеми

підвищення захищеності передаваної інформації в інформаційно-комунікаційних системах шляхом розробки моделей та методів параметричного перетворення сигнально-кодових конструкцій, що забезпечують підвищену завадостійкість, прихованість та стійкість до несанкціонованого доступу.

Поставлена мета зумовила необхідність розв'язання таких завдань:

1) Розробити узагальнену модель захисту інформації на основі показників завадозахищеності (завадостійкості та прихованості) ІКС з урахуванням енергетичних, частотних та інформаційних ресурсів каналу зв'язку та граничних умов їх функціонування. На основі цієї моделі оцінити показники захисту інформації від НСД за критеріями енергетичної, структурної та інформаційної прихованості. Провести аналіз ефективності використання позиційних і непозиційних сигналів для формування шумоподібних сигнально-кодових конструкцій у комбінованих методах захисту інформації на основі інтеграції стохастичного шифрування, завадостійкого та таймерного кодування.

2) Оцінити ефективність сумісного використання таймерних і позиційних кодів для адаптації параметрів передавання сигнально-кодових конструкцій в ІКС, що функціонують в умовах нестаціонарного каналу зв'язку.

3) Проаналізувати ефективність застосування непозиційних ТСК для підвищення структурної прихованості та завадостійкості шляхом варіювання параметрів таймерного кодування. Виявити закономірності між рівнем структурної прихованості та завадостійкості на основі вибору оптимального значення параметра Δ як базового елемента формування ТСК, а також оцінити здатність таймерного кодування до виявлення та виправлення спотворень у сигнально-кодових конструкціях.

4) Розробити багаторівневу систему захисту інформації, яка забезпечує синергетичне поєднання статистичного шифрування, завадостійкого, таймерного кодування та декореляції помилок. Оцінити ефективність використання таймерних сигналів для компенсації надлишкових елементів, які виникають у процесі статистичного шифрування та завадостійкого кодування.

5) Провести аналіз впливу параметрів ТСК на рівень структурної прихованості та завадостійкості шумоподібних сигналів. Запропонувати критерії вибору параметрів ТСК з урахуванням складності їх реалізації, а також вимог до забезпечення прихованості та завадостійкості.

6) Дослідити та оцінити методи синтезу шумоподібних сигналів на основі ТСК з використанням різних підходів до спектрального розширення. Розробити умови забезпечення енергетичної прихованості для обраних методів. Запропонувати алгоритми розширення спектра із застосуванням ТСК та сформувати методику обчислення показників структурної прихованості шумоподібних сигналів.

Об'єктом дослідження є процеси формування та інтеграції методів захисту інформації в сигнально-кодових конструкціях для забезпечення прихованості під час передавання в інформаційно-комунікаційних системах.

Предметом дослідження є методи та алгоритми параметричного перетворення сигнально-кодових конструкцій, спрямовані на підвищення прихованості та завадостійкості передавання інформації в умовах радіоелектронного конфлікту.

Методи дослідження. У дисертаційній роботі використано сукупність методів і прийомів, заснованих на принципах системного аналізу, формалізації та моделювання. Зокрема, дослідження базуються на методах, що ґрунтуються на теоріях прихованості, криптографії, радіоелектронних систем і комплексів, теорії ймовірностей та моделювання складних систем. Для перевірки гіпотез і оцінювання ефективності запропонованих рішень застосовано аналітичне та імітаційне моделювання.

Наукова новизна одержаних результатів. Наукова новизна одержаних результатів полягає у вирішенні важливої науково-прикладної проблеми підвищення захищеності ІКС шляхом розробки нового теоретичного підходу до інтеграції методів параметричного перетворення сигнально-кодових конструкцій. Запропоновано концепцію сумісного використання непозиційних таймерних сигналів, методів розширення спектра, стохастичного шифрування, завадостійкого кодування та алгоритмів декореляції помилок з метою зниження спотворення кодових блоків.

Наукова новизна одержаних результатів полягає в такому:

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 $s_{\text{опт}}$, 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.

Практичне значення одержаних результатів полягає в тому, що:

– 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 $R_{\text{РЦК}} = 0{,}55$ до $R_{\text{РЦК-ТСК}} = 1{,}05$, 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 47, 28, … , 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 $H_{\text{з}}$, 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 $N_{\tau\text{ТСК}} = B_{t_0} \times m$ з урахуванням бази елемента Найквіста B_{t_0}; 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 приховність 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 приховність у порівнянні з позиційними кодами (РЦК). Проведено кількісний аналіз впливу параметрів ТСК на структурну приховність. Наприклад, при $m = 8$, $s = 5$, $i = 3$, базова структурна приховність дорівнює $S_{\text{тск}} = 12$ дв.вим. Розширення спектра методом ПРС-ПВП із базою $B_{t_0} = 8$ і $N_{\text{пвп}} = 64$, а також застосування модуляції ФМ-2, дозволяє збільшити приховність до $S_{\text{тск пвп}} = 77$ дв.вим. Подальше збільшення бази до $B_{t_0} = 16$ 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.

Одержані в роботі наукові і практичні результати знайшли впровадження в діяльності, що підтверджено відповідними актами 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».

Особистий внесок здобувача. Усі результати наукових, теоретичних і практичних досліджень, які викладено в дисертації, отримано автором самостійно.

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.

Апробація результатів дисертації. Основні наукові результати дисертаційної роботи доповідались на 21-му міжнародному та всеукраїнському симпозіумі, науково-практичній та науково-технічній конференціях [24–44] у таких містах: Київ, Одеса, Славськ, Львів, Чернівці, Черкаси, Буча.

Публікації. За матеріалами дисертаційної роботи 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.

Структура й обсяг роботи. Робота складається зі вступу, шести розділів, висновків, списку використаних джерел та додатків. Загальний обсяг роботи становить 340 сторінок, із них 291 − основного тексту з 65 рисунками та 36

таблицями, список використаних джерел нараховує 154 найменувань на 19 сторінках, 8 сторінок додатків.

ОСНОВНИЙ ЗМІСТ ДИСЕРТАЦІЙНОЇ РОБОТИ

У вступі розкрито сутність і стан наукової проблеми та обґрунтовано її актуальність, визначено мету роботи й коло вирішених завдань, показано наукову новизну та практичну значущість одержаних результатів, наведено інформацію про особистий внесок здобувача, апробацію та впровадження наукових результатів роботи.

У першому розділі – «Стан проблеми забезпечення захищеності інформаційно-комунікаційних систем у сучасних умовах. Вибір напрямків досліджень» – проведено аналіз наукових джерел за темою дисертаційного дослідження, що дало змогу оцінити стан забезпечення захищеності ІКС з позицій теорії завадостійкості, прихованості, криптографії, а також ефективності функціонування каналів зв'язку згідно з підходами А. Зюко та інших дослідників. Обґрунтовано доцільність розробки узагальненої моделі захисту інформації, що дозволяє оцінювати рівень завадозахищеності ІКС з урахуванням ресурсів каналу зв'язку та граничних умов його функціонування.

У роботі підкреслюється необхідність комплексного підходу до захисту інформації, що охоплює кілька рівнів моделі OSI – фізичний, канальний та інші. Також, досліджуються задачі забезпечення завадозахищеності каналів зв'язку в умовах РЕБ, де важливим є здатність систем протидіяти засобам РЕР та НСД. Визначено, що ефективність таких систем зростає при реалізації багаторівневого захисту переданої інформації, в основі якого – сигнально-кодові перетворення з використанням методів шифрування, завадостійкого та таймерного кодування.

Запропоновано модель системи оцінок параметрів захищеності сигналів, що містить критерії завадостійкості, енергетичної та структурної прихованості. Проведено аналіз впливу методів підвищення прихованості на завадостійкості передачі інформації в каналі, з урахуванням зміни частотної та енергетичної ефективності.

Реалізація багаторівневої моделі захисту інформації охоплює декілька рівнів сигнального перетворення та дає змогу суттєво підвищити загальну захищеність системи зв'язку. В умовах радіоелектронного конфлікту важливим є забезпечення кожного рівня захисту відповідними методами формування СКК і перетворення даних. При виборі таких методів доцільно враховувати взаємозалежність між показниками завадостійкості, енергетичної, структурної та інформаційної прихованості, а також характер ведення РЕБ і можливі дії протиборчої сторони. Отже, пошук ефективної системи оцінювання методів захисту інформації з урахуванням взаємозв'язку між критеріями завадозахищеності та прихованості є важливим і актуальним науковим завданням, вирішення якого потребує побудови узагальненої моделі захисту для ІКС.

Система оцінювання захищеності методів захисту інформації має ґрунтуватися на критеріях ефективності, що відображають здатність протидіяти засобам РЕР і НСД. У межах РЕБ можуть реалізовуватися різні сценарії впливу на системи зв'язку спеціального або критичного призначення. Залежно від складності сценарію дій противника на етапі проєктування ІКС доцільно впроваджувати різні

види прихованості: енергетичну (ослаблення сигналу до рівня нижчого за чутливість засобів виявлення), структурну (ускладнення аналізу сигнальної структури), та інформаційну (захист змісту за допомогою шифрування). Усі ці аспекти мають бути інтегровані в узагальнену модель захисту, що базується на параметричному перетворенні сигнально-кодових конструкцій.

Енергетична прихованість забезпечується завдяки використанню сигнально-кодових конструкцій, які мають властивості маскування, що ускладнює їх виявлення засобами РЕР в радіоканалі. Для цього застосовуються методи параметричного перетворення вузькосмугових сигналів, зокрема: ППРЧ, пряме розширення спектра ПРС ПВП, ЛЧМ, а також комбіновані методи розширення спектра. У результаті вузькосмуговий сигнал із базою $B_y \approx 1$ перетворюється на широкосмуговий з базою $B_{\text{ш}} >> 1$. Маскувальний ефект досягається, коли амплітуда або спектральна щільність корисного сигналу знижується до рівня шуму в каналі, що робить його виявлення ускладненим.

Оцінимо взаємозв'язок між умовою забезпечення необхідної достовірності передачі і енергетичної прихованості сигнальних конструкцій для методу прямого розширення спектра ПВП. Розглянемо теорему Шеннона про пропускну спроможність каналу:

$$C = \Delta F \log_2 \left(1 + \frac{P_{\text{с}}}{P_{\text{ш}}}\right) \tag{1}$$

де ΔF – смуга частот, яка призначена для передавання даних; $P_{\text{с}}$ – потужність сигналу на виході передавача; $P_{\text{ш}}$ – потужність завади в каналі.

З виразу (1) випливає, що теоретично передавання інформації в каналі зв’язку можливе з будь-якою швидкістю, що не перевищує пропускну здатність, і з будь-якою заданою достовірністю. Водночас забезпечення енергетичної прихованості можливе за таких умов:

$$\begin{cases} B_{\text{ш}} = T\Delta F \to \infty \\ P_{\text{с}}/P_{\text{ш}} \to 1 \end{cases} \tag{2}$$

та

$$P_{\text{с}}/P_{\text{ш}} \leq 1. \tag{3}$$

При виконанні (3) передавання здійснюється сигнальними конструкціями, рівень яких не перевищує потужність фону або змінюється за частотою настільки динамічно, що унеможливлює їхнє надійне виявлення засобами радіотехнічної розвідки (РТР). У такому випадку сигнал набуває властивостей малопомітності, що є ознакою реалізації максимальної енергетичної прихованості.

Водночас реалізація умов (2) та (3) має сенс лише за умови дотримання необхідної завадостійкості та мінімально допустимої швидкості передавання. Це вимагає побудови узагальненої моделі захисту інформації, яка дозволяє одночасно враховувати достовірність, енергетичну прихованість та ефективність використання каналу зв’язку.

Теорема. Існує взаємозв'язок між завадостійкістю передавання даних і умовами забезпечення енергетичної прихованості сигнальних конструкцій (2) і (3).

Доведення. Розглянемо другу частину теореми Шеннона, відповідно до якої для будь-якого рівня достовірності передавання існує код, що забезпечує завадостійку передачу даних із імовірністю помилки, близькою до нуля, за умови:

$$R < C = \Delta F \log_2 \left(1 + \frac{P_с}{P_ш}\right),$$

де R – швидкість передавання.

Нехай для розширення спектра сигналу використовується ПВП, яка представлена у вигляді двійкового завадостійкого коду з параметрами:

$$n = k + r, \tag{4}$$

де k та r – кількість інформаційних і перевірочних елементів відповідно.

Відповідно до теореми Шеннона про кодування, якщо:

$$n \to \infty \tag{5}$$

то й $k \to \infty$, але повільніше зростає лише r, що призводить до: зменшення частки контрольних елементів; зростання коригувальної здатності коду; збільшення достовірності передавання. Для наочності в табл. 1 наведено параметри циклічного коду.

Припустимо, що збільшення довжини кодового блоку n на інтервалі часу $T = nt_0$ здійснюється за рахунок зменшення тривалості одного елемента:

$$t_0 > t_0^*, \tag{6}$$

де t_0^* – тривалість елемента після кодування. З урахуванням кодової швидкості $\gamma_к = k/n$, отримаємо:

$$t_0^* = \gamma_к t_0. \tag{7}$$

Зменшення тривалості імпульсу призводить до зменшення енергії одного елемента сигналу, а отже – до зменшення помітності сигналу в радіоканалі (підвищення енергетичної прихованості).

Разом із цим, швидкість передавання при розширенні спектра падає в n/k разів, що, однак, компенсується зростанням достовірності при необмеженій смузі частот $\Delta F \to \infty$. Зі збільшенням n кодова швидкість

$$\gamma_к \to 1, \tag{8}$$

водночас база ШПС збігається з довжиною послідовності, тобто:

$$B_ш = n \to \infty. \tag{9}$$

Таблиця 1 - Параметри циклічного коду

№	n	k	r	d_0	γ_k
1	7	4	3	3	0,571
2	15	11	4	3	0,733
3	31	21	10	5	0,733
4	63	45	18	7	0,714
5	127	99	28	9	0,779
6	255	215	40	11	0,843
7	511	430	261	19	0,841

Таким чином, при збільшенні бази широкосмугового сигналу $B_ш$, що відповідає умові (2), забезпечується одночасне зростання достовірності передавання та енергетичної прихованості. Умова (3), тобто $P_с/P_ш \leq 1$, при цьому виконується внаслідок зменшення енергії кожного імпульсу при збереженні або підвищенні рівня достовірності.

Отже, виконання умов (2) та (3) вимагає застосування завадостійкого кодування великої довжини (із зростаючим n) та зменшення амплітуди елементів

сигналу, що призводить до реалізації: високої енергетичної прихованості (сигнал зливається з фоновим шумом); високої достовірності (через підвищення завадостійкості). Це й треба було довести.

У реальних системах зв'язку з кодовим розділенням каналів в якості дозволених комбінацій для розширення спектра вузькосмугового сигналу використовуються ортогональні ПВП, наприклад, Уолша, кількість яких можна порівняти з базою сигналу $B_{\text{ш}}$. З усієї загальної безлічі комбінацій $N_{\text{заг}} = 2^n$ вибирається тільки $N_{\text{р}} = n - 1$ взаємно-ортогональних ПВП. Кодова відстань між будь-якою парою послідовності Уолша, на відміну від циклічних кодів, відповідає фіксованому значенню:

$$d_0 = n/2. \tag{10}$$

що забезпечує здатність виявлення до $t_0 = d_0 - 1$ помилок. Теоретично це означає, що при кореляційному прийомі правильне розпізнавання ПВП можливе за умови, що кількість спотворених бітів t_0^* не перевищує половини довжини послідовності, тобто $t_0^* \leq n/2$. Виявлення сигналу засобами РЕР свідчить про подолання рівня захисту каналу на фізичному рівні, тобто про порушення умов енергетичної прихованості. У разі реалізації другого сценарію протидії, спрямованого на розкриття змісту перехопленого повідомлення, необхідним є попереднє розпізнавання структури сигнальних конструкцій. Структурна прихованість визначається кількістю двійкових вимірювань, які необхідно виконати для встановлення структури сигналу:

$$S = \log_2 A, \tag{11}$$

де A – потужність ансамблю реалізацій, що визначається кількістю усіх можливих комбінацій параметрів сигнально-кодової конструкції (СКК). До таких параметрів належать: несуча частота, тип модуляції, структура кодування, час надходження сигналу, фазові та частотні зсуви тощо. Отже, структурна прихованість тісно пов’язана з методами побудови сигнальної структури: чим більше змінних параметрів у СКК, тим вищий ступінь їхньої прихованості. Для підвищення структурної прихованості передавач має формувати максимально широкий ансамбль сигналів зі змінними в часі характеристиками. Збільшення кількості реалізацій можливе, зокрема, шляхом використання складніших видів модуляції, таких як BPSK (ФМ-2), 4-QAM, 8-QAM, 16-QAM, 32-QAM тощо. На рис. 1 представлено залежність структурної прихованості від ступеня позиційності СКК M. Зрозуміло, що підвищення структурної прихованості за рахунок ускладнення сигнальних конструкцій призводить до перерозподілу ресурсів каналу зв’язку. Перехід до багатопозиційних систем модуляції покращує частотну ефективність:

$$\gamma = R/\Delta F, \tag{12}$$

однак супроводжується зниженням енергетичної ефективності:

$$\beta = R/h_0^2, \tag{13}$$

де R – швидкість передавання інформації, $h_0^2 = P_s/N_0$ – відношення середньої потужності сигналу до спектральної щільності адитивного білого гаусового шуму N_0.

Для оцінки впливу перерозподілу ресурсів на завадостійкість і структурну прихованість було проведено імітаційне моделювання сигналів типу BPSK, 8-QAM,

16-QAM, 32-QAM у каналі з АБГШ. Результати, представлені на рис. 2, демонструють залежність імовірності помилки на біт p_0 від h_0^2.

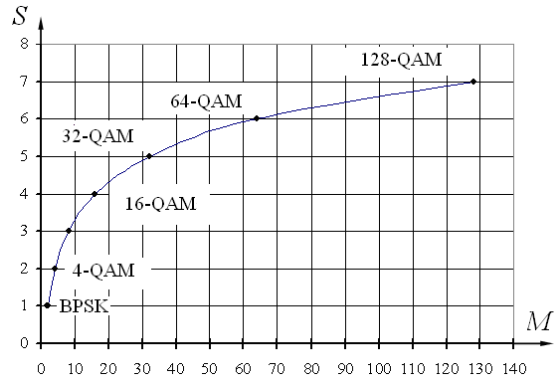

Рисунок 1 - Залежність структурної прихованості систем модуляції

Аналіз результатів показав, що складніші види модуляції забезпечують вищу швидкість передавання, однак зменшують завадостійкість сигналу. Водночас багатопозиційні модуляції сприяють зростанню структурної прихованості сигнальних конструкцій за рахунок збільшення ансамблю реалізацій.

Подальше підвищення структурної прихованості можливе шляхом ускладнення форми модулюючого сигналу. У цьому контексті доцільно застосовувати ТСК, які поєднуються з методами модуляції та розширення спектра. Зазвичай захищеність на основі енергетичної прихованості реалізується саме через розширення спектра вихідного сигналу, що, як уже зазначалося, веде до зниження частотної ефективності каналу. Вочевидь, що взаємозалежність між показниками енергетичної та частотної ефективності каналу створює можливість для оптимізації процесу підвищення енергетичної прихованості сигнальних конструкцій. Крім того, застосування широкосмугових сигналів сприяє покращенню електромагнітної сумісності систем радіозв'язку з іншими передавальними пристроями.

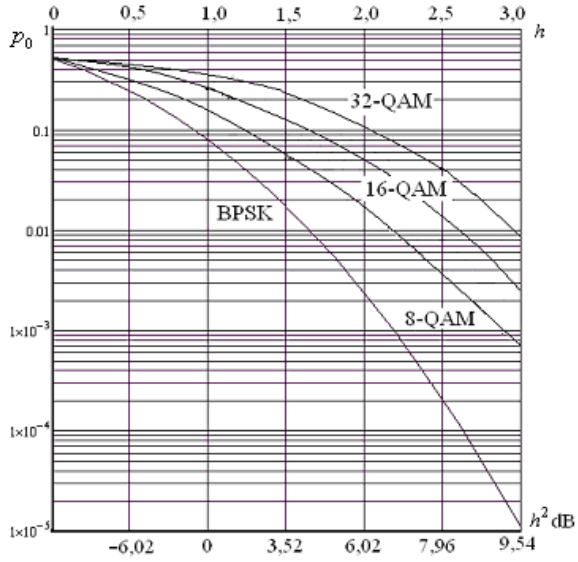

Рисунок 2 - Залежності ймовірності помилок систем з BPSK, 8-QAM, 16-QAM, 32-QAM від h_0^2

Узагальнена модель оцінювання захищеності методів передавання інформації передбачає кількісне оцінювання рівня захищеності в завадозахищених ІКС на основі системи показників, яка враховує витрати енергетичних, частотних та інформаційних ресурсів каналу зв'язку, зокрема за такими критеріями:

1) максимальна енергетична прихованість досягається в того методу передавання, який за заданої смуги широкосмугового сигналу ΔF та необхідного рівня достовірності забезпечує мінімальне відношення сигнал/шум h_0^2:

$$\min h_0^2 = E\{\Delta F; P_{\text{НП}}(n)\}, \qquad (14)$$

де $P_{\text{НП}}(n)$ – ймовірність невиявленої помилки в кодовому блоці довжини n; символ $E\{\cdot\}$ позначає функціональну залежність рівня прихованості від параметрів;

2) максимальна структурна прихованість досягається у того методу формування сигнальних конструкцій, який протягом заданого інтервалу побудови сигналу $T_{\text{СК}}$ та при забезпеченні необхідної достовірності дозволяє сформувати найбільший ансамбль реалізацій A:

$$\max A = S\{T_{\text{СК}}; P_{\text{НП}}(n)\}. \quad (15)$$

Формули (14) та (15) свідчать, що суттєвий потенціал зростання прихованості радіотехнічних об’єктів досягається шляхом комбінування параметрів сигналів у частотно-часовому просторі, що дозволяє застосовувати спектральні методи захисту інформації з використанням складних СКК і великих баз ШПС $B_{\text{ш}}$. Запропонована модель дозволяє здійснювати порівняльний аналіз методів захисту за критеріями прихованості та завадостійкості з урахуванням витрат канальних ресурсів, що є ключовим для побудови ефективних захищених каналів зв’язку в умовах радіоелектронної протидії.

Отже, на підставі проведеного аналізу сформульовано основні напрями подальших досліджень, обґрунтовано критерії та показники ефективності методів захисту інформації в умовах радіоелектронного конфлікту. На цій основі здійснено математичну формалізацію наукової проблеми, що полягає в забезпеченні комплексної захищеності ІКС шляхом інтеграції методів кодування, шифрування та розширення спектра сигналу.

У другому розділі – «Підвищення завадостійкості передавання даних на основі сумісного використання блокових завадостійких кодів та таймерних сигналів у системах захисту інформації» – проведено аналіз якості та швидкості передавання даних у нестаціонарному каналі. Розглянуто можливість адаптивного обміну між якістю і швидкістю передавання залежно від поточного стану каналу. Зокрема, проаналізовано ефективність реалізації такого обміну в інтервалах «хорошого» стану каналу за допомогою ТСК із подальшим відновленням якості передачі шляхом використання розрядно-цифрових кодів.

Розв’язання задачі підвищення достовірності передачі в таких умовах здійснюється двома підходами: застосуванням надлишкових кодів (у системах із прямим каналом) та використанням адаптивних методів (у системах зі зворотним зв’язком). Відомі методи визначення параметрів завадостійкого коду здебільшого спрямовані на пошук оптимальної надлишковості для забезпечення заданого рівня вірності приймання. Проте навіть мінімально припустиме значення надлишковості розрядно-цифрових кодів призводить до зменшення швидкості передавання в каналі. Проведений аналіз показує, що при виборі параметрів завадостійкого коду часто не враховується наявний запас завадостійкості у бінарних системах передавання, який притаманний реальним каналам зв’язку.

Для виконання поставленого завдання була обрана модель Елліота–Гільберта, яка описує нестаціонарний канал зв’язку у вигляді двох станів: «хорошого» та «поганого». Такий підхід є обґрунтованим з погляду функціонування систем радіозв’язку в умовах дії засобів РЕР. У «хорошому» стані каналу ймовірність вірного приймання даних на кілька порядків перевищує середню ймовірність помилки, тоді як у «поганому» стані вона наближається до 0,5, що свідчить про повне глушіння каналу. Зазвичай канал перебуває в «хорошому» стані до 98–99% часу, тоді як «поганий» стан спостерігається лише 1–2% часу.

Наприклад, при співвідношенні сигнал/шум $h \geq 10$ у «хорошому» стані, ймовірність бітової помилки становить $p_{\text{х}} \leq 10^{-9}\ldots10^{-8}$, що забезпечує значний запас завадостійкості відносно середнього значення помилки $\bar{p}_{\text{е}}$. Водночас, якщо в «поганому» стані (з питомою вагою $\gamma_{\text{п}} = 0{,}01$) ймовірність помилки становить $p_{\text{п}} =$

0,5, а в «хорошому» стані $\gamma_х = 0{,}99$ та $p_х < 10^{-8}$, то середня ймовірність помилки в каналі: $\bar{p}_е = \gamma_х \cdot p_х + \gamma_п \cdot p_п = 0{,}99 \cdot 10^{-8} + 0{,}01 \cdot 0{,}5 \approx 5 \cdot 10^{-3}$ визначається "поганим" станом. При цьому вибір надлишковості коду доцільно здійснювати або з урахуванням найгіршого стану каналу, або на основі середньої ймовірності помилки в нестаціонарному середовищі. Оцінимо можливість збільшення швидкості передавання інформації в реальному каналі. Якщо алфавіт каналу має розмірність "a" станів, то на інтервалі тривалості $T_с = mt_0$ може існувати $N_р = a^m$ реалізацій.

Збільшення кількості реалізацій сигнальних конструкцій можливе за рахунок зменшення мінімальної відстані між ЗММ у каналі з базою, що дорівнює одиниці, тобто за рахунок підвищення швидкості передавання вище класичної межі Найквіста. Прикладом такого підходу є ТСК, у яких відстань між ЗММ не менша за найквістовий інтервал $t_0 = 1/\Delta F$, однак вона не є кратною цьому інтервалу. Замість цього відстань обирається кратною деякому підінтервалу $\Delta = t_0/s$, де ($s \in 2, 3, \ldots k$). Загальна відстань між ЗММ тоді визначається як $\tau_с = t_0 + \Delta i$. Значення s вказує, наскільки зменшується інтервал Δ відносно базової тривалості t_0. Така форма організації ЗММ дозволяє ефективно усунути міжсимвольні спотворення (МСС) при збільшенні швидкості передавання інформації, що ілюструє перевагу використання ТСК для побудови завадостійких систем зв'язку.

При використанні РЦК збільшення пропускної здатності досягається шляхом ущільнення енергетичної відстані сусідніх сигнальних станів модуляції інформаційного параметра a_k (фаза, амплітуда, частота) на інтервалі Найквіста t_0, що описується залежністю:

$$C = \log_2 a_k. \tag{16}$$

Зменшення енергетичної відстані між дозволеними ТСК дозволяє збільшити кількість реалізацій на інтервалі їх побудови $T_с$, що призводить до зростання пропускної здатності передавання інформації. Кількість дозволених реалізацій ТСК з i-фронтами дорівнює:

$$N_p = C^i_{ms-i(s-1)} \times (a_k - 1)^i. \tag{17}$$

Максимальна кількість інформації, що передається при цьому складає:

$$J_{\max} = \log_2 C^i_{mS-i(S-1)} + i \log_2 (a_k - 1), \tag{18}$$

де $i = 1, \ldots, m$ – кількість ЗММ. При значенні a_k=2 права частина виразу (18) буде дорівнювати нулю і перетворюється у вираз (16). Сумарна кількість реалізацій $N_{p\Sigma}$ складає:

$$N_{p\Sigma} = \sum_{i=1}^{m} C^i_{ms-i(s-1)}. \tag{19}$$

Пропускна здатність дискретного каналу без пам'яті оцінюється за формулою:

$$C = \frac{1}{m}\left(\log_2 N_{p\Sigma} - H_в\right), \tag{20}$$

де $\log_2 N_{p\Sigma} = H_{max}$ – максимальне значення інформації без втрат, що передається сигнальними конструкціями, побудованих на інтервалі часу $T_с$; $H_в$ – втрати інформації через спотворення сигнальних конструкцій у приймачі. Рівень втрат інформації в каналі із завадами впливає на пропускну здатність:

$$H_в \le (1 - P_п)\log_2(1 - P_п) + P_п \log_2 \frac{P_п}{N_р - 1}. \tag{21}$$

де $\boldsymbol{P}_п$ – імовірність прийняття помилкового рішення про прийом СКК.

Імовірності помилкового і вірного прийому сигнальних конструкцій при використанні множини з числом відрізків від 1 до m визначаються як:

$$P_{\text{п}} = 1 - \left[2\Phi\left(2h/S\right)\right]^i, \tag{22}$$

$$P_{\text{в}} = 1 - P_{\text{п}}, \tag{23}$$

де $\Phi\left(2h/S\right)$ – фукція Крампа. Для каналу з двома станами («хороший» та «плохий») загальна пропускна здатність розраховується з урахуванням показників питомої ваги кожного із них:

$$\bar{C} = \gamma_x C_x + \gamma_n C_n. \tag{24}$$

Залежності значень $\overline{C}$ від h при m = 5, i = 3 та s = 5, 7, 9 представлені на рис. 3. Бачимо, що в реальних каналах зв'язку в "хорошому" стані каналу (h≥10) пропускна здатність системи зв'язку з ТСК більша в 2 рази в порівнянні з РЦК. Це обгрунтовує доцільність використання ТСК для підвищення швидкості передавання інформації в «хорошому» стані каналу.

Розглянемо можливість перетворення надлишку пропускної здатності на підвищення якості передачі за умови, що імовірність перебування каналу у «хорошому» стані становить $p_x < 0{,}99 \cdot 10^{-8}$, а у «поганому» - $p_x = 0{,}5$.

Для порівняння розглянемо дві системи передачі:

1) код Хеммінга з параметрами: m= 5 інформаційних бітів, r = 4 перевірочних бітів, n = 9 загальна довжина кодового слова, $N_{\text{р рцк}}$ = 512, режим виправлення однократних помилок ($t_{\text{в}}$=1); 2) таймерний сигнал, який забезпечує $N_{\text{р тск}}$ = 680 реалізацій на інтервалі $5t_0$ при i = 3, s= 7.

Розрахунок параметрів для РЦК виконується для середньої імовірності помилки $\overline{p} = 5 \cdot 10^{-3}$ і коефіцієнта групування $\alpha = 0{,}32$.

Відносна ефективна швидкість передачі позначається як R і наведена у табл. 2. Імовірність помилки в кодовому слові для РЦК $P_{\text{п}} = P(\geq 1, n) = \overline{p} \cdot n^{1-\alpha}$ або з урахуванням виправлення однократної помилки $P(\geq 2, n) = \overline{p} \cdot (n/2)^{1-\alpha}$. Для ТСК з урахуванням того, що $2h/s = \Delta/2\sigma$, формула (22) перетворюється в такий вираз:

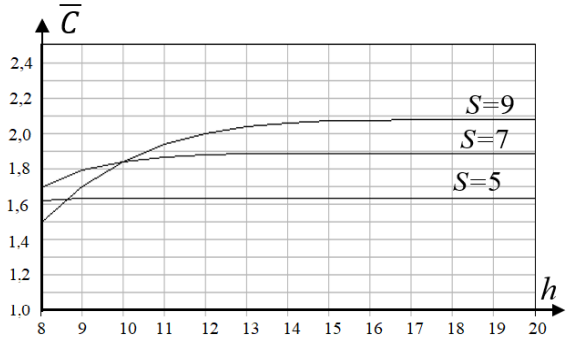

Рисунок 3 - Залежності $\bar{C}$ від h при параметрах ТСК m = 5, i = 3 та s = 5, 7, 9

$$P_{\text{п}} = 1 - \left[2\Phi\left(\Delta/2\sigma\right)\right]^i. \tag{25}$$

При s = 7 для «хорошого» стану каналу використовується відповідне середньоквадратичне відхилення фронту ЗММ фронту СКК $\sigma = 0{,}0178t_0$. Аналіз прикладу показує, що ТСК дозволяють отримати в 1,32 раза більше реалізацій на інтервалі $5t_0$, ніж РЦК. При цьому передача ТСК здійснюється за час, у 1,8 раза коротший, ніж для РЦК. Це означає, що протягом одного і того самого інтервалу часу T_i можливо передати більшу кількість сигнальних конструкцій, ніж при

використанні РЦК. Якщо припустити, що кількість помилок у каналі на інтервалі T_i залишається сталою, тоді за рахунок збільшення кількості переданих конструкцій імовірність помилки для ТСК зменшується. Проведені розрахунки підтверджують це: ймовірність помилки при використанні ТСК є нижчою, ніж у РЦК навіть з виправленням однократних помилок (табл. 2). Це означає, що в умовах «хорошого» стану каналу можливо передавати значно більший обсяг інформації за допомогою таймерних сигналів, ніж при використанні РЦК. Частину приросту відносної швидкості передачі можна використати для підвищення завадостійкості системи шляхом застосування кодів, здатних виправляти помилки.

Таблиця 2 - Розрахункові параметри однобічної системи на базі ТСК та РЦК

№	Параметри кодових комбінацій	$N_{\text{р}}$	R	$P_{\text{п}}$
1	РЦК (n = 9, m = 5)	512	0,55	$2{,}2 \times 10^{-2}$
2	РЦК (n = 9, m = 5, $t_{\text{в}}$= 1)			$1{,}4 \times 10^{-2}$
3	ТСК (n = 12, m = 5, s = 7)	680	1,88	$1{,}79 \times 10^{-4}$
4	РЦК (n = 9, r = 4, $t_{\text{в}}$= 1) сумісно з ТСК (m = 5, i = 3, s= 7)	680	1,05	$1{,}12 \times 10^{-4}$

Таким чином, у бінарній системі передачі існує можливість трансформувати запас завадостійкості в збільшення швидкості без втрати якості передавання завдяки використанню оптимальних структур сигнальних конструкцій.

У третьому розділі – «Захист інформації на основі непозиційних таймерних сигнальних конструкцій» – розглянуто можливості підвищення завадостійкості та прихованості СКК шляхом варіативного використання параметрів таймерного кодування. Обґрунтовано доцільність застосування ТСК у поєднанні з позиційним завадостійким кодуванням і стохастичним шифруванням для компенсації надлишковості перевірчих і випадкових елементів. Потенційна структурна прихованість визначається через кількість можливих сигнальних конструкцій $N_{\text{р}}$, що використовуються для передавання інформаційних символів:

$$S = \log_2 N_{\text{р}}. \tag{26}$$

Оцінимо можливість збільшення числа реалізацій $N_{\text{р}}$ за допомогою таймерного кодування на інтервалі часу $T_{\text{с}} = nt_0$, де n – кількість елементів Найквіста. Базовим параметром побудови ТСК є часовий елемент Δ, за допомогою якого в межах часового інтервалу $T_{\text{с}}$ задаються тривалості імпульсів, $t_{\text{с}} = t_0 + k\Delta$, де $k = 0{,}1{,}2{,}\ldots, s \cdot (n-2)$. Тривалості імпульсів $t_{\text{с}}$ кратні базовому елементу Δ (де $\Delta = t_0/s$; $s = 1,\ 2,\ 3,\ \ldots,\ l$ – цілі числа) і повинні задовольняти умові Найквіста:

$$t_{\text{с}} \geq t_0 = 1/\Delta F. \tag{27}$$

Параметр $s = t_0/\Delta$ визначає кількість Δ на інтервалі t_0. Збільшення числа реалізацій таймерних сигналів $N_{\text{р}}$ на інтервалі $T_{\text{с}}$ в порівнянні з РЦК досягається за рахунок зменшення енергетичної відстані між сигнальними конструкціями і визначається величиною $\Delta < t_0$, тоді:

$$N_{\text{р}} = [ns - i(s-1)]!/i!\,(ns - is)!, \tag{28}$$

де i – число інформаційних моментів модуляції. Варіювання значеннями, n, s і i дає можливість синтезувати різні безлічі сигнальних конструкцій, які відрізняються структурою побудови і кількістю реалізацій $N_{ч2}$. Збільшення N_p, а, отже, і структурної прихованості за рахунок зменшення інтервалу Δ призводить до падіння завадостійкості, що потрібно враховувати при виборі параметрів ТСК. У табл. 3 наведені реалізації N_p, отримані методом підбору в залежності від параметрів n, s, i для різних значень мінімальної кодової відстані $d_0(\Delta) \geq 1$. Для $n = 7$, $i = 3$ і $s = 5$ число реалізацій $N_{\text{р}}$=1771 (табл. 1, №1), тоді як для РЦК всього $N_{\text{рРЦК}}$=2^7=128. При $s = 6$ можна отримати більшу кількість реалізацій $N_{\text{р}}$ = 2925 (табл. 1, № 3). Подальше збільшення числа комбінацій ТСК забезпечується шляхом вибору розширення часового інтервалу $T_{\text{с}}$. Для $n = 8$, $i = 3$, s =5 значення $N_{\text{р}}$ = 3276 (табл. 1, №4). З табл. 3 бачимо, що зі збільшенням $d_0(\Delta)$ число реалізацій $N_{\text{р}}$ зменшується. За умови, що

$$d_0(\Delta) \geq 2\,, \tag{29}$$

можна реалізувати завадостійке кодування на основі ТСК шляхом вибору дозволених та недозволених комбінацій. Для визначення $d_0(\Delta)$ запропоновано використовувати кодову відстань по Хеммінгу з урахуванням кількості часових інтервалів елементів Δ:

$$d_0(\Delta) = \sum_{j=1}^{W} x_j \oplus z_j, \tag{30}$$

де x_j і z_j – логічний стан відрізків ТСК ("0" або "1") по елементах Δ; $W = n \cdot s$ – кількість елементів Δ на інтервалі часу $T_{\text{с}}$. У табл. 3 надано значення вибірок ТСК з $d_0 \geq 2$, які отримано методом підбору.

Таблиця 3 - Кількість реалізацій ТСК у залежності від параметрів n, s, i і d_0

№	Параметри ТСК			Вибірки ТСК у залежності від d_0								
	N	i	s	1	2	3	4	5	6	7	8	9
1	7	3	5	1771	891	248	146	79	53	36	28	22
2	7	3	6	2925	1469	395	231	121	85	53	44	31
3	7	3	7	4495	2255	591	344	176	121	76	60	44
4	8	3	5	3276	1638	438	252	133	91	59	47	33
5	8	3	6	5456	2736	714	408	316	146	94	70	50
6	8	3	7	8436	4218	1079	615	316	212	137	102	75

На рис. 4 подано приклади реалізації сигнальних конструкцій з різною тривалістю імпульсів і кодовою відстанню $d_0(\Delta)$ з параметрами $n = 7$, $i = 3$, s =5: $t_{\text{с}1}$=5 Δ, $t_{\text{с}2}$=6Δ, $t_{\text{с}3}$=24Δ для ТСК-1; $t_{\text{с}1}$=6Δ, $t_{\text{с}2}$=10Δ, $t_{\text{с}3}$=19Δ – ТСК-2; ТСК-3) $t_{\text{с}1}$=10Δ, $t_{\text{с}2}$=17Δ, $t_{\text{с}3}$=8Δ – ТСК-3. Комбінації ТСК-1 і ТСК-2 мають відстань $d_0(\Delta)$=6, ТСК-1 і ТСК-3 – $d_0(\Delta)$=21, ТСК-2 і ТСК-3 – $d_0(\Delta)$=15. Як бачимо з табл. 3, зі збільшенням $d_0(\Delta)$ кількість реалізацій $N_{\text{р}}$ зменшується, що відповідно до (26) знижує структурну прихованість сигнальних конструкцій $S_{\text{тск}}$ (рис. 5). Суперечливий характер зміни показників структурної прихованості $S_{\text{тск}}$ та завадостійкості слід враховувати при розробці алгоритмів обміну даними в системі зв'язку. Компенсувати зменшення показника $S_{\text{тск}}$ в цьому випадку пропонується шляхом застосування різних множин сигнальних конструкцій $\{N_{\text{тск}_i}(d_0(\Delta))\}$ з певним значенням $d_0(\Delta)$ для різних сеансів передавання інформації, тоді

$$S_{\text{тск}} = \log_2\left(\sum_{z=1}^{L} N_{\text{тск}_i}(d_0)\right), \tag{31}$$

де L – кількість множин ТСК. Отже, від вибору значень n, s та i залежить як завадостійкість, так і структурна прихованість сигнальних конструкцій.

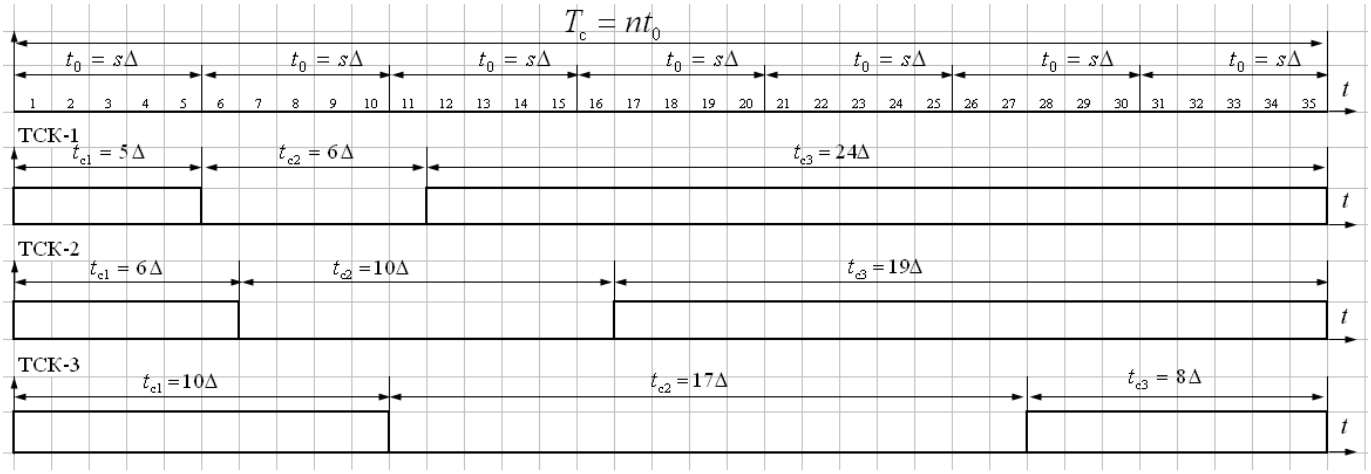

Рисунок 4 - Приклади реалізації ТСК з різними значеннями $d_0(\Delta)$

З технічної сторони для реалізації таймерного кодування доцільно використовувати рівняння якості, за допомогою якого можна формувати дозволені комбінації:

$$\sum_{k=1}^{i} A_k x_k \equiv 0 (\mathrm{mod}\, A_0), \qquad (32)$$

де $A_k(k = 1, i)$ – вагові коефіцієнти, що представляють собою набір простих чисел; A_0 – значення модуля; x_k – номери відділків значущих моментів модуляції (ЗММ) імпульсів t_{ci}.

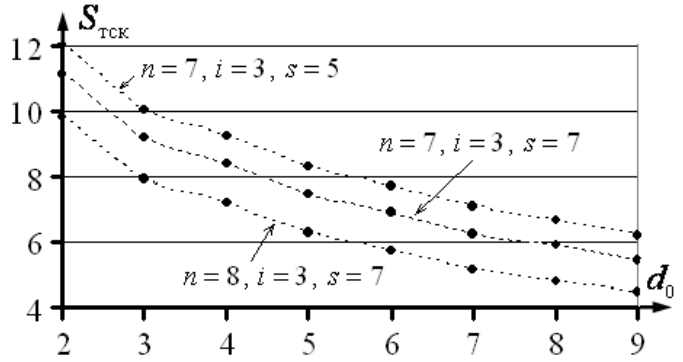

Рисунок 5 - Залежність структурної прихованості $S_{тск}$ від $d_0(\Delta)$ для ТСК, що отримані методом підбору

Якщо сигнальна конструкція задовольняє умови (32), тоді вона є дозволеною. Вибірки N_p дозволених кодових комбінацій з $d_0(\Delta) = 4$, що формуються за допомогою рівняння якості з A_0=19, A_1=2, A_2=3, A_3=7 і параметрів побудови n, s, i, наведені в табл. 2. Також в табл. 3 надані реалізації ТСК зі значеннями $d_0(\Delta) \geq 5$, отриманими з вихідної множини з $d_0(\Delta) = 4$.

Як бачимо з табл. 4 кількість дозволених ТСК, що задовольняють рівняння якості (32) із заданими $A_k(k = 1, i)$ і A_0 значно менше, ніж при повному переборі усієї множини ТСК (28). Для $n = 7$, $i = 3$, s =5 і $d_0(\Delta) = 4$ можна отримати N_p=93 (табл. 4, №1) із загального числа реалізацій $N_{pзаг}$=1771, тоді як при повному переборі N_p=146 (табл.3, №2). При $d_0(\Delta)$=5 кількість реалізацій суттєво знижується N_p=37 (табл. 4, № 1), а при повному переборі N_p=79 (табл. 3, №1).

Отже, рівняння якості (28) є зручним інструментом для реалізації завадостійкого кодування на основі ТСК. Проте, кількість дозволених комбінацій при цьому менше, ніж при повному переборі (табл. 3), що необхідно враховувати при розробці алгоритмів підвищення структурної прихованості на основі ТСК. Синтезувати різні безлічі сигнальних конструкцій можна за рахунок зміни A_0, A_1, A_2, A_3 в межах допустимих значень. Використання сумарної множини комбінацій

дозволяє підвищити структурну прихованість (31) і забезпечити задану достовірність.

Отже, дослідження в третьому розділі показують, що збільшення структурної прихованості можливо на обмеженому інтервалі часу за допомогою ТСК у порівнянні з позиційними кодами. Проте, виявлена зворотна закономірність між показниками структурної прихованості і завадостійкості, що пов'язана із зменшенням базового елемента Δ або/та збільшення кодової відстані.

Таблиця 4 - Вибірки реалізацій ТСК по рівнянню якості з A_0=19, A_1=2, A_2=3, A_3=7 и n, s, i, $d_0(\Delta)$

№	Параметри ТСК			$N_{\text{р}}$	Вибірки дозволених ТСК у залежності від $d_0(\Delta)$					
	m	i	S		4	5	6	7	8	9
1	7	3	5	1771	93	37	27	24	15	13
2	7	3	6	2925	154	59	43	41	23	19
3	7	3	7	4495	236	88	68	58	34	29
4	8	3	5	3276	173	65	52	40	27	22
5	8	3	6	5456	288	106	82	68	42	35
6	8	3	7	8436	444	156	123	98	60	49

Для вирішення цієї проблеми запропоновано застосування більшої кількості різних множин ТСК у процесі передавання інформації. Це дозволяє компенсувати зменшення показника структурної прихованості при обмеженому значенні Δ та кодової відстані, які потрібні для забезпечення заданої достовірності.

У четвертому розділі – «Підвищення захищеності інформації на основі інтегрованих методів перетворення даних» – запропоновано багаторівневий захист інформації з використанням стохастичного шифрування, завадостійкого та таймерного кодування. Підвищення прихованості та завадостійкості засноване на використанні трьох перетворювачів даних: внутрішнього, проміжного, зовнішнього. Внутрішній перетворювач використовує стохастичне шифрування (СШ) для забезпечення інформаційної прихованості повідомлень. Перевагою СШ є можливість формування різного набору комбінацій шифрограми для однакового повідомлення. Проміжний перетворювач реалізує завадостійке кодування блоковим кодом для забезпечення розрахункової завадостійкості. Зовнішній перетворювач реалізує таймерне кодування для забезпечення структурної прихованості сигнальних конструкцій та компенсації надлишкових елементів при стохастичному шифруванні та завадостійкому кодуванні.

Для підвищення інформаційної прихованості передаваного повідомлення запропоновано при стохастичному шифруванні враховувати ентропію дискретного джерела інформації, що пов'язано з визначенням кількості випадкових комбінацій для кожного символу b_j алфавіту. Відповідно до виразу Шеннона ентропія для випадку подій з нерівноймовірними станами визначається формулою:

$$H_{\text{НР}}(U) = -\sum_{j=1}^{L} p_j(u_j) \times \log_2 p_j(u_j). \quad (33)$$

Ентропія алфавіту обраної мови з урахуванням ймовірності появи символів у тексті становить $H_{\text{НР}}(U)$ = 4,42. Ентропія для рівноймовірних символів алфавіту $H_{\text{Р}}(U)$ = 5. Вочевидь, що підвищити інформаційну прихованість при стохастичному

шифруванні можливо при рівноймовірному законі появі випадкових комбінацій в шифрограмі повідомлення, тобто

$$H(U) \to H_p(U), \tag{34}$$

а також за умови, що

$$z \to \infty, \tag{35}$$

де $z = k + l$ – кількість двійкових елементів у випадковій кодової комбінації; k – кількість інформаційних елементів; l – кількість додаткових біт, які додаються до інформаційних елементів при стохастичному шифруванні.

Умову (34) можливо забезпечити, якщо кількість випадкових комбінацій вибирати з урахуванням ймовірності появи $p_j(u_j)$ кожного символу b_j використовуваного алфавіту. Умова (35) суттєво зменшує кодову швидкість, тому вибір значення z має бути обмежений з урахуванням вимог до швидкості передавання і інформаційної прихованості. При блоковому кодуванні довжина випадкової кодової комбінації збільшується на r елементів, тобто $n = k + l + r$, де r – кількість перевірочних елементів. Використання стохастичного шифрування зменшує кодову швидкість, оскільки:

$$\gamma_{\text{кш}} = k/(k + l + r_2) < \gamma_к = k/(k + r_1), \tag{36}$$

де $\gamma_{\text{кш}}$ – кодова швидкість при спільному використанні стохастичного шифрування і блокового кодування; $\gamma_к$ – кодова швидкість блокового коду; r_1 – кількість перевірочних елементів для інформаційної комбінації з k елементів; r_2 – кількість перевірочних елементів для комбінацій із z елементів.

Зрозуміло, що підвищити інформаційну прихованість повідомлення можна шляхом збільшення числа комбінацій в ансамблі C. Це означає, що $z=[\log_2 M]$ також збільшується. Для порівняльного аналізу в табл. 3 надана структура кодового блоку, що формується в залежності від варіанту кодування інформаційної послідовності k. Так для структури блоку $n = k + r_1$ забезпечується тільки завадостійке кодування (табл. 4, рядок №1). При стохастичному шифруванні ($n = k + l$) може бути забезпечена тільки інформаційна прихованість.

При комбінованому стохастичному шифруванні на основі РЦК із структурою блоку $n = k + l + r_2$ реалізується інтегрований захист каналу як від випадкових завад, так і НСД (табл. 5, № 3). Завадостійке кодування на основі ТСК дозволяє здійснити не тільки контроль по достовірності передавання інформації, а також – збільшити кодову швидкість $\gamma_к$. Пояснюється це тим, що інтервал побудови ТСК менше, ніж для завадостійких позиційних кодів, тобто $m_{\text{ТСК}} \le k + r$ (табл. 4, № 5). При сумісному використанні стохастичного шифрування та завадостійкого кодування комбінація позиційного коду $n = k + l + r_2$ замінюється на таймерну конструкцію.

Для підвищення інформаційної прихованості та збільшення кількості кодових реалізацій пропонується використовувати набір ТСК з двох комбінацій, одна з яких є дозволеною комбінацією, а друга може бути як дозволеною так і недозволеною та визначається за допомогою другої кодової книги. Сумісне використання блокового завадостійкого та таймерного кодування дозволяє збільшити завадостійкість, тому загальна ймовірність невиявленої помилки в кодовому блоці:

$$P_{\text{НП}} = P_{\text{НП-РЦК}} \times P_{\text{НП-ТСК}}, \tag{37}$$

де $P_{\text{НП-РЦК}}$ – ймовірність невиявленої помилки при блочному завадостійкому кодуванні; $P_{\text{НП-ТСК}}$ – ймовірність невиявленої помилки при таймерному кодуванні.

При цьому інтервал побудови двох ТСК менше ніж для РЦК, тобто $m_{\text{ТСК1}} + m_{\text{ТСК2}} < k + l + r_2$, а мінімальна кодова відстань $d_0(\Delta)$ визначається обраним ансамблем дозволених комбінацій (табл. 5, № 5).

Таблиця 5 - Варіанти формування кодових комбінацій

№	Варіант кодування	Склад кодового блоку		
1	Завадостійке кодування на основі РЦК	K	r_1	-
2	Стохастичне шифрування	K	l	-
3	Стохастичне шифрування сумісно з блоковим завадостійким кодом	K	l	r_2
4	Завадостійке кодування на основі ТСК	$m_{\text{ТСК}} \le k + r$		
5	Стохастичне шифрування на основі РЦК і двох ТСК	K	l	r_2
		$x_{\text{ТСК}}(t)$: $m_{\text{ТСК}} < k + l + r_2$		
6	Стохастичне шифрування на основі РЦК і двох ТСК	K	l	r_2
		$m_{\text{ТСК1}} + m_{\text{ТСК2}} < k + l + r_2$		

Для оцінки ефективності стохастичного шифрування проведено імітаційне моделювання для двох варіантів реалізації перетворювача:

1) кількість випадкових кодових комбінацій є змінною величиною і визначається з урахуванням ймовірності появи символу алфавіту в тексті повідомлення;

2) однакова кількість випадкових кодових комбінацій для кожного символу алфавіту в тексті повідомлення.

Ефективність стохастичного шифрування була оцінена по дисперсії D_{xv} і D_{xc} відповідно для першого і другого варіантів у залежності від загальної кількості використовуваних випадкових комбінацій N_1. У табл. 6 представлені результати досліджень для текстів різної довжини та n_2.

Таблиця 6 - Результати оцінок D_{xc} и D_{xv} для двох методів стохастичного шифрування

n_1	N_1	Текст великого розміру (500 сторінок)		Довільний текст з 10000 комбінацій		Текст пісні «Englishman in New York»	
		D_{xv}	D_{xc}	D_{xv}	D_{xc}	D_{xv}	D_{xc}
9	512	14 269 734,3	669 472 420,0	1 121,4	34 866,3	0,4	32,9
10	1024	4 408 878,1	124 230 180,0	22,7	8 772,3	0,1	7,8
11	2048	299 586,9	31 292 662,2	0,8	2 126,0	0,0	2,0
12	4096	40 566,6	8 025 058,9	0,3	531,7	0,0	0,5
13	8192	4 036,7	2 082 843,9	0,2	135,9	0,0	0,1
14	16384	316,2	543 439,8	0,1	33,8	0,0	0,0
15	32768	15,1	145 240,0	0,1	8,2	0,0	0,0
16	65536	1,4	40 101,8	0,0	1,8	0,0	0,0
17	131072	0,2	11 453,7	0,0	0,4	0,0	0,0

Бачимо, що при збільшенні розрядності кодування n_1 дисперсія D_{xv} для першого варіанту стохастичного шифрування зменшується значно швидше ($D_{xv} \to 0$), ніж D_{xc} для другого варіанту. На виході стохастичного шифратора можна сформувати потік комбінацій з приблизно рівними ймовірностями появи, що ускладнює використання частотного тесту комбінацій шифрограми при дешифруванні у випадку її перехоплення. Також виявлено, що при стохастичному

шифруванні великих об’ємів текстів (500 сторінок) для досягнення умови $D_{xv} \to 0$ необхідна більша розрядність n_1 випадкових комбінацій. При цьому дисперсія $D_{xv} = 0{,}2$ буде отримана при розрядності n_1 = 17. Для тексту з 10000 комбінацій $D_{xv} = 0{,}2$ і n_1 = 13. Найкращий результат одержано для невеликих текстів (пісня «Englishman in New York»): $D_{xv} = 0{,}1$ і n_1 = 10.

Отже, запропонований метод комбінованого стохастичного шифрування може бути застосований для розробки реальних завадозахищених систем зв'язку, у яких вирішується задача підвищення прихованості і завадостійкості передавання секретної інформації.

У п’ятому розділі – «Дослідження та обґрунтування вибору параметрів таймерних сигналів у системах захисту інформації на основі розширення спектра» – надана оцінка параметрам ТСК для завдання формування шумоподібних сигналів. Запропоновано критерії вибору параметрів ТСК з урахуванням складності реалізації сигнальних конструкцій, забезпечення прихованості і завадостійкості.

При вирішенні завдання синтезу шумоподібних таймерних сигналів важливим є обґрунтований вибір параметрів побудови ТСК. Таймерне кодування дозволяє формувати значну кількість різних множин реалізацій $N_\text{р}$ в залежності від параметрів *m*, *s* та *i*, що є основою для підвищення прихованості сигнальних конструкцій. З цього приводу доцільним є аналіз кожного з цих параметрів і надання оцінки їх впливу на наступні властивості: складність реалізації сигнальних конструкцій, завадостійкість, прихованість.

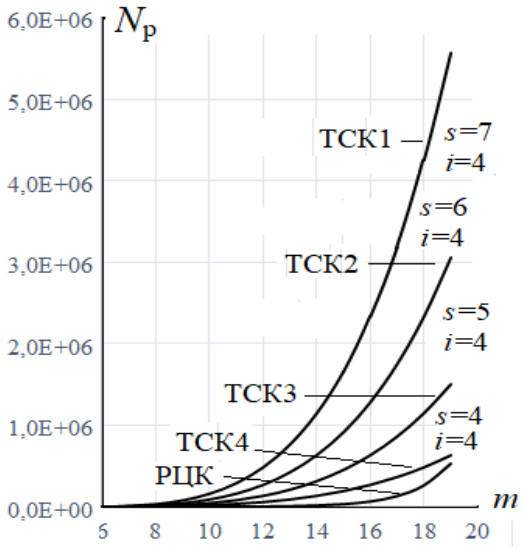

Рисунок 6 - Залежності $N_\text{р}$ від *m*, *s* та *i*

Важливим показником побудови ТСК є вибір кількості інтервалів Найквіста *m* для побудови сигнальних конструкцій. Часовий інтервал побудови таймерних сигналів T_c задається певною кількістю інтервалів Найквіста *m*. На рис. 6 наведені залежності реалізації $N_\text{р}$ для множин ТСК1 (*s*=7, *i*=4), ТСК2 (*s*=6, *i*=4), ТСК3 (*s*=5, *i*=4), ТСК4 (*s*=4, *i*=4) від кількості інтервалів Найквіста *m*. Також на рис. 6 надана залежність кількості реалізацій для РЦК. Бачимо, що потужність таймерних сигналів по можливості формування кількості комбінацій суттєво перевищує реалізації РЦК. Побудовані закономірності реалізацій ТСК дозволяють зробити висновок, що збільшення кількості *m* дозволяє суттєво збільшити число реалізацій $N_\text{р}$. Наприклад, для *m*=6, *s*=5, *i*=4 можна побудувати $N_{\text{ртск}}$=1001 реалізацій ТСК. При підвищенні кількості інтервалів Найквіста до *m*=19 та при незмінних *s*=5, *i*=4 можна побудувати значно більшу кількість реалізацій $N_\text{р}$= 1502501. Структурна прихованість згідно (26) $S_{\text{тск}}$(*m*=6, *s*=5, *i*=4)=9,96 дв.вим та суттєво підвищується при збільшенні значення *m* та складає $S_{\text{тск}}$(*m*=19, *s*=5, *i*=4)=20,5 дв. вим. Такий підхід побудови сигнальних конструкцій за допомогою кількості інтервалів *m* не суперечить умові забезпечення максимально можливого значення структурної прихованості, проте

збільшуються вимоги до точності реєстрації значущих моментів відновлення в приймачі. У зв'язку з цим доцільним є обмеження кількості інтервалів m, а збільшення числа реалізацій $N_{\text{ртск}}$ пропонується за рахунок зміни параметрів s та i.

Розглянемо можливості збільшення числа реалізацій за рахунок використання ТСК з різним числом ЗММ i. На рис. 7 надано залежності $N_{\text{р}}$ від i, m та s=5, за якими можна побачити максимальні значення кількості реалізацій за певним значенням ЗММ. Так, для m=8 максимальне значення реалізацій $N_{\text{р}}$=15504 досягається при i =5, для m=10 отримуємо $N_{\text{р}}$=230230 при i =6. Отже, при виборі параметрів ТСК для завдання розширення спектра обґрунтованим є вибір оптимального значення $i_{\text{опт}}$, при якому забезпечується максимальне значення реалізацій та структурної прихованості, тобто:

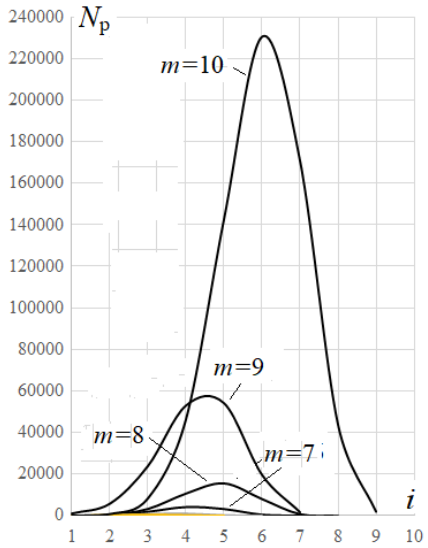

Рисунок 7 - Залежності $N_{\text{р}}$ від i, m та s=5

$$\max N_{\text{р}} = S\{i_{\text{опт}}, n, s, P_{\text{НП}}(n)\}. \quad (38)$$

Проте можливе використання множин комбінацій, у яких значення i буде змінюватися від одного до m – 1 (табл. 7). Це суттєво збільшить ансамбль реалізацій $N_{\text{р}}$ та підвищить структурну прихованість, тобто:

$$\max N_{\text{р}\Sigma} = S\{i = 1, 2, .. m-1, m, s, P_{\text{НП}}(n)\}. \quad (39)$$

Умова (39) використовує сумарне значення реалізацій ТСК з різною кількістю ЗММ. У табл. 6 наведено результати отриманої кількості реалізацій у залежності від m, s та $i = 1, 2, \dots, m-1$. Бачимо, що досягнути достатньої кількості комбінацій можливо не за рахунок збільшення кількості інтервалів Найквіста, а за допомогою об'єднання реалізацій з різним числом ЗММ при фіксованому значенні m.

Таблиця 7 - Кількість сумарних реалізацій Т $N_{\text{р}\Sigma}$ при $i = 1, 2, \dots, m-1$

m	s			
	3	4	5	6
5	188	344	570	881
6	594	1251	2327	3969
7	1872	4543	9495	17886
8	5895	16492	38739	80607
9	18533	59829	38739	363203
10	58424	217285	644760	1636943

Розглянемо варіант збільшення числа реалізацій за рахунок підвищення значення s. На рис. 8 надано залежності $N_{\text{р}}$ від s, m, i=3, з яких можна побачити, що з ростом часових інтервалів s суттєвого збільшується кількість комбінацій ТСК, а також спостерігається підвищення структурної прихованості.

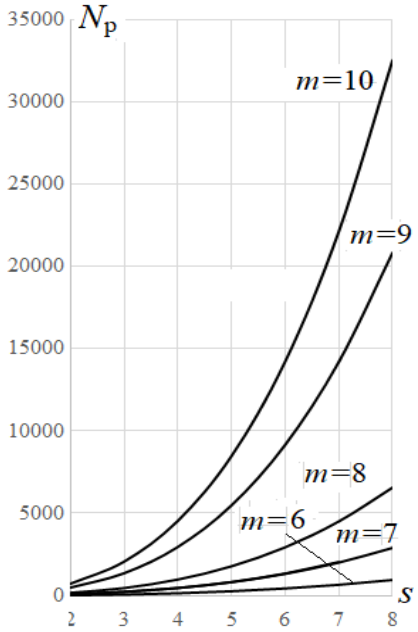

Рисунок 8 - Залежності $N_{\text{р}}$ від s, m, i=3

Проте при збільшенні s зменшується часовий інтервал Δ і за певних значеннях s=const та m можна досягти максимального значення пропускної здатності:

$$C_{\text{тск}} = \frac{log_2 N_{\text{р}} - \bar{i} H_{\text{з}}\left(\frac{z_i}{k_i}\right) - H_{\text{з}}}{m}, \qquad (40)$$

де $H_{\text{з}}$ – ентропія на прийомі таймерних сигналів, яка визначається за формулою:

$$H_{\text{з}} = -\left[p_{\text{В}}\, log_2 p_{\text{В}} + (1 - p_{\text{В}})\, log_2 \frac{(1-p_{\text{В}})}{N_p - 1}\right], \qquad (41)$$

$p_{\text{В}}$ – ймовірність вірного прийому таймерних сигналів; $H_{\text{з}}\left(\frac{z_i}{k_i}\right)$ – умовна ентропія, яка характеризує невизначеність ймовірності ТСК з k-переходами за умови, що приймач отримав сигнал з i-переходами та визначається як:

$$H\left(\frac{z_i}{k_i}\right) = -\sum_{i=1}^{z_0} P\left(\frac{z_i}{k_i}\right) \log_2 P\left(\frac{z_i}{k_i}\right),$$

де $P\left(\frac{z_i}{k_i}\right)$ – ймовірність одержання зменшення ЗМВ переходу на $z\Delta$. Залежності пропускної здатності каналу з різним рівнем флуктуаційних шумів ($h = u_c/u_з$) та величини s надано на рис. 9.

Залежності під номерами 1…3 побудовані для значень $h = 7{,}5$ і m =8, 6, 5 відповідно, під номерами 4…6 для h =5,5 і m =8, 6, 5 відповідно. Залежності 1, 2, … 6 дають зрозуміти, що при виборі параметра s, потрібно враховувати умову забезпечення максимальної пропускної здатності. Для залежності 4, 5 та 6 отримуємо оптимальне значення $s_{\text{опт1}} = 6$, при якому забезпечується максимальне значення $C_{\text{тск}}$. Для залежності 1, 2 та 3 отримуємо $s_{\text{опт2}} = 8$. За умови $s > s_{\text{опт}}$ зменшується часовий інтервал Δ, що призводить до збільшення показника $H_{\text{з}}$, який характеризує втрати через збільшення спотворених сигнальних конструкцій. Отже, виявлено протиріччя між умовою підвищення структурної прихованості шляхом збільшення s та необхідністю обмеження цього показника

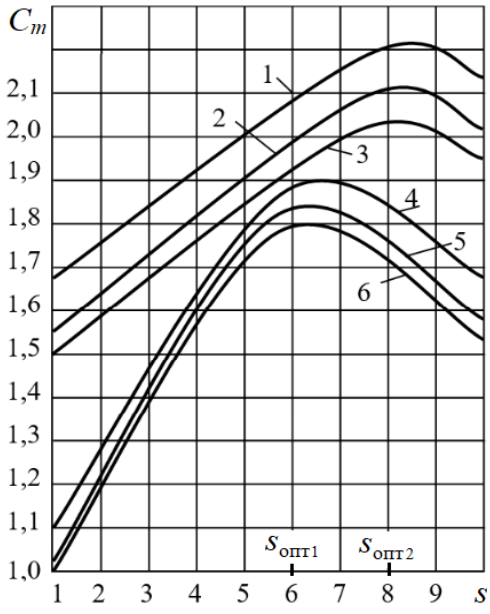

Рисунок 9 - Залежності пропускної $C_m = f(s)$ при

значенням $s \le s_{\text{опт}}$ при заданому m та відношенням сигнал/шум h.

Таким чином, дослідження в п'ятому розділі дали змогу визначити основні вимоги по вибору параметрів ТСК для завдання формування шумоподібних сигналів за допомогою різних методів розширення спектра. Визначено обмеження на вибір параметрів ТСК, які впливають на складність реалізації шумоподібних таймерних сигналів, їх передавання та прийму, забезпечення завадостійкості та прихованості.

У шостому розділі – «Методи формування шумоподібних таймерних сигналів» – надана оцінка умовам забезпечення енергетичної прихованості для методів розширення спектра за критеріями частотної та енергетичної ефективності використання каналу. Запропоновано алгоритми розширення спектра непозиційних ТСК з урахуванням конструктивних особливостей їх побудови та вимог для забезпечення завадостійкості. Наведено обґрунтування доцільності використання шумоподібних таймерних сигналів з адаптивними параметрами для задачі підвищення прихованості сигнальних конструкцій.

Енергетична прихованість спрямована на ускладнення виявлення факту передаваного сигналу засобами РЕР противника. Ефективність методів розширення спектра запропоновано оцінювати на основі аналізу таких показників: база сигналу $B = \Delta f T >> 1$ – перша умова; частотна ефективність $\gamma = R/\Delta f_{\text{еф}}$ – друга умова; 3) ефективність використання каналу по потужності $\beta = R/h_0^2$ – третя умова.

Для завдання аналізу розглянемо такі базові методи розширення спектра: ППРЧ; ПРС-ПВП; ЛЧМ. Методи ППРЧ, ПРС-ПВП та ЛЧМ задовольняють першу та другу умови, згідно з якими використовується збільшена смуга частот, тобто $B >> 1$. Характерним є те, що виконання другої умови обґрунтовується «погіршенням» показника частотної ефективності. Третя умова забезпечується тільки методом ПРС-ПВП, що пояснюється суттєвим зменшенням тривалості інформаційного елемента t_0 за рахунок імпульсів розширення ПВП з інтервалом часу $\tau \ll t_0$ та перерозподілу потужності сигналу в широкому діапазоні частот Δf. Отже, методи розширення спектра на основі ППРЧ і ЛЧМ забезпечують певний рівень енергетичної прихованості за розглянутими параметрами лише частково, тобто задовольняють першу та другу умови.

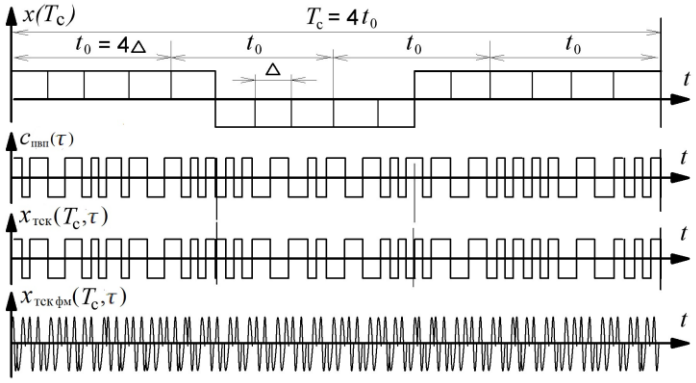

Рисунок 10 - Формування шумоподібного таймерного сигналу $x_{\text{штск фм}}(T_{\text{с}}, \tau)$

З урахуванням особливостей побудови ТСК використання для них алгоритму прямого розширення спектра за допомогою ПВП, який призначений для позиційних кодів, не видається можливим. Пояснюється це тим, що розширення спектра відбувається для імпульсних елементів однаковою тривалістю часу t_0 з певною базою B_{t_0}. В ТСК тривалість імпульсів $t_{\text{с}} \ge t_0$ різна, що означає необхідність використання іншого алгоритму розширення спектра. У зв'язку з цим пропонується

виконувати розширення спектра на всьому інтервалі T_c побудові ТСК. У цьому випадку кількість імпульсів $N_{\tau\text{ТСК}}$ ПВП для розширення спектра ТСК складає:

$$N_{\tau\text{ТСК}} = B_{t_0} \times m. \quad (42)$$

Очевидно, що значення $N_{\tau\text{ТСК}}$ повинно бути парним деякому числу $N_\Delta = s \times n$, де N_Δ − кількість Δ на інтервалі $T_\text{с}$. Наприклад, якщо $s = 4$, n = 4, $N_\Delta = 16$, $B_{t_0} = 16$, тоді для узгодження ТСК і ПВП необхідно, щоб $N_\text{ТСК}$ = 64. Якщо $s = 4$, n = 3, $N_\Delta = s \times n$ = 12, $B_{t_0} = 16$, тоді $N_\text{ТСК}$ = 48.

Сформуємо широкосмугову послідовність $x_\text{тск}(T_\text{с}, \tau)$ на основі ТСК. Нехай $x(T_\text{с}, \Delta)$ бінарний таймерний сигнал на інтервалі його формування $T_\text{с} = mt_0$, де $c_\text{пвп}(\tau)$ – послідовність Уолша на інтервалі $T_\text{с}$. При цьому тривалість елементів ПВП $\tau \le \Delta$. Шляхом перемноження значення рівня кожного i-го розряду послідовності $c_\text{пвп}(\tau)$ на j-те значення рівня таймерного сигналу $x(T_\text{с}, \Delta)$ на інтервалі часу $T_\text{с}$ отримуємо шумоподібний сигнал:

$$x_\text{тск}(T_\text{с}, \tau) = c_{\text{пвп}i}(\tau) \times x_{\text{тск}j}(T_\text{с}, \Delta). \quad (43)$$

У результаті, кожне позитивне («1») або негативне значення («–1») ТСК замінюється імпульсами ПВП з тривалістю τ. Використання прямої та інвертованої ПВП $c_\text{пвп}(\tau)$ забезпечує визначення полярності імпульсів тривалістю $t_\text{с}$ ТСК при реєструванні ЗМВ на інтервалі $T_\text{с}$ при кореляційному прийомі. Далі імпульси $x_\text{тск}(T_\text{с}, \tau)$ надходять на фазовий модулятор, на виході якого утворюється шумоподібний таймерний сигнал:

$$x_\text{штск фм}(T_\text{с}, \tau) = g(\tau) \cdot cos(\, 2\pi f_0 \tau + x_\text{тск}(T_\text{с}, \tau)). \quad (44)$$

На рис. 10 наведено приклад синтезу шумоподібного ТСК $x_\text{штск фм}(T_\text{с}, \tau)$ з параметрами: m=4; s=4; i=2; $B_{t_0} = 16$, тоді $N_\text{ТСК}$ = 54.

Згідно (28) з такими параметрами можна побудувати $N_\text{штск фм} = 45$ шумоподібних ТСК. Для РЦК кількість шумоподібних сигнальних комбінацій $N_\text{рцк фм} = 16$, що менше в 2,8 рази ніж при використанні ТСК. Такий запас кількості сигнальних конструкцій дозволяє використати ТСК для формування дозволених комбінацій за допомогою рівняння якості (16). Це зменшить кількість реалізацій шумоподібних ТСК, проте дасть можливість контролювати якість комбінацій, що надходять з каналу в приймач. На кількість реалізацій ТСК впливає значення параметрів s та m. Вибір значення s і m відбувається з урахуванням відношення сигнал/шум h (рис. 9), яке визначається перед початком кожного сеансу передачі в результаті тестування каналу.

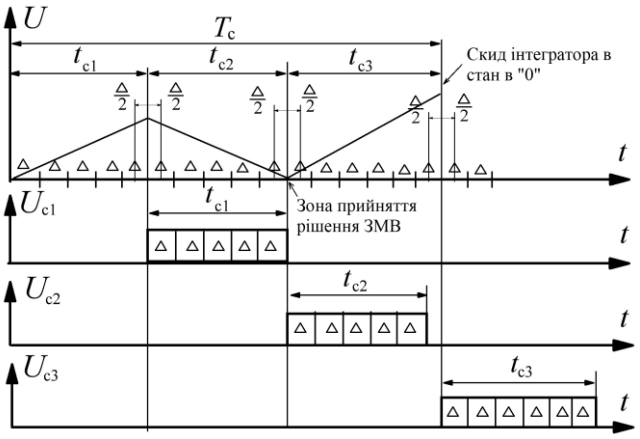

Рисунок 11 - Визначення ЗМВ імпульсів $t_\text{с}$ ТСК з виходу інтегратора кореляційного приймача

Отже, адаптація до поточного стану каналу параметрів ТСК при

формуванні шумоподібного сигналу дозволяє досягти максимальної пропускної здатності C_m (рис. 6) при кожному сеансі передачі.

З урахування непозиційності ТСК визначення тривалості імпульсів t_{c1}, t_{c2} і t_{c3} відбувається на точкам екстремумах напруги з виходу інтегратора кореляційного приймача (рис. 11) на інтервалі часу T_c. У межах інтервалу $[-\frac{\Delta}{2} ... \frac{\Delta}{2}]$ визначаються ЗМВ імпульсів ТСК. Структурна прихованість шумоподібного ТСК при розширенні спектра ПВП та використанні певного виду модуляції визначається такою формулою:

$$S_{\text{тск пвп}} = \log_2 N_{\text{р}} + \log_2 N_{\text{пвп}} + \log_2 N_{\text{см}}, \quad (45)$$

де N_p – кількість реалізацій ТСК; $N_{\text{пвп}}$ – кількість імпульсів ПВП; $N_{\text{см}}$ – кількість сигнальних конструкцій системи модуляції. На рис. 12 надано залежності $S_{\text{тск пвп}}$ від параметрів ТСК і кількості імпульсів розширення ПВП $N_{\text{пвп}}$. Бачимо, що на загальну прихованість $S_{\text{тск пвп}}$ більшою мірою впливає показник $N_{\text{пвп}}$. Наприклад, при параметрах ТСК $m = 8$, $s = 5$, $i = 3$ структурна прихованість $S_{\text{тск}} = 12$ дв. вим. При розширенні спектра ПВП $N_{\text{пвп}} = 64$ та ФМ-2 отримуємо $S_{\text{тск пвп}} = 12 + 64 + 1$=77 дв. вим. При цих параметрах шумоподібного сигналу доля $S_{\text{тск}}$ і $S_{\text{см}}$ складає усього 18%. Для збільшення значень $S_{\text{тск}}$ і $S_{\text{см}}$ доцільним є використання систем модуляції з більшим числом сигнальних конструкцій (наприклад, КАМ-4 або КАМ-8), а також комбінацій таймерних сигналів з різними ЗММ:

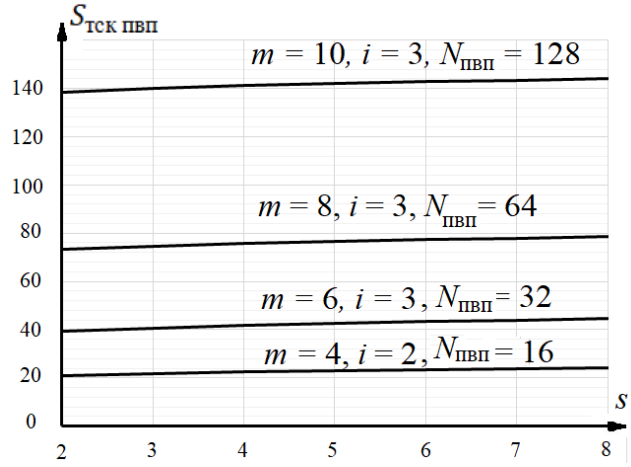

Рисунок 12 - Залежності $S_{\text{тск пвп}}$ від параметрів ТСК і $N_{\text{пвп}}$

$$N_{\text{р}}(n, i) = \sum_{i=1}^{n} \frac{[(n \cdot s) - [(s-1) \cdot i]]!}{i! \cdot [[(n \cdot s) - [(s-1) \cdot i]] - i]!}. \quad (46)$$

При використанні методу ППРЧ робоча частота радіосигналу змінюється за псевдовипадковим законом, який відомий тільки відправнику і отримувачу. Розширення спектра ТСК відбувається в межах інтервалу T_c шляхом передавання одного або кількох промодульованих елементів Δ таймерного сигналу (ФМ-2 або ФМ-4) на різних частотах. База сигналу визначається такою формулою:

$$B_f = (F_{max} - F_{min})/\Delta f, \quad (47)$$

де F_{max}, F_{min} – межі частотного діапазону; Δf – розмір частотного каналу.

При розширенні спектра ТСК, тривалість радіосигналу на одній частоті зменшується, тобто

$$t_{\text{пер ппрч}} = \Delta \times z < t_0, \quad (48)$$

де $z = 1, 2, \ldots, s - 1$ – кількість елементів Δ. Це означає, що

$$\Delta f = 1/\Delta z, \quad (49)$$

де $z = 1,2 \ldots sm$. Значення z визначає скільки елементів Δ ТСК буде передаватися на одній частоті Δf.

Зменшення інтервалу часу передавання на одній частоті обґрунтовується особливостями побудови ТСК, а також сучасними можливостями сканерів радіочастотного спектра SDR по виявленню радіосигналів ППРЧ. Для ТСК пропонуються такі методи розширення спектра на основі ППРЧ: швидкий, повільний, багатоканальний, комбінований.

Для повільної ППРЧ швидкість зміни несучого коливання більша за найквістовий інтервал t_0 у разі, коли використовується позиційне кодування. У ТСК $\Delta < t_0$, тому час передачі несучого коливання для повільної ППРЧ визначатиметься з урахуванням елемента Δ, тобто:

$$T_{\text{пов ппрч}} = \Delta z, \qquad (50)$$

де z визначає кількість Δ на інтервалі $T_{\text{пов ппрч}}$. При виборі інтервалу передавання на одній частоті слід враховувати, що при більшому значенні $T_{\text{пов ппрч}}$ ймовірність ураження радіосигналу завадою в каналі збільшується. Для таймерного сигналу з параметрами побудови $m = 4,\ s = 4,\ i = 2$ (рис. 13 (а)) подано часові діаграми розширення спектра методом повільної ППРЧ з $T_{\text{пов ппрч}} = 4\Delta$ (рис. 13 (б)). Якщо $z = ms$, тоді зміна несучого коливання відбуватиметься на інтервалі $T_{\text{пов ппрч}} = T_{\text{с}}$, тобто для кожної ТСК.

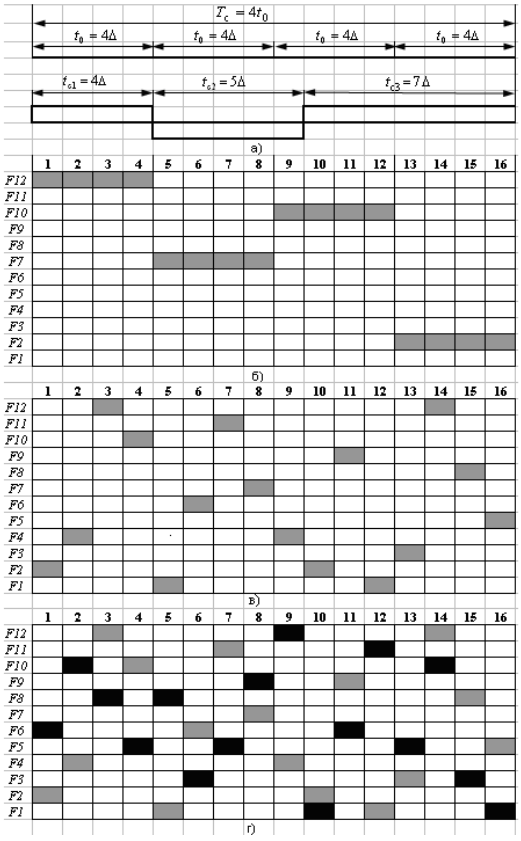

Рисунок 13 - Формування ППРЧ $x_{\text{штск фм}}(T_{\text{с}}, \tau)$

При швидкій ППРЧ (рис. 13 (в)) інтервал передавання несучої частоти менше або дорівнює інтервалу Δ:

$$\Delta \geq T_{\text{шм ппрч}}. \qquad (51)$$

Зменшення часу передавання несучої частоти (51) забезпечує менший вплив на сигнал цілеспрямованої вузькосмугової завади в порівнянні із повільною ППРЧ. Збільшення часу перебування сигналу на одній частоті.

Використання кількох каналів передавання однакової структури таймерного сигналу дає можливість реалізувати багатоканальну ППРЧ (рис. 13 (г)). Це означає, що час передавання несучої частоти $\Delta < T_{\text{бк ппрч}} \geq i\Delta$, дозволяє підвищити завадостійкість системи зв'язку шляхом мажоритарного прийняття рішення про полярність елемента Δ за умови використання непарної кількості F_i.

Структурна прихованість шумоподібного ТСК при розширенні спектра

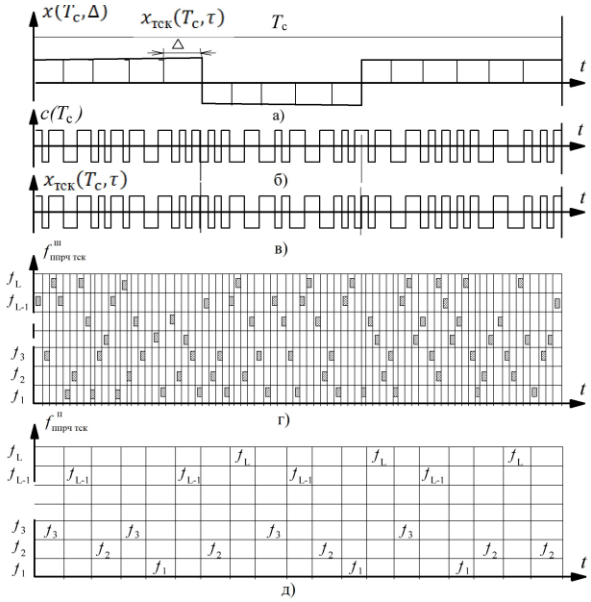

Рисунок 14 - Розширення спектра ТСК за допомогою ПВП та ППРЧ

методом ППРЧ та використанні певного виду модуляції визначається формулою:

$$S_{\text{тск пвп}} = \log_2 N_{\text{р}} + \log_2 N_{\text{ппрч}} + \log_2 N_{\text{см}}, \quad (52)$$

де $N_{\text{ппрч}}$ – кількість можливих варіантів слідування несучих частот. Розрахунок $N_{\text{ппрч}}$ визначається з урахуванням кількості доступних частот N_f та кількості стрибків на інтервалі комбінації таймерного сигналу $T_{\text{с}} = \Delta \times m \times s$. Для швидкої ППРЧ без повторень несущих частот отримуємо таку формулу:

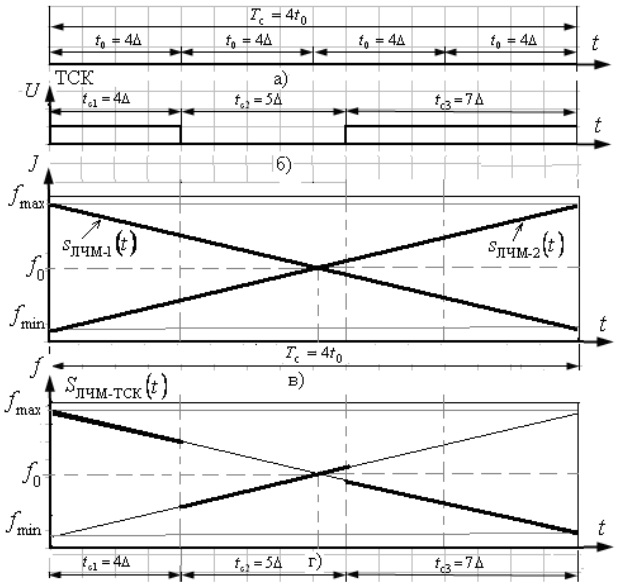

Рисунок 15 - Залежності несущих частот ЛЧМ при формуванні широкосмугових ТСК

$$N_{\text{ппрч бп}} = N_f!/\left(N_f - ms\right). \quad (53)$$

Збільшити кількість реалізацій можливо з повторенням несущих частот:

$$N_{\text{ппрч п}} = N_f{}^{ms}. \quad (54)$$

Для ТСК (рис. 13 (а)) з параметрами $m = 4$, $s = 4$, N_f=32 отримуємо: $N_{\text{ппрч бп}} = 1{,}26 \times 10^{22}$; $N_{\text{ппрч п}} = 1{,}21 \times 10^{24}$. Структурна прихованість $S_{\text{тск ппрч бп}} = \log_2 N_{\text{ппрч бп}} = 73{,}4$ і $S_{\text{тск ппрч п}} = \log_2 N_{\text{ппрч п}} = 80$, що свідчить про переваги методу ППРЧ з повторенням несущих частот приблизно в 1,08 рази.

При комбінованому методі розширення спектра ТСК поєднуються два методи ПРС-ПВП та ППРЧ (рис. 14). Спершу спектр ТСК $x_{\text{тск}}(t_{\text{с}})$ розширюється за допомогою елементів $\tau = \Delta/j$ (де j =1, 2, 3, … – кількість елементів τ на інтервалі Δ) ПВП $x_{\text{тск}j}(T_{\text{с}}, \Delta)$ в широкосмуговий сигнал $x_{\text{тск}}(T_{\text{с}}, \tau) = c_{\text{пвп}i}(\tau) \times x_{\text{тск}j}(T_{\text{с}}, \Delta)$. Після фазового модулятора таймерний сигнал $x_{\text{штск фм}}(T_{\text{с}}, \tau)$ проходить розширення спектра за допомогою методу швидкої ППРЧ:

$$u'(t) = x_{\text{штск фм}}(T_{\text{с}}, \tau) \times U_0 \, cos(\omega(g(t)t)), \quad (55)$$

де $cos(\omega(g(t)t))$ – набір частот, який є функцією від кодового сигналу $g(t)$. Структурна прихованість комбінованого методу оцінюється за формулою:

$$S_{\text{тск пвп-ппрч}} = \log_2 N_{\text{р}} + \log_2 N_{\text{пвп}} + \log_2 N_{\text{см}} + \log_2 N_{\text{ппрч}}, \quad (56)$$

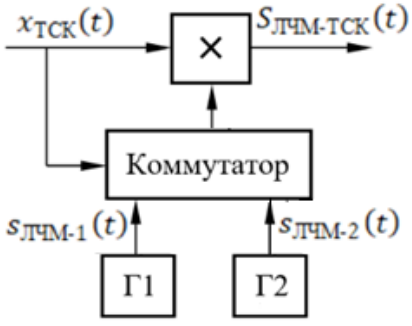

Рисунок 16 - Структурна схема розширення спектра ТСК за допомогою ЛЧМ в передавачі

де $\log_2 N_{\text{ппрч}} = S_{\text{тск ппрч}}$ – структурна прихованість методу ППРЧ. Розширення спектра ТСК з параметрами $m = 8$, $s = 5$, $N_{\text{пвп}} = 32$; $i = 3$, $N_{\text{пвп}} = 64$, $N_f = 32$ забезпечує структурну прихованість $S_{\text{тск пвп-ппрч}} = 12 + 64 + 1{+}80 = 157$ дв.вим. Бачимо, що використання комбінованого методу розширення спектра ТСК збільшує структурну прихованість у 2 рази та більше в залежності від значень бази методів ПРС-ПВП та ППРЧ. При інтерпретації структурної прихованості з криптостійкістю можна зробити висновок, що для систем зв’язку з комбінованим розширенням спектра

ТСК навіть при невеликих значеннях $N_{\text{пвп}} = 64$ і $N_f = 32$ отримуємо $S_{\text{тск пвп-ппрч}} = 157$ дв. вим., що перевищує критостійкість системи шифрування DES з довжиною ключа $k_{\text{DES}} = 56$ та AES з $k_{\text{AES}} = 128$.

Розширення спектра ТСК з використанням ЛЧМ запропоновано на основі двох опорних несущих сигналів $S_{\text{ЛЧМ-1}}(T_c)$ і $S_{\text{ЛЧМ-2}}(T_c)$, частоти яких при модуляції імпульсів сигнальної конструкції змінюються за лінійним законом на інтервалі T_c. При цьому використовуються лінійно спадаючий та зростаючий закони зміни частот для $S_{\text{ЛЧМ-1}}(T_c)$ і $S_{\text{ЛЧМ-2}}(T_c)$ (рис. 15 (г)) відповідно. На рис. 15 (г) надано процес розширення спектра ТСК $x(T_c, \Delta)$ з параметрами: $m = 4$, $s = 4$, $i = 2$. Процес перемикання двох генераторів Г1 і Г2 ЛЧМ для підключення опорних сигналів $S_{\text{ЛЧМ-1}}(T_c)$ і $S_{\text{ЛЧМ-2}}(T_c)$ залежить від тривалості імпульсів у межах T_c (рис. 15 в), що забезпечує формування ШПС $S_{\text{ЛЧМ-ТСК}}(T_c)$. Приймання шумоподібного таймерного сигналу відбувається за допомогою двох кореляційних приймачів з генераторами Г1 і Г2 (рис. 17), які служать для формування опорних сигналів $S_{\text{ЛЧМ-1}}(T_c)$ і $S_{\text{ЛЧМ-2}}(T_c)$ відповідно. Результати перемноження $S_{\text{ЛЧМ-ТСК}}(T_c)$ на $S_{\text{ЛЧМ-1}}(T_c)$ і $S_{\text{ЛЧМ-2}}(T_c)$ на інтервалі часу T_c надходять на пристрій підсумування сигналів «+», вихід якого з'єднується з пристроєм визначення екстремуму (ПВЕ). ПВЕ фіксує максимальне і мінімальне значення напруги сигналу, що дає змогу вирішальному пристрою (ВП) визначити на інтервалі часу Δ.

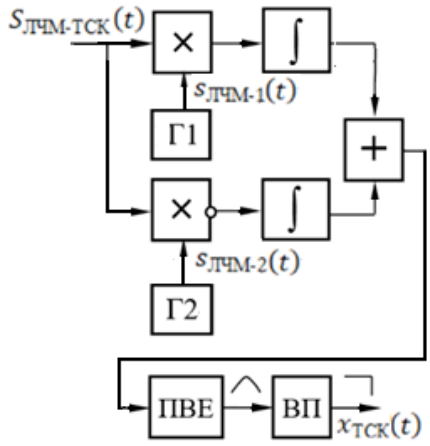

Рисунок 17 - Структурна схема кореляційного приймача

Система зв'язку повинна мати достатньо точну систему тактової і циклової синхронізації для відновлення фронтів імпульсів ТСК на інтервалі T_c. Наприкінці кожного інтервалу часу T_c здійснюється обнуління інтеграторів імпульсами, що формуються за допомогою пристрою циклової синхронізації приймача. Проведено імітаційне моделювання ЛЧМ таймерного сигналу в каналі з шумом. На рис. 18 надано часові діаграми відновлення фронтів таймерного сигналу за допомогою двох кореляційних приймачів: (а) – шумоподібний таймерний сигнал $U_{\text{шпс}}$ на вході приймача $h = P_c/P_i = 0{,}25$; (б) – результуючий сигнал з виходу пристрою складання сигналів «+»; (в) – визначення ЗМВ ТСК за максимальним та мінімальним значенням напруги сигналу $U_{\text{інт}}$, що надходять з ПВЕ. Проведене імітаційне моделювання дало

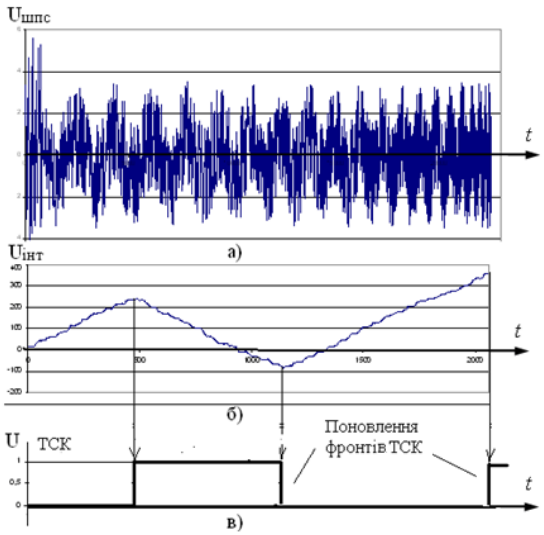

Рисунок 18 - Кореляційний прийом шумоподібного таймерного сигналу

змогу визначити, що відновлення фронтів сигналу можливе навіть за умови, коли шум набагато більше корисного сигналу.

У шостому розділі з урахуванням структури побудови ТСК та вимог із забезпечення завадостійкості запропоновано алгоритми розширення спектра. Проведені розрахунки структурної прихованості шумоподібних таймерних сигналів. За критеріями частотної та енергетичної ефективності використання каналу надана оцінка умовам забезпечення енергетичної прихованості для методів розширення спектра.

У **висновках** наведено основні наукові досягнення й отримані результати. Вказано також перспективи подальших досліджень за темою цієї роботи.

У **додатках** роботи надано відповідні акти реалізації та впровадження дисертаційного дослідження.

ВИСНОВКИ

У дисертаційній роботі наведено нове вирішення науково-технічної проблеми підвищення захищеності ІКС. Обґрунтовано доцільність комплексного підходу до захисту інформації від НСД. Надано оцінку комбінованим методам захисту інформації в умовах радіоелектронного конфлікту. Запропоновано відповідні критерії й показники ефективності метода мів передавання даних на основі розроблених алгоритмів розширення спектра таймерних сигналів.

Отримано нові наукові й практичні результати, що полягають в такому:

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 з урахуванням ресурсів каналу, що полягає в такому: найбільша енергетична прихованість у того метода передавання, який при заданій смузі широкосмугового сигналу ΔF і заданої достовірності передавання інформації забезпечує найменше співвідношення сигнал/шум h_0^2, тобто $\min h_0^2 = E\{\Delta F; P_{\text{НП}}(n)\}$; найбільша потенційна структурна прихованість у того метода формування сигнальних конструкцій, який на заданому інтервалі часу побудови сигнальних конструкцій $T_{\text{СК}}$ і необхідної достовірності передавання забезпечує можливість синтезу більшого числа комбінацій А, тобто $\max \text{A} = S\{T_{\text{СК}}; P_{\text{НП}}(n)\}$.

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. Дослідження показали, що використання таймерних сигналів з параметрами m = 5, s = 7, $N_{\text{рТСК}}$=680 забезпечує збільшення відносної швидкості передавання інформації на інтервалах «хорошого» стану каналу (відношення сигнал/шум h = 12, $P_{\text{пТСК}}$= $1{,}79\times10^{-4}$) з $R_{\text{РЦК}}$ =0,55 для РЦК з параметрами n = 9, m = 5, $t_{\text{в}}$= 1, $N_{\text{рРЦК}}$=512, $P_{\text{пРЦК}}$= $1{,}4\times10^{-2}$ до $R_{\text{ТСК}}$=1,88. Це свідчить про те, що використання таймерних сигналів на

інтервалі «хорошого» стану каналу дозволяє зменшити час передавання інформації в три рази і більше. Сумісне використання ТСК і РЦК дозволяє підвищити завадостійкість в 1,59 рази при збільшенні $R_{\text{РЦК}}$ =0,55 до $R_{\text{РЦК-ТСК}}$ =1,05, що свідчить про зменшення часу передавання заданого обсягу інформації в два рази.

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. Доведено, що збільшення структурної прихованості можливо на обмеженому інтервалі часу передавання інформації за допомогою таймерних сигналів у порівнянні з позиційними кодами. Так, для $n = 7$, $i = 3$ і $s = 5$ число реалізацій $N_{\text{р}}$=1771 та структурної прихованості $S_{\text{тск}}$ = 11, тоді як для РЦК всього $N_{\text{рРЦК}}$=2^7=128 та $S_{\text{рцк}}$ = 7. Визначено, що використання ТСК в якості завадостійкого коду з мінімальною кодовою відстанню $d_0 = 2, 3, 4, 5$ зменшує кількість дозволених комбінацій у порівнянні з $N_{\text{р}}$=1771 в 2, 7, 12, 22 рази відповідно. Така закономірність характерна для множин ТСК з іншими параметрами n, i та s. Результати дослідження дали змогу виявити зворотну закономірність між показниками структурної прихованості і завадостійкості, що пов'язана із зменшенням базового елементу побудови таймерних сигналів Δ або/та збільшення кодової відстані. Для вирішення цієї проблеми запропоновано використання більшої кількості різних множин ТСК у процесі передавання інформації. Такий підхід дозволяє компенсувати зменшення показника структурної прихованості при обмеженому значенні Δ та кодової відстані, які потрібні для забезпечення заданої достовірності.

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. Запропоновано враховувати ентропію дискретного джерела інформації для визначення кількості випадкових комбінацій для кожного символу b_i алфавіту залежно від ймовірності його появи. Такий підхід штучно змінює ентропію джерела видачі інформації з нерівномірним законом появи символів у повідомленні з $H_{\text{НР}}(U)$ = 4,42 до $H_{\text{Р}}(U)$ = 5 (для алфавіту з 32 символів) та забезпечує рівноймовірний закон появи кодових комбінацій у шифрограмі. Оцінку ефективності стохастичного шифрування зроблено на основі імітаційного моделювання для порівняльного аналізу варіантів залежно від загальної кількості використовуваних випадкових комбінацій N_1 та довжини випадкової комбінації n. Визначено, що варіант реалізації системи стохастичного шифрування, у якому використовується підбір випадкових кодових комбінацій шифрограми з урахуванням ймовірності появи символу в тексті дозволяє зменшити дисперсію залежно від довжини кодової комбінації n=9, 10, …, 17 у межах від 28, 47, … , 57269 рази відповідно, що забезпечує зменшення дисперсії $D_{xy} \to 0$. Це дозволяє формувати потік випадкових комбінацій шифрограми з приблизно рівними ймовірностями появи та ускладнити використання частотного тесту при

дешифруванні перехопленого повідомлення. Для компенсації надлишковості випадкових комбінацій стохастичного шифрування і блокового кодування запропоновано використання ТСК.

5. Уперше встановлено закономірності впливу параметрів ТСК на рівень структурної прихованості та завадостійкості шумоподібних сигналів. Визначено, що з погляду зменшення складності прийому шумоподібних таймерних сигналів доцільно використовувати фіксоване значення ЗММ i, кількість реалізацій яких при цьому залежить від інтервалів Найквіста m та елементів s. Аналіз впливу фіксованої кількості ЗММ в ТСК дозволяє зробити висновок, що максимальна кількість реалізацій може бути досягнута при певному значенні i, яке, як правило, менше m на 2-4 позиції. Визначено вплив зростання числа реалізацій ТСК при збільшенні інтервалів побудови m =6, 7, … , 19, що дозволяє підвищити структурну приховність $S(s{=}7,\ i{=}4)$ в межах від 12 до 22 дв. вим. Збільшення кількості реалізацій можливо шляхом використання ТСК з різним ЗММ, що дозволяє підвищити структурну приховність. Так при $S(m$ =19, s=6, i=1, 2, … , 19) =40 дв. вим., що у порівнянні з $S(m$ =19, s=6, i=4) =21 дв. вим. більше майже у 2 рази. Обґрунтовано вибір оптимального значення параметра $s_{\text{опт}}$ залежно від h^2 в каналі, при якому забезпечується максимальна пропускна здатність $C_{\text{тск}}$. Визначено, що зменшення часового інтервалу Δ при $s > s_{\text{опт}}$ для числа реалізацій ТСК та підвищення прихованості призводить до збільшення показника втрат $H_{\text{з}}$, який характеризує збільшення спотворених сигнальних конструкцій. Отже, виявлено протиріччя між умовою підвищення структурної прихованості шляхом збільшення s та необхідністю обмеження цього показника значенням $s \le s_{\text{опт}}$ при заданому m та відношенням сигнал/шум h.

6. Розвинуто теорію систем зв’язку з шумоподібними сигналами на основі ТСК, що пов’язано з розробкою нових алгоритмів розширення спектра для непозиційних сигналів та визначенням оптимальних параметрів таймерних сигналів. Запропоновано три умови забезпечення енергетичної прихованості для методів розширення спектра (ППРЧ, ПРС-ПВП та ЛЧМ) за критеріями частотної та енергетичної ефективності використання каналу: база сигналу $B = \Delta f T >> 1$ – перша умова; частотна ефективність $\gamma = R/\Delta f_{\text{еф}}$ – друга умова; ефективність використання каналу відповідно до потужності $\beta = R/h_0^2$ – третя умова. Аналіз показав, що методи ППРЧ та ЛЧМ задовольняють тільки двом умовам, а метод ПРС-ПВП задовольняє всі умови. З урахуванням особливостей побудови ТСК запропоновано загальний принцип розширення спектра на інтервалі часу побудови сигнальної конструкції T_c, що пояснюється непозиційністю імпульсів у порівнянні з позиційними РЦК. На загальне значення структурної прихованості ПРС-ПВП впливає структурні прихованості ТСК, ПВП та системи модуляції. При параметрах ТСК $m = 8,\ s = 5,\ i = 3$ структурна приховність $S_{\text{тск}} = 12$ дв. вим. Розширення спектра ТСК методом ПРС-ПВП ($B_{t_0} = 8,\ N_{\text{пвп}} = 64$) та використання ФМ-2 дозволяє досягти значення структурної прихованості $S_{\text{тск пвп}}$ =77 дв. вим. При базі ПВП $B_{t_0} = 16$ та $N_{\text{пвп}} = 128$ структурна приховність шумоподібного таймерного сигналу збільшується практично в 2 рази $S_{\text{тск пвп}}$ =141 дв. вим. При формуванні ШПС структура ПВП змінюється і становиться унікальною після розширення

спектра кожної ТСК.

Надано аналіз структурної прихованості шумоподібного ТСК при розширенні спектра методом ППРЧ. Використання швидкої ППРЧ дозволяє при параметрах ТСК $m = 4,\ s = 4$ та незначної кількості частот N_f=32 забезпечити наступну структурну прихованість $S_{\text{тск ппрч бп}} = 73{,}4$ і $S_{\text{тск ппрч п}} = 80$ для системи зв'язку з повторення та без повторенням несущих частот відповідно.

При комбінованому розширенні спектра на основі ПРС-ПВП і ППРЧ структурна прихованість шумоподібного таймерного сигналу збільшується в 2 рази і більше. Розширення спектра ТСК з параметрами $m = 8,\ s = 5,\ N_{\text{пвп}} = 32;\ i = 3,\ N_{\text{пвп}} = 64,$ $N_f = 32$ забезпечує структурну прихованість $S_{\text{тск пвп-ппрч}} = 157$ дв.вим. При інтерпретації структурної прихованості з криптостійкістю можна зробити висновок, що значення $S_{\text{тск пвп-ппрч}} = 157$ дв. вим. перевищує криптостійкість системи шифрування DES з довжиною ключа $k_{\text{DES}} = 56$ та AES з $k_{\text{AES}} = 128$. Надано імітаційне моделювання розширення ТСК за допомогою ЛЧМ, що дало змогу з'ясувати, що відновлення фронтів сигнальної конструкції можливо при значенні $h = 0{,}25$ на вході приймача, тобто коли шум перевищує корисний сигнал у 4 рази.

Розроблено нові алгоритми кореляційного прийому широкосмугових таймерних сигналів (для ПРС-ПВП та ЛЧМ), які враховують структуру побудови непозиційних сигналів.

Висока ефективність розроблених теоретичних положень, запропонованих методів захисту інформації на основі стохастичного шифрування і способів розширення спектра ТСК підтверджені результатами експериментальних досліджень, які одержано методами аналітичного та імітаційного моделювання.

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.

АНОТАЦІЯ

Кільдішев В. Й. Моделі та методи захисту інформації на основі параметричного перетворення передаваних сигнально-кодових конструкцій. – На правах рукопису**.**

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – системи захисту інформації. – Державний університет інтелектуальних технологій і зв'язку Міністерства освіти і науки України, Одеса, 2025.

Дисертаційну роботу присвячено важливій науково-практичній проблемі підвищення захищеності ІКС на основі інтеграції методів перетворення даних, що містить сумісне використання непозиційних таймерних та методів розширення спектра, хаотичних сигналів, стохастичного шифрування та завадостійкого кодування, алгоритмів зменшення спотворення кодових блоків шляхом декореляції помилок. Теоретично обґрунтовано систему оцінок захищеності методів передавання широкосмугових сигналів з урахуванням ресурсів каналу, які ґрунтуються на оптимальному використанні частотного й енергетичного ресурсів каналу зв'язку. Запропоновано метод зменшення часу передавання заданого обсягу інформації на основі сумісного використання таймерних і позиційних кодів, що важливо для підвищення ефективності системи зв'язку в умовах радіоелектронного конфлікту, а також надано оцінку реалізації методу адаптивного обміну якості інформації на швидкість передавання залежно від стану нестаціонарного каналу. Доведено доцільність вибору оптимальних параметрів таймерних сигнальних конструкцій для досягнення обґрунтованої структурної прихованості з урахуванням забезпечення максимальної пропускної спроможності в каналі при заданому значенні сигнал/шум. Удосконалено систему захисту інформації на основі комбінованих методів перетворення даних, за впровадження яких реалізовано багаторівневий захист інформації з використанням стохастичного шифрування з вибором оптимальної кількості випадкових комбінацій шифрограми, завадостійкого та таймерного кодування. Обґрунтовано використання таймерних сигналів для компенсації надлишкових елементів стохастичного шифрування та завадостійкого кодування. Запропоновано критерії вибору параметрів ТСК для завдання формування шумоподібних сигналів з урахуванням складності реалізації сигнальних конструкцій, забезпечення прихованості і завадостійкості. Обґрунтовано доцільність використання шумоподібних таймерних сигналів для підвищення структурної

прихованості сигнальних конструкцій, що важливо при передаванні секретних повідомлень в умовах радіоелектронного конфлікту.

Ключові слова: захист інформації, захищеність, НСД, прихованість передавання, розширення спектра, шумоподібний сигнал, стохастичне шифрування, таймерне кодування, псевдовипадкова послідовність, кодове розділення каналів.

ABSTRACT

Kildishev V. Increasing the security of telecommunications systems based on coding, encryption and spectrum spreading methods. – Manuscript copyright.

Dissertation for the doctor's degree of technical sciences in a specialty 05.13.21 – information security systems. – Odessa State University of Intellectual Technologies and Communications, Ukraine, Odessa, 2025.

The dissertation work is devoted to the important scientific and practical problem of increasing the security of telecommunication systems based on the integration of data conversion methods, which includes the joint use of non-positional timer and spread spectrum methods, chaotic signals, stochastic encryption and noise-resistant coding, algorithms for reducing code block distortion by decorrelation of errors. The proposed system of security assessments of broadband signal transmission methods taking into account channel resources, which are based on the optimal use of frequency and energy resources of the communication channel, is theoretically substantiated. A method for reducing the transmission time of a given volume of information based on the joint use of timer and positional codes is proposed, which is especially important for increasing the efficiency of the communication system in conditions of radio-electronic conflict, and an assessment of the implementation of adaptive exchange of information quality for the transmission speed depending on the state of the non-stationary channel is also provided. The feasibility of choosing the optimal parameters of timer signal structures to achieve reasonable structural concealment is proven, taking into account ensuring maximum bandwidth in the channel at a given signal/noise value. An improved information protection system based on integrated data conversion methods is implemented, in which multi-level information protection is implemented using statistical encryption with the selection of the optimal number of random combinations of the ciphertext, noise-resistant and timer coding. The use of timer signals to compensate for redundant elements of statistical encryption and noise-resistant coding is substantiated. Criteria for selecting TSC parameters for the task of forming noise-like signals are proposed, taking into account the complexity of implementing signal structures, ensuring concealment and noise resistance. The feasibility of using noise-like timer signals to increase the structural concealment of signal structures is substantiated, which is important when transmitting secret messages in conditions of radio-electronic conflict.

Keywords: information protection, security, unauthorized access, transmission secrecy, spectrum spreading, noise-like signal, statistical encryption, timer coding, pseudo-random sequence, code division multiplexing.

Подписана до друку 16.10.2025 р.
Обсяг 1,9 друк. арк. Формат 60х88/16.
Тираж 100 прим. Папір друкарський. Різографія.
Надруковано з готового оригінал-макету.
Копіцентр «Магістр»
65000, м. Одеса, вул. Мечникова, 36
тел. (098) 878-74-36