Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)

Кафедра Інфокомунікаційної інженерії ім. В.В. Поповського
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Дослідження методів мінімізації уразливості систем передачі з прямим розширенням спектра
(тема)

Виконав:
студент _2_ курсу, групи ___АМСЗІм-22-2_____
Руденко О.С.
(прізвище, ініціали)
Спеціальність: _____125 Кібербезпека_____
(код і повна назва спеціальності)
Тип програми: _____освітньо-професійна_____
(освітньо-професійна або освітньо-наукова)
Освітня програма: _Адміністративний менеджмент__
у сфері захисту інформації
(повна назва освітньої програми)

Керівник: _доцент кафедри ІКІ ім. В.В. Поповського_
Філіппенко О.І.
(посада, прізвище, ініціали)

Допускається до захисту
Зав. кафедри _____ ___Лемешко О.В.___
(підпис) (прізвище, ініціали)

2024 р.

Харківський національний університет радіоелектроніки

Факультет _____Інфокомунікацій_____
(повна назва)
Кафедра _____Інфокомунікаційної інженерії імені В.В. Поповського_____
(повна назва)
Рівень вищої освіти _____другий (магістерський)_____
Спеціальність _____125 Кібербезпека_____
(код і повна назва)
Тип програми _____освітньо-професійна_____
Освітня програма __Адміністративний менеджмент у сфері захисту інформації___
(повна назва)

ЗАТВЕРДЖУЮ
Зав. кафедри_____
(підпис)
«____» _____2024р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту _____Руденку Олексію Сергійовичу_____
(прізвище, ім'я, по батькові)
1. Тема роботи: __Дослідження методів мінімізації уразливості систем передачі з прямим розширенням спектра_____
затверджена наказом по університету від «03» _листопада_ 2023р. №1291 Ст.
2. Термін подання студентом роботи до екзаменаційної комісії___25.01.2024р.____
3. Вихідні дані до роботи: системи передачі з прямим розширенням спектру DSSS
4. Перелік питань, що потрібно опрацювати в роботі:
1) Аналіз методів формування та синхронізації DSSS сигналів_____
2) Аналіз принципів побудови приймального тракту системи DSSS, визначення способів блокування прийому сигналів_____
3) Аналіз методів протидії системам з DSSS, аналіз впливу та ефективності кожного з них, дослідження їх ефективності при різних умовах_____
4) Аналіз методів захисту від кожного типу протидії_____
5) Аналіз проблем у системах, що використовують DSSS (IEEE802.11 та IEEE802.15.4)_____
6) Моделювання системи з DSSS в умовах дії однотонового глушіння та адитивного білого гаусівського шуму (АБГШ), побудова графіків ефективності глушіння_____

5. Перелік графічного матеріалу із зазначенням креслень, плакатів, комп'ютерних ілюстрацій: _____Демонстраційний матеріал у вигляді ppt-презентації_____

6. Консультанти розділів роботи

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		(підпис)	(дата)
Основна частина	доцент Філіппенко Олег Ігорович		

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання	06.11.2023	Виконано
2	Збір матеріалів для дослідження	13.11.2023	Виконано
3	Розробка 1 розділу	22.11.2023	Виконано
4	Розробка 2 розділу	04.12.2023	Виконано
5	Розробка 3 розділу	19.12.2024	Виконано
6	Розробка 4 розділу	26.12.2023	Виконано
7	Розробка 5 розділу	05.01.2024	Виконано
8	Оформлення кваліфікаційної роботи	12.01.2024	Виконано

Дата видачі завдання _____6 листопада 2023 року _____

Студент _____Руденко О.С.
(підпис)

Керівник роботи _____Філіппенко О.І.
(підпис)

РЕФЕРАТ

Пояснювальна записка: 77 с., 28 рис., 3 табл., 17 джерел.

ШИРОКОСМУГОВИЙ СИГНАЛ, ПРЯМЕ РОЗШИРЕННЯ СПЕКТРА, ПСЕВДОВИПАДКОВА ПОСЛІДОВНІСТЬ, ГЛУШІННЯ, ІНТЕРФЕРЕНЦІЯ, БЕЗПРОВОДОВИЙ ЗВ’ЯЗОК

Об'єкт дослідження – процес передачі даних в системах з прямим розширенням спектра.

Предмет дослідження – вразливості систем передачі з прямим розширенням спектра.

Мета роботи – дослідження потенційних ризиків для систем комунікацій з прямим розширенням спектру через аналіз їх характеристик, методів формування, а також засобів мінімізації вразливостей цих систем.

Методи досліджень – моделювання, спостереження, аналіз та порівняння.

Безпроводові системи передачі інформації відіграють ключові значення в функціонуванні всіх галузей людської цивілізації. Збільшення кількості радіопередаючих пристроїв призводить до постійного погіршення сигнально-перешкодної обстановки і, в той же час, невпинно розвиваються та вдосконалюються методи протидії безпроводовим системам, спрямовані на перехоплення інформації, ускладнення та навіть унеможливлення функціонування зазначених систем.

У роботі виконано дослідження принципів побудови систем з DSSS (Direct Sequence Spread Spectrum), проаналізовані основні типи загроз та наведені рекомендації, спрямовані на мінімізацію шкідливого впливу основних методів протидії.

Запропоновано імітаційну модель системи з DSSS для дослідження її функціонування в умовах впливу АБГШ та тонової перешкоди.

ABSTRACT

The report contains: 77 p., 28 fig., 3 tables, 17 sources.

WIDEBAND SIGNAL, DIRECT SPREAD SPECTRUM, PSEUDORANDOM SEQUENCE, JAMMING, INTERFERENCE, WIRELESS COMMUNICATION

The research object is the process of data transmission in systems with a direct spread spectrum.

The subject of research is vulnerabilities of transmission systems with direct spectrum expansion.

The aim of the work is investigation of potential risks for communication systems with direct spectrum expansion through the analysis of their characteristics, methods of formation, as well as means of minimizing the vulnerabilities of these systems.

Methods of research are modeling, observation, analysis and comparison.

Wireless data transmission systems play a key role in the functioning of all branches of human civilization. The increase in the number of radio transmitting devices leads to a constant deterioration of the signal and interference situation, and at the same time, the methods of countering wireless systems are constantly being developed and improved, aimed at intercepting information, complicating and even preventing the functioning of these systems.

The research of the principles of building systems with DSSS was carried out, the main types of threats were analyzed, and recommendations aimed at minimizing the harmful effects of the main jamming techniques were presented.

A simulation model of the system with DSSS is proposed. The model can be used to investigate the performance of a system with DSSS under the influence of AWGN (Additive White Gaussian Noise) and single tone jamming.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

АБГШ – адитивний білий гаусівський шум

АРП – автоматичне регулювання підсилення

ПВП – псевдовипадкові послідовності

ПР – показник розрізнення

РЕВ – радіоелектронний вплив

РС – радіоспостереження

ШШС – широкосмугові шумоподібні сигнали

AJ – Antijam

AWGN – Additive White Gaussian Noise

BBN – Broadband Noise

BER – Bit Error Rate

BPSK – Binary Phase Shift Key

CDMA – Code Division Multiple Access

CW – Continuous Wave

DSSS – Direct Sequence Spread Spectrum

FHSS – Frequency Hopping Spread Spectrum

JSR – Jam to Signal Ratio

PBN – Partial-Band Noise

PN-код – псевдовипадковий код (послідовність бітів, яка виглядає як випадковий шум)

QPSK – Quaternary Phase Shift Key

SIR – Signal to Interference Ratio

SNR – Signal to Noice Ratio

THSS – Time Hopping Spread Spectrum

WLAN – Wireless Local Area Network

WPAN – Wireless Personal Area Network

WSN – Wireless Sensor Network

XOR – виключне «АБО»

ВСТУП

На сьогоднішній день безпроводові системи передачі інформації не тільки стали невід'ємною частиною нашого повсякденного життя, можна з впевненістю сказати, що вони відіграють ключові значення в функціонуванні всіх галузей людської цивілізації. Збільшення кількості радіопередаючих пристроїв призводить до постійного погіршення сигнально-перешкодної обстановки і в той же час постійно розвиваються засоби виявлення каналів зв'язку і методи несанкціонованого доступу для отримання інформації або радіопригнічення. Враховуючи вищезазначене, забезпечення захисту передачі даних по радіоканалам є критично важливою задачею.

Однією з технологій, що дозволяють частково вирішити зазначені проблеми в системах передачі інформації, є методи з розподіленим спектром, зокрема, системи з прямим розширенням спектра (DSSS – Direct Sequence Spread Spectrum). Хоча DSSS забезпечує стійкість до перешкод і конфіденційність передачі даних, вона також може бути уразливою перед атаками, такими як перехоплення інформації, передача хибних даних або постанова завад, які ускладнюють або унеможливлюють роботу мережі.

Метою даної роботи є виявлення потенційних ризиків для систем з DSSS через дослідження характеристик сигналів, методів їх формування та обробки, дослідження існуючих методів протидії системам з DSSS задля подальшої розробки рекомендації спрямованих на зменшення вразливостей комунікаційних систем.

Перший розділ присвячено загальним даним про системи зв’язку з прямим розширенням спектру, наведені основні характеристики, їх властивості, переваги та недоліки, а також сучасні технології зв’язку, що використовують пряме розширення спектра.

Далі проведено аналіз методів формування, передачі, прийому та обробки сигналів комунікаційної системи, який дозволив виявити деякі потенційні вразливості, притаманні системам з DSSS.

Третій розділ присвячено дослідженню найбільш поширених технологій протидії системам передачі з прямим розширенням спектра, проаналізовано їх вплив на роботу систем та їх ефективність при різних умовах. Аналіз, проведений

в другому і третьому розділах дозволив запропонувати ряд рекомендації для захисту систем з DSSS від кожного типу протидії.

Четвертий розділ присвячено аналізу проблем у безпроводових мережах стандартів IEEE 802.11 та IEEE 802.15.4.

В п’ятому розділі наведено короткий опис реалізованої імітаційної моделі системи з DSSS для дослідження впливу АБГШ та однотонової перешкоди. Також представлені результати чисельного моделювання та їх аналіз.

Окремі результати роботи доповідались на двох міжнародних наукових конференціях [1, 2].

1 СИСТЕМИ ПЕРЕДАЧІ З ПРЯМИМ РОЗШИРЕННЯМ СПЕКТРА

В даному розділі наведені основні характеристики систем з DSSS (Direct Sequence Spread Spectrum), їх властивості, переваги та недоліки, а також сучасні технології зв’язку, що використовують пряме розширення спектра.

1.1 Розширення спектра прямою послідовністю

Відомо [3], що більшість проблем, які притаманні системам безпроводової передачі інформації, можуть бути вирішені при використанні широкосмугових шумоподібних сигналів (ШШС). Основною ідеєю використання передачі з розширенням спектра, є можливість розширення спектра корисної інформації в смугу, яка у багато разів перевищує смугу сигналу повідомлення.

За методом модуляції розділяють наступні технології розширення спектра сигналу, що передається [4]:

– розширення спектру прямою послідовністю (DSSS) або пряме розширення спектру за допомогою ПВП (Псевдо-Випадкової Послідовності);

– розширення спектра за допомогою стрибків по частоті (FHSS – Frequency Hopping Spread Spectrum);

– розширення спектра за допомогою стрибків у часі (THSS – Time Hopping Spread Spectrum), де сигнал передається у визначених часових інтервалах (вікнах або слотах), які виникають псевдовипадково, а на приймальному боці синхронізується робота приймача саме для конкретних часових вікон;

– лінійна частотна модуляція сигналів (chirp modulation);

– комбіновані методи розширення спектру.

В рамках даної роботи нас цікавить саме розширення спектру прямою послідовністю. Основна ідея такого розширення полягає в тому, що при передачі сигнал розподіляється на більш широкий спектр частот, ніж потрібно для передачі самої інформації. Це досягається шляхом додавання до вихідного сигналу псевдовипадкового шуму, відомого як код чи спектральний код (spread code).

Відповідно, до опису систем з DSSS, що наведено в [5], вони поширюють цифровий сигнал, що несе інформацію, по широкій смузі пропускання, і ця смуга пропускання займається миттєво, тобто сигнал поширюється по всій смузі пропускання одночасно. Взяття обмеженого енергетичного сигналу даних і

поширення цієї енергії в дуже широкій смузі пропускання призводить до того, що енергія, присутня на будь-якій конкретній частоті або малому діапазоні частот, буде мінімальною. Часто вона настільки мала, що є нижчою за тепловий шум на цій частоті. Приймачі, які просто досліджують спектр на відповідній частоті роботи таких систем зв'язку, помилково сприймуть сигнал за шум і промахнуться. Для виділення вхідного сигналу з шуму і відновлення вихідних даних потрібен приймач, який знає спектральний код.

Основне покликання використання DSSS – підвищення стійкості до перешкод і забезпечення безпеки передачі даних але, не дивлячись на це, цим системам все ж притаманні деякі вразливості.

1.2 Властивості систем з прямим розширенням спектра

Властивості систем передачі з прямим розширенням спектра, наведені в даному розділі було отримано в результаті аналізу наступних публікацій [3, 4, 6].

1) Низька ймовірність перехоплення. Оскільки DSSS сигнал використовує весь час практично повну широкосмугову ділянку виділеного спектру, то це призводить до дуже малої нормованої за частотою щільності потужності (ват/герц). Часто ці сигнали знаходяться нижче рівня шуму в точці прийому. Цей факт суттєво ускладнює детектування такого сигналу і відповідно, визначає малу ймовірність перехоплення чи втручання в передачу даних.

2) Використання кодувальних послідовностей для розподілу сигналу по спектру, що включає в себе множення кожного біта даних на біт кодувальної послідовності.

Кодування забезпечує захист інформації, що передається від підслуховування («чужий» DSSS-приймач використовує іншу кодову послідовність і не зможе декодувати інформацію не від свого передавача). При цьому при використанні на приймачі іншої кодової послідовності на виході смугового фільтра сильно зменшується відношення рівня сигналу, що передається до рівня шуму, (тобто випадкових або навмисних перешкод), так що переданий сигнал на виході фільтра вже як би невиразний в загальному шумі.

3) Стійкість до перешкод. Розподілення сигналу по широкому спектру дозволяє уникнути впливу окремих смуг частот, які можуть бути перешкодами або затримувати передачу даних. Завдяки частотній

надмірності система з використанням ШШС успішно працює за наявності в смузі ряду вузькосмугових перешкод. Уражені ділянки спектра можна вирізати без шкоди функціонування основної системи.

В свою чергу, можливість роздільного прийому одного або ряду променів, що запізнюються в умовах дії багатопроменевості, також підвищує завадостійкість прийому ШШС.

4) Можливість виявлення та корекції помилок. Деякі системи з прямим розширенням спектру можуть використовувати спеціальні коди для виявлення та виправлення помилок в передачі даних.

5) Сприймання слабких сигналів. Системи комунікацій можуть працювати навіть при низьких рівнях сигналу, дозволяючи сприймати сигнали в умовах слабкого зв'язку.

6) Енергетична скритність. Низький рівень спектральної щільності потужності дозволяє реалізувати скритність передачі даних та створити системи безпроводового зв’язку підвищеної скритності.

7) Сумісність з іншими радіосигналами.

Більше одного DSSS сигналу може існувати в одній і тій же смузі частот, оскільки кожен сигнал виглядає як випадковий шум для інших сигналів.

Ще одна надзвичайно корисна властивість DSSS-пристроїв полягає в тому, що завдяки низькому рівню щільності потужності сигналів у спектральній області вони практично не створюють перешкод звичайним радіопристроям (вузькосмуговим великої потужності), так як останні приймають широкосмуговий сигнал за шум в межах допустимого. І навпаки – звичайні пристрої не заважають широкосмуговим, тому що їх сигнали великої потужності «шумлять» кожен тільки у своєму вузькому каналі і не можуть повністю заглушити весь широкосмуговий сигнал.

8) Реалізація множинного доступу. Якщо багато користувачів використовують одночасно один і той же частотний канал, то відповідно велика кількість DSSS сигналів перекриваються у часі і за частотою. На приймальному боці когерентна демодуляція (кореляційний прийом) застосовується для витягнення кодової модуляції. Така обробка дозволяє сконцентрувати потужність сигналу саме від корисного абонента у вузькій смузі інформаційного сигналу. Якщо крос-кореляція між кодом абонента і іншими завадовими кодами мала, то когерентне детектування дозволяє у смузі пропускання інформаційного сигналу отримати значно меншу

потужність від завадових сигналів порівняно з сигналом корисного абонента.

Перелічені властивості роблять DSSS ефективним та доволі безпечним методом передачі даних у безпроводових мережах.

Також, слід зазначити, що наведені властивості притаманні не лише системам з DSSS, більшість з них є актуальними для систем з ШШС що використовують інші технології розширення спектра.

1.3 Переваги та недоліки технології розширення спектру прямою послідовністю

Аналіз переваг та недоліків технології розширення спектра з точки зору кібербезпеки дозволяє зрозуміти ризики та вигоди, пов'язані із застосуванням цієї технології в безпроводових мережах.

Основні властивості систем з DSSS, наведені в розділі 1.2, дозволяють навести перелік найбільш вагомих переваг таких систем, а саме:

– підвищена завадостійкість;

– можливість реалізації множинного доступу на підставі кодового розділення каналів;

– енергетична скритність завдяки низькому рівню спектральної щільності потужності;

– висока роздільна здатність під час вимірювання відстані;

– захищеність передачі даних;

– можливість протидіяти впливу навмисних завад;

– відносно невелика вартість реалізації;

– наявність сучасної елементної бази.

Відповідно до матеріалів, наведених в [3, 4, 5], можна сказати, що системам з DSSS притаманні наступні недоліки.

1) Висока споживана потужність. У порівнянні з іншими безпроводовими технологіями, які використовують менші ширини смуги, DSSS може вимагати більше потужності для передачі даних, що може бути недоцільним у пристроях які живляться від портативних джерел.

2) Складності, пов’язані з синхронізацією. Для виділення сигналу потрібна спеціальна обробка сигналу. Встановлення і підтримання

синхронізації прийнятого сигналу з кодовим сигналом приймача є достатньо складною задачею.

Необхідно відзначити, що самі по собі режими пошуку сигналу та синхронізації є найуразливішими режимами роботи радіоелектронної системи по відношенню до навмисних перешкод. Тривалість роботи у цих режимах напряму залежить від умов сигнально-перешкодової обстановки.

3) Зниження пропускної здатності, яке є пропорційним виграшу в завадостійкості, що не завжди прийнятно.

4) Залежність якості зв’язку від кількості користувачів. При використанні DSSS має місце поступове зниження якості зв’язку під час збільшення кількості користувачів, що одночасно займають один і той же радіоканал.

5) Сприйнятливість до множинного променевого розриву. Якщо сигнал дійсної передачі дістається до приймача через кілька різних шляхів (множинний променевий розрив), то це може викликати інтерференцію між сигналами і спотворення сигналу.

6) Низька ефективність спектра. Системи з прямим розширенням спектру використовують широкий спектр для передачі даних, що робить їх менш ефективним у використанні спектральних ресурсів, особливо в умовах обмеженої доступної смуги частот.

1.4 Технології зв’язку з прямим розширенням спектра

Для розуміння важливості захисту систем передачі даних з прямим розширенням спектра від різного роду кібернетичних загроз, розглянемо деякі сучасні безпроводові технології, які використовують DSSS модуляцію.

1) Wi-Fi (802.11b/g/n). Wi-Fi-мережі стандартів 802.11b, 802.11g і 802.11n використовують DSSS для передачі даних через безпроводове з'єднання.

Зокрема, 802.11b використовує DSSS для розширення спектра та забезпечення стійкості до перешкод. Цей стандарт працює у частотному діапазоні 2,4 ГГц та забезпечує швидкість передачі даних до 11 Мбіт/с.

2) Bluetooth. Стандарт Bluetooth також використовує DSSS в своїх специфікаціях передачі даних. Bluetooth – це безпроводова технологія для обміну даними між пристроями на невеликих відстанях.

3) Системи багатокористувацької комутації (CDMA – Code Division Multiple Access). В CDMA, кожен користувач використовує унікальний спектральний код (код користувача), який розширює його сигнал по всій ширині смуги частот. CDMA з DSSS використовується в безлічі мереж, включаючи безпроводові телефонні мережі, мобільний Інтернет, супутникові комунікації та інші безпроводові системи передачі даних.

4) Системи зв’язку для автомобілів (Car Communication Systems). DSSS застосовується в деяких безпроводових системах зв’язку для автомобілів, таких як системи зв’язку між автомобілями (V2V) і зв’язок між автомобілем та інфраструктурою (V2I).

5) Zigbee (802.15.4). Технологія Zigbee використовує DSSS для надійного безпроводового зв'язку в мережах в межах коротких відстаней, зазвичай для промислових та домашніх застосувань.

6) Digital Enhanced Cordless Telecommunications (DECT). DECT – це стандарт для безпроводового телефонного зв'язку, який також використовує DSSS для передачі голосу та даних між базовою станцією і безпроводовими телефонами.

7) Globalstar Satellite Communications. Globalstar використовує DSSS для безпроводового передавання голосу та даних через їх супутникову мережу.

Наведені приклади демонструють різноманітні галузі застосування DSSS у безпроводових комунікаціях. Дивлячись на них, можна зробити висновок, що кожна, без винятку, сучасна людина знайома як мінімум з такими технологіями як Wi-Fi, Bluetooth, CDMA та користується ними в повсякденному житті.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ФОРМУВАННЯ ТА СИНХРОНІЗАЦІЯ СИГНАЛІВ З ПРЯМИМ РОЗШИРЕННЯМ СПЕКТРА

Аналіз методів формування, передачі, прийому та обробки сигналів комунікаційної системи дозволяє виявити потенційні вразливості, притаманні системі що розглядається, а також запропонувати низку заходів спрямованих на усунення або послаблення виявлених вразливостей.

Розглянемо типові процеси, які мають місце в системах з прямим розширенням спектра при передачі даних.

В загальному випадку, система зв’язку з DSSS сигналами реалізується за наступним алгоритмом [7]:

– вихідний двійковий цифровий модулюючий сигнал модулюється псевдовипадковою кодовою послідовністю зі швидкістю, у кілька разів більшою, ніж швидкість передачі у вихідному сигналі;

– отриманий розширений сигнал має смугу частот яка в багато разів перевищує смугу частот інформаційного сигналу;

– кожному користувачу призначається своя власна персональна кодова послідовність, що має гарні кореляційні характеристики, тобто всі розширенні сигнали істотно відрізняються один від одного;

– розширений моделюючий сигнал використовується для модуляції несучої частоти одним із відомих методів, найчастіше використовують BPSK (Binary Phase Shift Key) або QPSK (Quaternary Phase Shift Key) фазову модуляцію;

– шумоподібний широкосмуговий сигнал випромінюється в ефір і всі користувачі одночасно працюють в виділеній смузі частот;

– в приймачі високочастотний сигнал переноситься на проміжну частоту, демодулюється і далі в baseband процесорі декодується за допомогою кодової послідовності, персонально призначеної даному користувачу і співпадаючою з кодовою послідовністю, що використовувалася при передачі цього сигналу; в результаті отримуємо вихідний інформаційний вузькосмуговий сигнал.

2.1 Фазова модуляція несучої частоти

Відповідно до [5, 8], Основними модуляціями, що використовуються для систем з прямим розширення спектру, є двійкова фазова модуляція (BPSK) та чотирьох фазова модуляція (QPSK).

Фазовий зсув несучого сигналу здійснюється шляхом накладення сигналу даних на несучу шляхом зміни фази останньої. Величина зміни фази залежить від кількості фазових станів. Для сигналу BPSK s(t) протягом інтервалу часу k,

$$s_k(t) = \sqrt{2R}\cos\left(2\pi f_0 t + d_k\frac{\pi}{2}\right), \qquad (k-1)T \le t < kT, \tag{2.1}$$

де R – середня потужність сигналу;

$d_k \epsilon \{+1, -1\}$ – представляє біти даних;

f_0 – несуча частота.

Для сигналу з двійковою модуляцією відбувається зсув фази на π радіан. Ці фазові стани проілюстровано на рисунку 2.1 а.

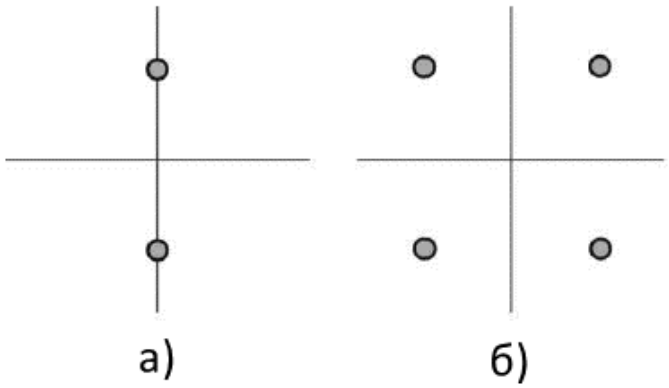

Рисунок 2.1 – Фазові стани модульованих сигналів

а) BPSK, б) QPSK

Спрощена схема комунікаційної системи зображена на рисунку 2.2. Двійкові цифри 1 і 0, або +1 і –1, представлені відповідними рівнями аналогового сигналу $+\sqrt{E_b}$ та $-\sqrt{E_b}$. Джерело інформації генерує послідовність інформаційних бітів, представлену $p(t)$. Вони модулюються на несучу та надсилаються через частину вільного простору каналу. Тут вони зазвичай пошкоджуються шумом і

перешкодами, перш ніж досягти приймача. У приймачі біти витягуються з несучої, генеруючи оцінку надісланих бітів, ці оцінки представлені $\hat{p}(t)$.

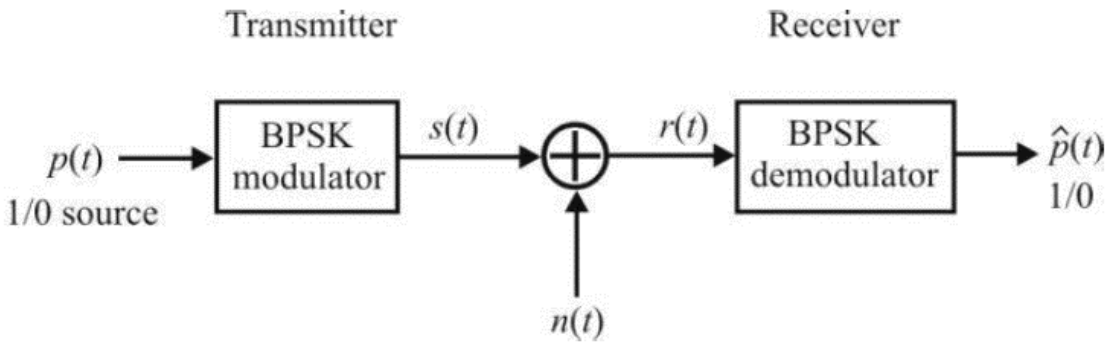

Рисунок 2.2 – Схема комунікаційної системи з двійковою фазовою модуляцією

Простий, але цілком ефективний модулятор для BPSK показаний на рисунку 2.3. Помноження несучої, створеної осцилятором на частоті f_0, на послідовність даних, представлену ±1, змушує фазу несучої змінюватися зі швидкістю передачі даних відповідно до послідовності даних.

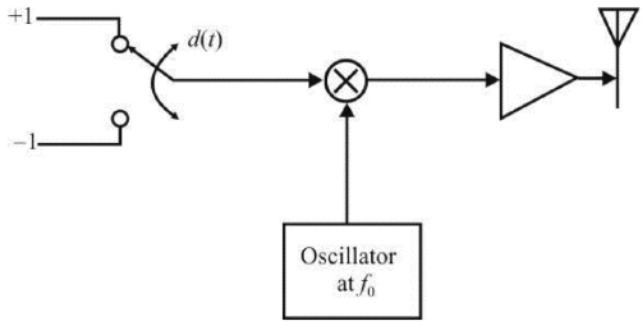

Рисунок 2.3 – Спрощена блок-схема передавача BPSK

Оптимальний детектор BPSK показаний на рисунку 2.4, який є корелятором, також відомим як узгоджений фільтр. Отриманий сигнал, спотворений шумом, спочатку множиться на сигнал, який є різницею між двома можливими безшумними символами. Потім отриманий продукт інтегрується для часу символу T. Інтегрований сигнал дискретизується в кінці періоду символу, при цьому вибірка порівнюється з пороговим значенням. Якщо поріг перевищено, то один із двох можливих символів оголошується присутнім. Якщо поріг не перевищений, то оголошується інший символ.

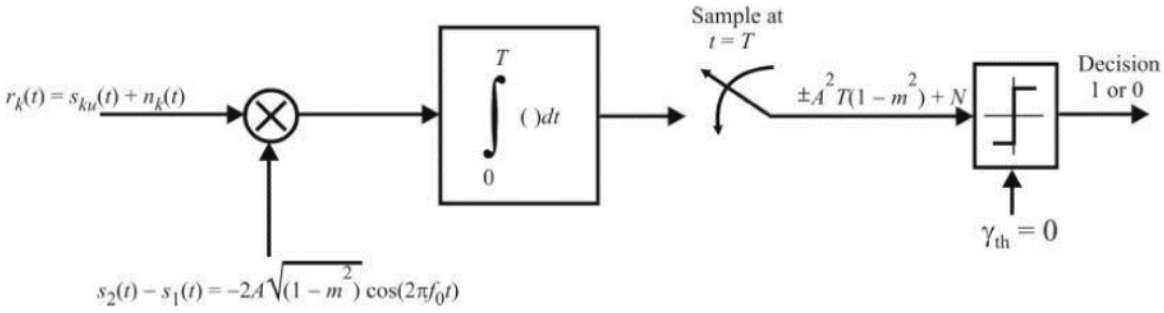

Рисунок 2.4 – Оптимальний кореляційний приймач для BPSK

В роботі [5] наведені дослідження продуктивності BPSK в АБГШ з перешкоджаючим тоном. Результати досліджень наведені на рис. 2.5 для різних рівнів відношення потужності сигналу до середньої потужності в тоні (SIR = R/I).

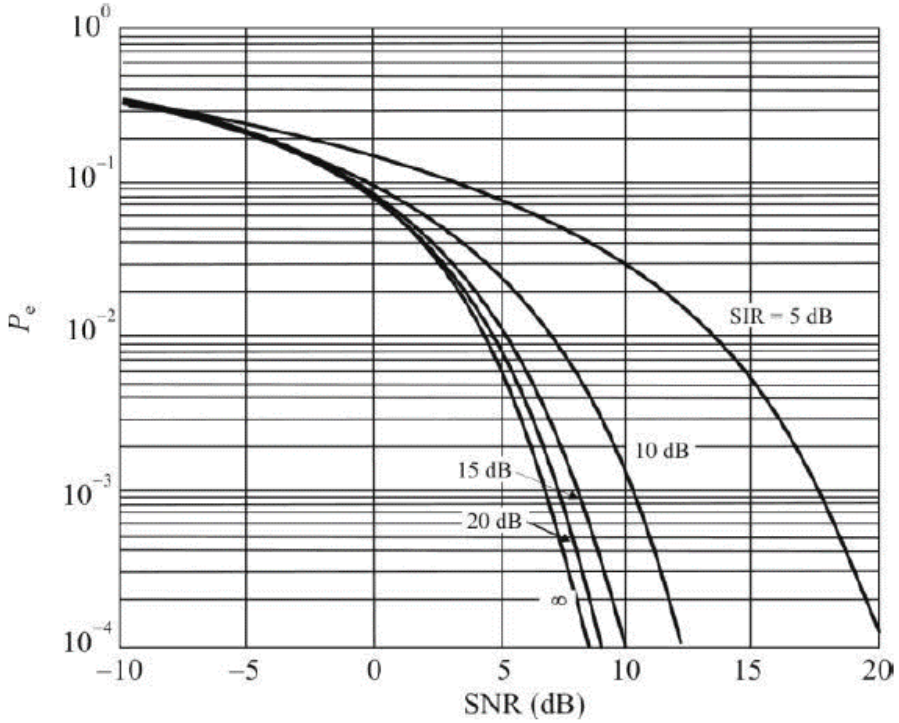

Рисунок 2.5 – Продуктивність BPSK в АБГШ з перешкоджаючим тоном

Аналіз графіка показує, що посилення сигналу перешкод призводить до погіршення продуктивності системи зв'язку з BPSK фазовою модуляцією. Слід зазначити, що цей результат є цілком закономірним, мета його наведення – порівняння з аналогійним графіком, наведеним нижче для системи з QPSK.

Чотирьох фазова модуляція являє собою подальший розвиток двійкової фазової модуляції. Для сигналу з чотирьох фазовою модуляцією (QPSK), де можливі 4 фазові стани, s(t) протягом інтервалу часу k,

$$s_k(t) = \sqrt{2R}\sin\left(2\pi f_0 t + d_k\frac{\pi}{2}\right), \qquad (k-1)T \le t < kT, \tag{2.2}$$

де $d_k \epsilon \{1, 3, 5, 7\}$ – представляє біти даних.

Фазові стани QPSK проілюстровано на рисунку 2.1 б. Значення фаз несучої зсунути відносно одна одної на $\pi/2$ радіан.

Незважаючи на більшу складність реалізації, основні причини використання чотирьох фазної модуляції полягають у тому, що в цих системах сигнал не піддається значним спотворенням, як двійковий сигнал, при проходженні разом з завадою через нелінійний пристрій і займає смугу радіочастот у 2 рази меншу в порівнянні з двійковим сигналом при тій самій швидкості передачі інформації. Інакше кажучи, при використанні чотирьох фазної модуляції в той самій смузі частот об'єм інформації що передається може бути збільшений вдвоє в порівнянні з двох фазною модуляцією.

Дослідження продуктивності QPSK в АБГШ з перешкоджаючим тоном наведені на рис. 2.6.

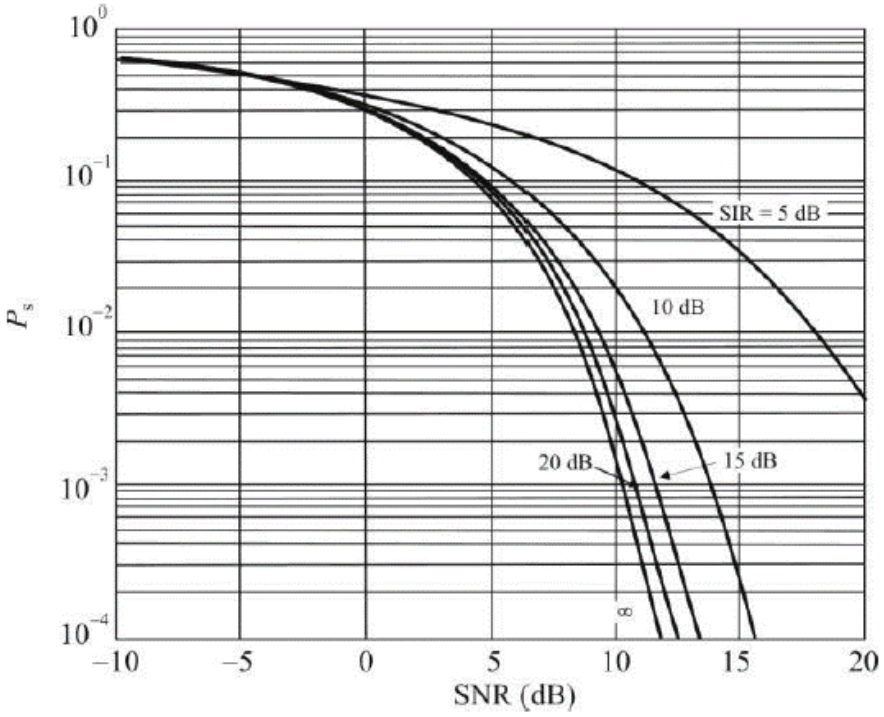

Рисунок 2.6 – Продуктивність QPSK в АБГШ з перешкоджаючим тоном

Порівнюючи рисунок 2.5 з рисунком 2.6, ми бачимо, що продуктивність QPSK приблизно на 5 дБ гірша, ніж BPSK за того самого рівня перешкоджаючого тону. Це означає, що QPSK вимагає сигналу на 5 дБ сильнішого, ніж BPSK, для того самого коефіцієнту бітових помилок (BER – Bit Error Rate) за наявності перешкод.

Тут і далі в поточній роботі ми будемо використовувати коефіцієнт BER в якості критерія ефективності протидії роботі комунікаційної системи. Так, для підтримання успішного спілкування в заданому діапазоні, фахівці зосереджуються на отриманні BER нижче значення 10^{-3} (в середньому один біт помилки з 1000). І, навпаки, зловмисники концентрують зусилля на розробку стратегії протидії комунікаціям задля підвищення цього значення до рівня 10^{-1} або більше. Якщо заявлений рівень BER 10^{-1} досягнутий, то можна зробити висновок щодо успішного глушіння комунікацій. Потенційно можливі рівні BER для різних технологій глушіння та за різних умов наведені в наступному розділі.

Таким чином, фазова модуляція QPSK має переваги щодо зайнятості спектру порівняно з BPSK модуляцією, однак характеристики системи зв’язку з QPSK більш чутливі до шуму та перешкод.

2.2 Виграш обробки

Відповідно до [4, 5, 7] найважливішою характеристикою систем з розширенням спектра є виграш обробки, який в свою чергу і визначає переваги, які надає розширення спектру сигналу. Також цей параметр називають коефіцієнтом посилення системи або коефіцієнтом розширення спектра сигналу та позначають, як G. Наведений нижче опис виграшу обробки було взято в [4].

Виграш обробки – це коефіцієнт, що показує, у скільки разів відношення сигнал/шум (S/N) або відношення сигнал/завада (S/I) на виході збільшується порівняно з аналогічними параметрами на вході системи.

Тобто виграш обробки може бути визначено як:

$$G=\frac{(S/N)_{вих}}{(S/N)_{вх}}. \qquad (2.3)$$

Досить часто виграш обробки оцінюється і з спектральної точки зору як:

$$G = \frac{\Delta f_{рч}}{\Delta F} = \frac{\Delta f_{рч}}{R} = \frac{\Delta f_{рч}}{f_b}, \quad (2.4)$$

де $\Delta f_{рч}$ – ширина смуги пропускання для радіочастотного сигналу;

ΔF – ширина смуги модулюючого сигналу;

$R = f_b$ – швидкість передачі інформації.

Оскільки ширина спектра радіочастотного сигналу з розширеним спектром практично визначається спектром ПВП, то його можна визначити як відношення частоти слідкування дискретів f_d до частоти $F = f_b$, з якою надходить інформаційна послідовність.

$$G = \frac{f_d}{F}. \quad (2.5)$$

Тобто, виграш обробки можна трактувати, як системний виграш, який відображує ті переваги, які надає розширення спектру сигналу.

Високе значення виграшу обробки приводить до таких позитивних наслідків:

– покращується ослаблення завад, оскільки властивості системи зв’язку стосовно завадостійкості прямо пропорційні значенню G;

– ємність системи зв’язку також прямо пропорційна виграшу обробки.

Тому, збільшення швидкості передачі псевдо-випадкового коду (а значить і більше розширення смуги частот, що займає сигнал) покращує характеристики системи у цілому.

З поняттям виграшу обробки G також пов’язаний ще один параметр, який визначає якісні характеристики системи з розширеним спектром, а саме коефіцієнт завадозахищенності.

Коефіцієнт завадозахищенності M враховує необхідне значення відношення сигнал/шум і можливі енергетичні втрати під час реалізації системи (L_c) і визначається за наступним виразом:

$$M_I = G - [L_c + (S/N)_{вих}]. \quad (2.6)$$

Смуга радіочастот, що задіяна при передачі сигналу розширеного спектра, здійснює безпосередній вплив на характеристики системи [8]. Так, якщо для системи виділена смуга 20 МГц, то виграш обробки буде обмежений саме цією смугою 20 МГц.

В свою чергу, використання фазової модуляції QPSK вполовину зменшує смугу радіочастот і відповідно виграш обробки також буде функцією половини смуги частот. Наприклад, якщо система передачі інформації при використанні BPSK модуляції потребує смуги радіочастот шириною 20 МГц, то застосування QPSK модуляції скорочує необхідну смугу частот до 10 МГц, що зменшує коефіцієнт виграшу на 3 дБ.

2.3 Коди псевдовипадкового розширення

Ключовим аспектом для технологій зв’язку з прямим розширенням спектра є використання ПВП. Зазначені послідовності використовуються для формування сигналів DSSS систем та спрямовані на вирішення наступних задач.

1) Розширення спектру. ПВП, також відомі як спектральні коди, використовуються для розширення спектру сигналу. Це означає, що сигнал розподіляється по широкому діапазону частот, що допомагає уникнути інтерференції та знижує ймовірність перехоплення сигналу.
2) Забезпечення стійкості до перешкод. Завдяки використанню псевдовипадкових послідовностей, сигнал стає стійким до перешкод, таких як шум, інші сигнали та електромагнітна інтерференція.
3) Безпека і конфіденційність. Послідовності виглядають як випадковий шум для чужих приймачів. Це робить системи з DSSS більш захищеним від перехоплення сигналу і забезпечує конфіденційність передачі даних.
4) Ідентифікація користувачів. Кожен користувач може мати свою унікальну ПВП. Це дозволяє ідентифікувати конкретних користувачів в мережі та відокремлювати їхні сигнали від інших користувачів.
5) Виправлення помилок. Деякі послідовності можуть бути використані для виявлення та виправлення помилок в передачі даних, що підвищує надійність зв'язку.

Вибір типу кодових послідовностей в широкосмугових системах, їх довжини та частоти проходження символів накладає певні обмеження на

можливості систем, а їх аналіз дозволяє виявити потенційні загрози та ризики з точки зору інформаційної безпеки.

Існує багато варіантів генерації кодів псевдовипадкового розширення [5, 9], лише декілька з яких будуть описані в даній роботі. Зокрема, m-послідовності та коди Голда. Враховуючи, що більшість послідовностей зазвичай, але не завжди, генеруються за допомогою регістрів зсуву, ми також торкнемося цієї теми в поточному розділі. Матеріали, наведені нижче у розділі, були отримані при аналізі даних з [4, 8].

Вибір кодової послідовності є дуже важливим як з точки зору реалізації множинного доступу, так і боротьби з міжсимвольною інтерференцією. До кожної кодової послідовності, яка генерується за допомогою набору кодо-генеруючих функцій, висувається декілька важливих вимог.

– кодова послідовність повинна бути періодичною і мати постійну довжину;

– кодова послідовність повинна бути легко відокремлена від її зсунутої у часі копії;

– кодова послідовність повинна бути легко відокремлена від інших кодових послідовностей.

Перші дві вимоги особливо важливі з точки зору боротьби з наслідками ефекту багатопроменевого розповсюдження, який проявляються як у зовнішньому середовищі, так і в середині приміщень. Третя вимога є важливою саме з точки зору ефективної реалізації множинного доступу. Для визначення відмінностей у кодових послідовностях відповідно до першої і другої вимог коди необхідна оцінка автокореляційної та взаємної кореляційної функцій.

Існує декілька можливих варіантів генерації кодових послідовностей. Один з найбільш розповсюджених методів є генерація кодової послідовності за допомогою регістрів зсуву зі зворотним зв’язком.

Регістр зсуву представляє собою набір комірок (які нумеруються від 1 до r) і кожна комірка містить інформацію, яка під дією тактового імпульсу зсуває свій вміст до виходу в процесі зчитування нового контенту на вході регістру. У стандартній конфігурації регістра зсуву зі зворотним зв’язком вхід комірки m буде функцією комірки m-1, а вихід комірки r (остання комірка регістру зсуву) формує бажану кодову послідовність. Функція, що зв’язує виходи комірки m-1 і комірки r з входом комірки може бути як лінійною так і нелінійною. Узагальнена схема генерації кодової послідовності зображена на рисунку 2.7.

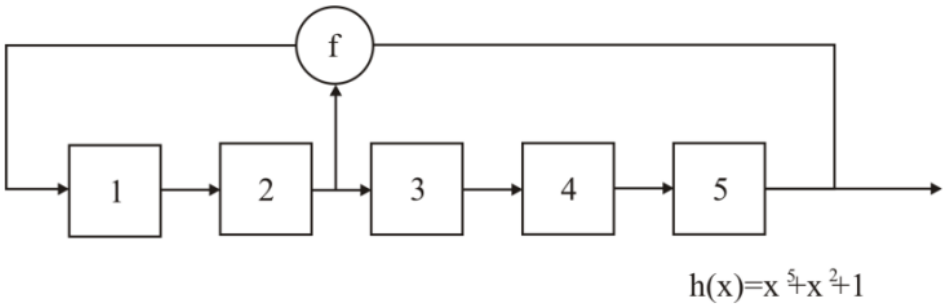

Рисунок 2.7 – Узагальнена структурна схема генерації кодової послідовності

В результаті можливі варіанти реалізації регістрів зсуву як з лінійним зворотним зв'язком, та і з нелінійним.

У загальному випадку конфігурація лінійного двійкового регістру зсуву з n комірок описується генеруючим поліномом степені n.

$$h(x) = h_n x^n + h_{n-1} x^{n-1} + \ldots + h_1 x^n + h_n x^1 + 1 \qquad \left(h_i \in \{0,1\}\right). \tag{2.7}$$

Число n визначає кількість комірок у регістрі зсуву. Наприклад, на рисунку 2.7 зображено лінійний двійковий регістр зсуву який може генерувати послідовність на підставі генеруючого поліному

$$h(x) = h_5 x^5 + h_2 x^2 + 1. \tag{2.8}$$

Слід зазначити, що із застосуванням таких регістрів зсуву відбувається генерація більшості розширюючи кодових послідовностей.

Важливу роль у цифрових системах, системах з розширенням спектра і системах вимірювання відстані відіграють лінійні коди максимальної довжини або послідовності з максимальною довжиною регістр зсуву – m-послідовності.

М-послідовності генеруються окремим лінійним регістром зсуву. Зокрема, послідовність з максимальною довжиною періоду (N=2n-1) генерується n-каскадним регістром зсуву з лінійним зворотним зв'язком. Для генерації m-послідовності ступінь генеруючого поліному повинна дорівнювати n. На рисунку 2.8 наведена апаратна реалізація генератора m-послідовності.

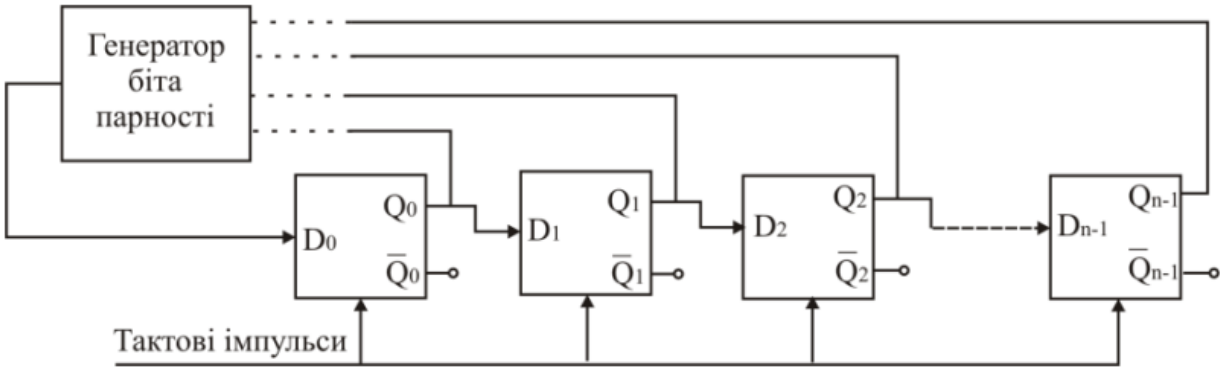

Рисунок 2.8 – Узагальнена принципова схема генератора m-послідовності

Генератор складається з лінійки послідовно включених D-тригерів, виходи Q яких з'єднані з входами наступних тригерів, за виключенням входу D_0 першого тригера. Деякі з виходів Q тригерів не з'єднані з генератором біта парності, що відзначено на рис. 2.8 пунктирною лінією.

Загальна кількість тригерів n і кількість тригерів, що підключені до генератора біта парності визначають відповідно довжину і властивості PN-коду (псевдовипадкового коду), що формується.

На виході генератора біта парності формується логічний нуль за наявності парної кількості логічних нулів на входах і логічна одиниця за наявності непарних логічних 1 на входах. Генератор біта парності представляє собою суматор за модулем 2.

Важливою характеристикою для ПВП є її довжина. Для лінійних кодів максимальної довжини завжди можна знайти такий порядок підключення виходів тригерів до генератора біта парності для якого формується послідовність максимальної довжини з періодом символів

$$L = 2^n - 1, \tag{2.9}$$

де n – кількість тригерів.

Кількість різних можливих m-послідовностей. Визначається кількістю розрядів і місцем підключення зворотного зв'язку.

Способи генерації m-послідовностей добре досліджені та наведені в спеціальній літературі, наприклад в [5, 9]. В рамках даної роботи ми лише розглянемо деякі їх властивості, що роблять їх особливо важливими для систем передачі з прямим розширенням спектра [4].

1) Властивість балансу. Так, в одному періоді m-послідовності міститься $(2^{n-1} - 1)$ нулів і 2^{n-1} одиниць.

2) Властивість зсуву під час додавання. Сума за модулем 2 m-послідовності та її довільного циклічного зсуву представляє собою інший циклічний зсув початкової m-послідовності.

3) Властивість періодичності автокореляційної функції. Якщо у початковій m-послідовності , яка складається з символів 0 та 1 провести заміну символів 0 на +1 і 1 на -1 і отримати послідовність з ансамблю -1 та 1, то періодична автокореляційна функція визначиться виразом

$$R_{xx}(t) = \begin{cases} 2^n - 1 & r = 0 \\ -1 & r \neq 0. \end{cases} \qquad (2.10)$$

Така послідовність є найкращою у тому сенсі, що не існує будь-якої іншої послідовності з мінімальним значенням автокореляціної функції для $r \neq 0$. Ця властивість має важливе значення під час їх використання як синхропреамбул для забезпечення символьної і циклової синхронізації.

4) Властивість випадковості. Оскільки m-послідовність є періодичною послідовністю, то вона не може вважатися повністю випадковою. Але для неї все ж таки можуть бути визначені статистичні властивості серій одиниць і нулів. Дійсно, у кожному періоді половина серій має довжину 1, чверть серій – довжину 2, восьма частина – довжину 3 і т. ін.

Два або більше незалежних сигнали можуть бути передані в одній і тій же смузі частот і потім успішно виділені, якщо їх кодові послідовності представляють собою циклічні зсуви m-послідовностей більше ніж на один символ.

М-послідовності мають гарні автокореляційні характеристики. Але, на практиці у телекомунікаційних системах з розширенням спектра m-послідовності застосовуються дуже мало. Це пояснюється тим фактом, що кількість m-послідовностей з однією й тою ж довжиною і однаковими кореляційними властивостями обмежена.

Для систем передачі з DSSS, де необхідно реалізувати взаємодію багатьох користувачів необхідно мати послідовності які реалізують велику кількість різних кодів з однаковими кореляційними властивостями. Для цих систем необхідно використовувати значно більшу кількість послідовностей з гарними крос-

кореляційними властивостями між ними. Метод побудови таких послідовностей було запропоновано Голдом.

Порівняно зі звичайними m-послідовностями, коди Голда є більш привабливими для використання у системах комунікацій з багатьма користувачами.

Послідовності або коди Голда утворюються шляхом застосування логічної операції XOR (виключне "АБО") з двома m-послідовностями, які обираються з умови вибору найкращої пари. Схема генерації послідовностей Голда з використанням трьохкаскадного регістру зсуву зображена на рисунку 2.9.

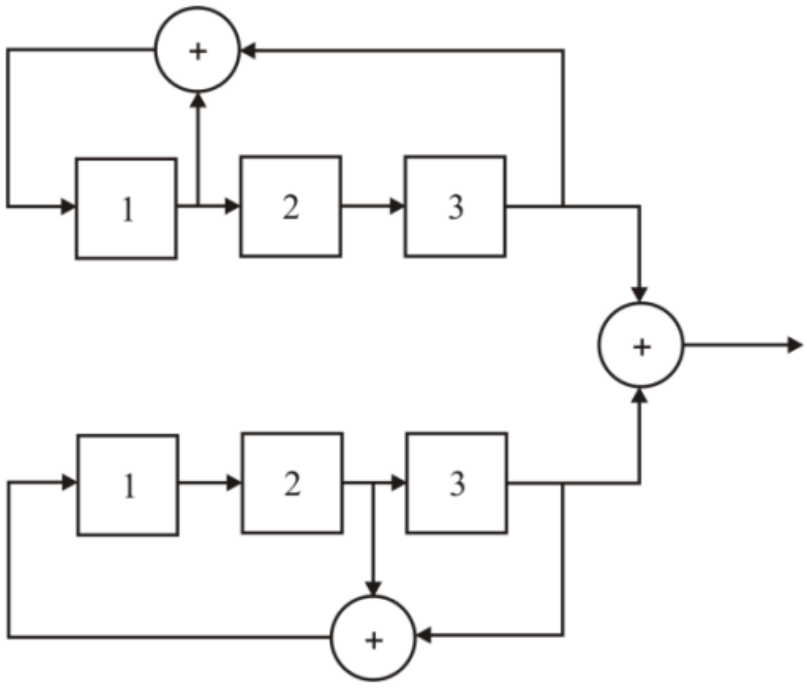

Рисунок 2.9 – Структурна схема реалізації послідовності Голда

Кількість послідовностей Голда, що генеруються за такою схемою рівняється 2^n-1. Вони отримуються шляхом зміни початкового значення регістру і додаванням двох m-послідовностей при використанні n-каскадного регістру зсуву.

Як видно з рис. 2.9, метод реалізовано на підставі додавання за модулем 2 двох різних m-послідовностей, які тактуються єдиним тактовим генератором. Найбільш суттєвий момент під час формування послідовності Голда з "гарними" кореляційними властивостями є у тому, що можуть бути застосовані тільки особливі пари m-послідовностей, які називають "кращими". Ці кращі пари m-послідовностей перелічені у таблицях, що наведені, наприклад, у [5].

Оскільки, обидві m-послідовності мають одну й ту ж довжину L і тактуються одним генератором, то послідовність Голда, що формується, також має довжину L, але не є послідовністю максимальної довжини.

Якщо n – кількість розрядів регістра зсуву у генераторі m-послідовностей , то довжина послідовності Голда $L=2^n-1$.

Підрахуємо чисельність різних послідовностей Голда, що формуються за допомогою двох генераторів m-послідовностей при різних початкових умовах. Необхідно відзначити, що за будь-якого нового циклічного зсуву початкових умов генераторів m-послідовностей формується нова послідовність Голда. Оскільки кожна m-послідовність має довжину L, то кількість різних зсувів між ними також рівняється L. Тому генератор послідовностей Голда на базі двох різних m-послідовностей може формувати $L=2^n-1$ послідовностей Голда.

Проведений аналіз питань розширення спектру кодами ПВП дозволяє зробити висновок, що одними з найголовніших властивостей ПВП є кореляційні властивості послідовностей, які в свою чергу залежать від типу кодової послідовності, частоти проходження її символів та довжини коду.

В даному випадку розділяють автокореляційні та взаємно кореляційні властивості кодів.

Автокореляція визначається як ступінь відповідності між кодом і зсунутим на деяке число позицій у часі його варіантом. Функція автокореляції показує залежність кількості збігів A та розбіжностей D символів двох кодових послідовностей по всій їх довжині від величини їх відносного зсуву.

В загальному вигляді автокореляція визначається інтегралом

$$\Psi(\tau) = \int_{-\infty}^{\infty} f(t)f(t-\tau)dt\,. \qquad (2.10)$$

Автокореляційна функція характеризує залежність автокореляції від зсуву сигналу у часі τ.

Функція автокореляції представляє найбільший інтерес при виборі кодових послідовностей для отримання найменшої вірогідності встановлення хибної синхронізації. Задача розпізнавання піків функції автокореляції при створенні системи зв’язку з великою розподільчою здатністю при погано підібраної кодової послідовності не має сенсу. Тому треба завчасно ретельно дослідити кодові

послідовності, навіть якщо відомо що вони належать до відносно гарних послідовностей.

Не менш важливе значення має взаємна кореляція двох кодів. Вона є мірою відповідності один одному двох різних кодових послідовностей і виражається в вигляді функції від величини відносного часового зсуву. Нажаль функції взаємної кореляції не притаманні такі гарні властивості, як функції автокореляції. Тому у випадку, коли велика кількість передавачів, що використовують різні коди, має працювати в одному частотному діапазоні, такі послідовності треба обирати так, щоб уникати взаємних перешкод між користувачами. Висока ступінь кореляції між опорною кодовою послідовністю приймача та кодовою послідовністю перешкоджаючої станції призводить до збільшення вірогідності хибного виявлення в приймачі і в деяких обставинах навіть до встановлення хибної синхронізації приймача.

Єдина різниця між автокореляційною та взаємно кореляційною функціями полягає у тому, що в загальний інтеграл згортки двох функцій підставляється відмінна від раніше розглянутої функція $g(t-\tau)$.

$$\Psi(\tau) = \int_{-\infty}^{\infty} f(t)g(t-\tau)dt\,. \qquad (2.11)$$

Функція взаємної кореляції представляє інтерес при використанні кодових послідовностей в таких системах, як системи з вільним доступом і кодовим розділенням каналів (або ж інша кодово-адресна система), в яких приймач реагує тільки на сигнал який містить відповідну адресу.

Найбільш небезпечною є ситуація при виборі кодових послідовностей з «поганими» взаємно корелюючими властивостями має місце в тому випадку, коли перешкоджаюча станція передає кодову послідовність що належить множині використовуваних кодових послідовностей. Це, в свою чергу, може привести до хибної синхронізації, оскільки на кожний приймач, розташований в зоні дії перешкоджаючої станції, буде впливати сигнал, частково корельований з його опорною кодовою послідовністю.

Також, в якості критерія, що характеризує кореляційні властивості кодової послідовності, двох кодових послідовностей, а також послідовності та будь-якого іншого сигналу і визначає спроможність приймача розпізнати відповідний момент

синхронізації кодової послідовності, використовують показник розрізнення (ПР) [8]. Цей показник визначається як різниця значень функцій авто- та взаємної кореляцій кодових послідовностей що відповідають основному і максимальному боковому пікам. Таким чином, конкретна кодова послідовність має різні значення ПР для функцій автокореляції та взаємної кореляції з некодованими сигналами. Очевидно, чим більше ПР, тим краща кодова послідовність.

Як було зазначено вище, дуже важливим параметром з точки зору безпеки передачі інформації є довжина коду розширення який використовується в системі комунікацій з прямим розширенням спектру. Довжина PN-коду напряму впливає на вірогідність перехоплення інформації та на рівень стійкості системи до глушіння [5].

Кодові послідовності умовно поділяють на послідовності з довгим періодом (або довгі) та на послідовності короткого періоду (короткі). Для довгих довжина L є кінцевою величиною і L>>N, де N – максимальна довжина періоду. Для коротких L<=N. Тобто, короткий код повторюється через кожен або кілька бітів даних, тоді як довгий код повторюється через набагато більшу величину бітів даних.

Оскільки послідовність короткого коду повторюється в кожному біті даних, а символом є або 1, або 0 для BPSK, або 00, 01, 10 або 11 для QPSK, відновити кодову послідовність можна відносно легко з використанням методу спроб та помилок. Однак, дана задача може бути ускладнена збільшенням довжини PN-коду. Чим довша послідовність, тим більше в ній зашифрованих кодових комбінацій, розгадка котрих буде займати все більше і більше часу та обчислюваних ресурсів. Наприклад, кодове слово довжиною 8 біт складається з 256 комбінацій, в той час, як кодове слово довжиною 20 біт вже складається з 1048575 комбінацій. Нарешті, довжина 256 біт дозволяє використовувати $1{,}1579 \cdot 10^{77}$ комбінацій.

Слід також зазначити, що збільшення довжини коду дає ще одну перевагу. Як відомо, повна енергія DSSS сигналу розподілена між усіма частотами сигналу. Нажаль, розподіл не є рівномірним через те, що не всі гармоніки несучої послідовності імпульсів мають однакову амплітуду. Фур’є аналіз показує, що чим довший код, тим більше гармонік потрібно для його формування. В цьому випадку повна енергія сигналу розподіляється по частотам більш рівномірно та має менший рівень потужності. Рівень сигналів стає співмірним з перешкодами,

які є завжди в ефірі. Такий сигнал важко виявити та перехопити, що є ваговою перевагою.

Таким чином, послідовності з довгими періодами є менш вразливими до різних типів протидії та є більш привабливими до використання, наприклад, в військові сфері. В випадках, коли вірогідність відновлення коду не викликає занепокоєння, можна використовувати короткі коди з перевагою у вартості комунікаційної системи. Наприклад, коди розширення для систем 3G+ персональних комунікаційних систем опубліковані у відкритій літературі, і це взагалі не є проблемою для їх комерційного застосування.

2.4 Встановлення та підтримання синхронізації

Однією з особливостей використання ШШС є необхідність початкової синхронізації приймального і передавального пристроїв за часом затримки та по частоті, особливо при великих значеннях невизначеності за цими параметрами. Без успішного завершення режиму пошуку ШШС, входження до синхронізму та його підтримання неможливе функціонування комунікаційної системи за цільовим призначенням.

Під повною синхронізацією маємо на увазі, що кодований сигнал, який надходить на вхід приймача, точно синхронізований як по початку кодової послідовності, так і по частоті проходження її двійкових символів (по відношенню до опорної кодової послідовності приймача). Кодова синхронізація необхідна в усіх широкосмугових системах через те, що кодова послідовність є свого роду ключем за допомогою якого здійснюється згортання спектру широкосмугових сигналів і виділення корисної інформації, а також розширення спектру будь-якого впливу що заважає.

Встановлення синхронізації є однією з найбільш важких задач при реалізації систем зв’язку з прямим розширенням спектру. Після встановлення синхронізації подальше її підтримання доволі часто забезпечується за рахунок вже отриманих часових співвідношень. Як правило, на початку роботи системи відсутні попередні часові прив’язки або, в кращому випадку, маємо дуже слабку часову прив’язку циклів роботи передатчика та приймача, наявність якої дозволяє миттєво встановити синхронізацію.

Для встановлення синхронізації застосовуються багато різних методів, деякі з них є доволі простими, а інші – більш складні з точки зору практичної реалізації.

Деякі з цих методів описані в роботах [5, 8, 10]. Відповідь на питання, який з цих методів є найкращим, залежить від призначення системи, часу, що відводиться для встановлення синхронізації, а також розмірів області невизначеності параметрів сигналів що приймаються.

Багато методів так званого грубого отримання сигналу (або синхронізації) базуються на блок-схемі, показаній на рисунку 2.10 [5]. Отриманий сигнал множиться на локально згенеровану псевдовипадкову послідовність з деяким фазовим зсувом, яке оцінюється. Якщо зсув відповідає такому ж зсуву в прийнятому сигналі, то сигнал на виході змішувача буде вузькосмуговим сигналом даних, що був згенерований в передавачі. Значна кількість енергії буде з'являтися зі смугового фільтра і згодом буде виявлена детектором енергії. Коли енергія перевищить відповідно вибраний поріг і буде досягнута груба синхронізація. Після цього приймач перейде в режим точної синхронізації/відстеження.

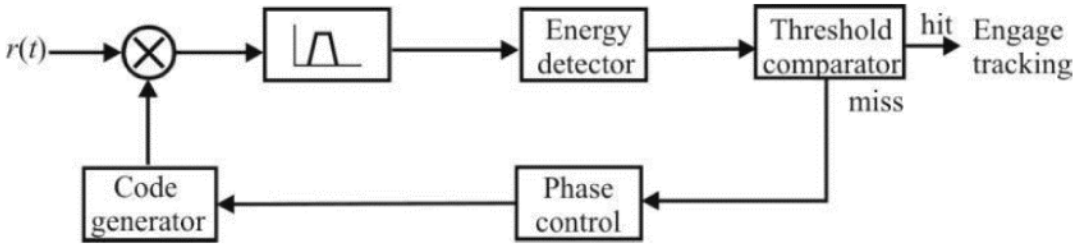

Рисунок 2.10 – Діаграма грубого отримання

Якщо локально згенерований зсув фази не збігається зі зсувом прийнятого сигналу, на виході змішувача все одно буде широкосмуговий сигнал, і через смуговий фільтр буде проходити невелика кількість енергії. Тоді виявлена енергія буде низькою і не перевищуватиме порогове значення. У цьому випадку фаза буде регулюватися вперед або назад за допомогою певного механізму. Зазвичай це досягається пропуском одного періоду мікросхеми тактового генератора. Цей процес триватиме, доки не буде знайдено правильний зсув фази.

Існує кілька форм детекторів енергії, які можуть бути використані, два з них – узгоджені фільтри та радіометри.

Незалежно від типу коду, який використовується, кодовий простір потрібно дослідити для визначення зсуву фази. Для цього є кілька способів. Найпростішим є послідовний підхід, коли за одну спробу виконується зміщення фази та

порівняння з порогом. Однак якщо довжина послідовності, N, досить велика, цей підхід може бути дуже повільним, якщо межі простору пошуку невідомі.

З іншого боку, можлива повністю паралельна реалізація, яка була б найшвидшим шляхом. У цій архітектурі N паралельно узгоджених фільтрів одночасно здійснюватимуть пошук у просторі коду, одне зміщення для кожного узгодженого фільтра. Фільтр із найбільшим виходом відповідатиме правильному зсуву фази. Однак якщо N велике, впровадження буде непомірним.

Між цими двома підходами, повністю послідовними та повністю паралельними, існують компроміси, які можуть бути реалізовані. Наприклад, замість повністю паралельної реалізації можна було б включити меншу кількість паралельно узгоджених фільтрів, і вони б розподілялися за часом.

Показником переваг будь-якого підходу до отримання сигналу DSSS є середній час, потрібний для досягнення синхронізації. Цей час є випадковою змінною через випадковість, що лежить в основі псевдовипадкових кодів. Передача може відбутися в будь-який час. Синхронізація, однак, є функцією приймача. Одержувач повинен знайти код у послідовності PN, щоб синхронізуватися з ним. Через цей випадковий характер часу отримання даних, його можна описати лише статистично за допомогою моментів і функцій розподілу.

Найменш бажаною ситуацією є встановлення хибної синхронізації. Коли це відбувається, приймач вважає, що він синхронізований, хоча це не так, тому він неправильно декодує вхідний сигнал, генеруючи не вірні дані або взагалі не генеруючи їх, доки не буде зроблена повторна спроба синхронізації.

Послідовний пошук є найпоширенішою формою методу пошуку DSSS. Середній час синхронізації для послідовного пошуку можна визначити за допомогою наступного виразу:

$$\varepsilon\{T_s\} = (C-1) \bullet T_{da}\left(\frac{2-P_d}{2P_d}\right) + \frac{T_i}{P_d}, \qquad (2.12)$$

де $T_{da} = T_i + T_{fa}P_{fa}$;

T_i – час оцінки для кожної комбінація фазових зсувів і частоти;

T_{fa} – час, необхідний для відхилення невірної комбінації;

P_d – вірогідність виявлення;

P_{fa} – вірогідність хибного виявлення;

$C = \Delta T / \Delta t$ (ціле число);

Δt – розмір кроку по фазі;

ΔT – час, протягом якого з'являється правильна фаза.

Необхідно відзначити, що самі по собі режими пошуку сигналу та синхронізації є найуразливішими режимами роботи радіоелектронної системи [6]. Під час синхронізації існує ризик встановлення хибної синхронізація, яка, в свою чергу, може виникати через завантажений радіоефір, а може бути результатом нав'язування імітаційних перешкод зловмисником. Саме тому середній час досягнення синхронізації може вважатися одним із критерієм якості системи зв'язку з прямим розширенням спектру.

З іншого боку тривалість роботи системи у режимах пошуку сигналу та синхронізації залежить від умов сигнально-перешкодової обстановки [5, 6]. Як показано в роботі [8], зменшення відношення S/N (сигнал/шум) збільшує вірогідність хибного виявлення сигналу.

Аналіз даних, наведених в роботі [10], дозволяє зробити висновки, що система синхронізації в режимі перевірки стану блокувань є вразливою до глибоких завмирань і імпульсних перешкод.

Після встановлення синхронізації необхідно подбати про її подальшу підтримку. При синхронізації опорного широкосмугового сигналу з сигналом що приймається необхідно підтримувати режим синхронізації на протязі всього часу роботи приймача. При цьому опорна кодова послідовність має точно відслідковувати кодову послідовність сигналу, що приймається. Для підтримки узгодження тактових частот прийнятої та опорної послідовності використовують активні методи стеження за частотою, деякі з цих методів наведені в роботах [5, 8].

5. Аналіз принципів побудови приймального тракту системи з DSSS.

На етапі проектування приймачів та передатчиків широкосмугових сигналів доводиться вирішувати широкий спектр специфічних задач, таких як:

- вибір реальної ширини смуги частот;
- аналіз впливу коефіцієнта шуму приймача;
- визначення вимог до динамічного діапазону та глибині регулювання автоматичного регулювання підсилення (АРП);

– врахування властивостей середовища розповсюдження сигналів та інші задачі.

Від рішень прийнятих на етапі проектування приймача напряму залежать робочі характеристики комунікаційної системи і насамперед рівень її надійності та завадостійкості. Проаналізуємо принципи побудови приймачів приймального тракту, наведені в роботі [8].

Побудова передавача та приймача широкосмугових сигналів в основному не відрізняється від побудови передавача та приймача будь-якої іншої системи, що працює в тому ж частотному діапазоні. Однак цілком зрозуміло, що необхідно брати до уваги ряд міркувань, перш за все пов'язаних з використанням ширшої смуги та наявністю великого динамічного діапазону сигналів, що одночасно приймаються.

Розглянемо задачу вибору смуги пропускання приймача. Шум і сигнали перешкод інших користувачів цієї ж лінії зв'язку є основним видом інтерференційних або штучних перешкод, що діють на приймач широкосмугових сигналів. Вони складаються з будь-яким іншим сигналом, що приймає, і обробляються тими ж способами.

Чутливість будь-якого приймача обмежується тим рівнем атмосферного шуму, що він приймає поруч із корисним сигналом, і навіть рівнем його власного внутрішнього шуму. Ці джерела шуму, як, втім, і будь-який інший сигнал, що заважає, створюють адитивну перешкоду. Потужність шуму атмосфери на вході приймача дорівнює:

$$N_{atm} = kTB, \tag{2.13}$$

де k – постійна Больцмана, яка дорівнює $1{,}38 \cdot 10^{-23}$ Дж/К;

T – шумова температура на вході приймача, в градусах Кельвіна;

B – шумова смуга приймача.

Ширина смуги частот приймача широкосмугових сигналів має відповідати ширині смуги частот корисного сигналу. Так, якщо сигнал повідомлення з заданою смугою частот при переносі в діапазон радіочастот розподіляється в смузі, яка в багато разів перевищує власну смугу частот, то і приймач змушений приймати шум, рівень якого збільшується пропорційно коефіцієнту розширення смуги частот корисного сигналу. Тобто, якщо сигнал, що займає двосторонню смугу частот 10 кГц, розподіляється в смузі 10 МГц (що відповідає виграшу при обробці

30 дБ), це призведе до збільшення потужності шуму на вході приймача також на 30 дБ.

Однак при розумному виборі смуги частот приймача можна виключити більшу частину потужності шуму, ніж сигналу, і, таким чином, отримати деякий виграш. Зокрема, в роботі [8] показано, що зменшення смуги пропускання приймача до значення, що становить 60% ширини основного пелюстки спектра сигналу, призводить до того, що буде прийматися тільки 90% вихідної потужності корисного сигналу, тобто втрати становитимуть 0,46 дБ. При цьому, однак, потужність шуму, що приймається, знизиться до 60% його первісного значення, що еквівалентно зменшенню потужності шуму на 2.2 дБ. Таким чином, такий простий спосіб зменшення смуги пропускання приймача призводить до виграшу щодо сигнал/шум приблизно дорівнює 1,7 дБ.

Після вибору смуги пропускання приймача, проаналізуємо вплив власного шуму приймача та внутрішньосистемних перешкод. Виявляється, що обидва джерела перешкод впливають майже однаково на стійкість до перешкод приймача. Якщо коефіцієнт шуму приймача або потужність внутрішньосистемних перешкод зростуть у кілька разів, то для збереження відношення сигнал/шум необхідно збільшити потужність корисного сигналу в таку ж кількість разів.

Зазначимо, що в більшості випадків не слід розраховувати на те, що приймач максимально придушуватиме сигнали, що заважають, і одночасно буде нормально функціонувати при мінімальному рівні високочастотного сигналу. Максимальна чутливість визначається тим мінімально можливим рівнем корисного сигналу, при якому забезпечуються нормальні умови прийому при дії перешкоди у вигляді шуму атмосферного і шуму вихідних каскадів приймача. Тому можна припустити, що в приймачі широкосмугових сигналів здійснюватиметься найкраще придушення перешкоди лише у випадку, коли рівень корисного сигналу на його вході буде на 3 дБ перевищувати мінімально можливий.

При побудові високочастотної частини приймача широкосмугового сигналу в порівнянні з високочастотними блоками передавача доводиться долати доволі багато труднощів і, головним чином, через наявність сигналів, що заважають, діючих до блоків обробки сигналу. В ідеальному випадку у приймачі прийнятий (по можливості з найменшими спотвореннями) корисний сигнал посилюється, здійснюється перенесення на проміжну частоту і потім без спотворень сигнал має бути поданий на вхід корелятора. Одночасно на вхід корелятора надходитиме

будь-який перешкоджаючий сигнал, частота якого виявляється в межах смуги частот, що займається корисним сигналом.

Зазвичай у системах з псевдовипадковими фазо модульованими сигналами при проходженні корисного сигналу одночасно з інтенсивним перешкоджаючим сигналом, зменшення відношення сигнал/шум може становити 6 дБ і більше. Тому необхідною умовою є лінійність амплітудної характеристики високочастотних каскадів приймача.

Чому ж у системах з фазомодульованими псевдовипадковими сигналами за наявності обмеження втрачається можливість ефективного придушення перешкод? По-перше, системи з псевдовипадковими фазомодульованими сигналами найбільш сильно схильні до впливу гармонійної штучної перешкоди і вплив цієї перешкоди майже не змінюється при зміні її частоти в діапазоні частот, що становить 10% (або більше) ширини спектра корисного сигналу. В роботі [8] показано, що відношення сигнал/перешкода на виході обмежувача при дії гармонійної перешкоди з постійним рівнем у гіршому випадку зменшується на 6 дБ. Крім того, він показав, що якщо для придушення приймача широкосмугових сигналів з обмежувачем використовується шум, ширина спектра шуму не має істотного значення.

У випадку, якщо в приймачі фазомодульованого псевдовипадкового сигналу необхідно використовувати обмеження сигналу (насправді, завжди десь у лінії є обмежувач), зазвичай застосовують багатофазну маніпуляцію, при якій обмеження сигналу не призводить до таких значних втрат, як при двійковій фазовій маніпуляції.

Особливу увагу при побудові приймальної апаратури, в якій має бути забезпечена лінійність, необхідно приділити аналізу діапазону змін рівня сигналу, в якому забезпечується лінійність амплітудної характеристики. Приймальний тракт від вхідних каскадів до входу корелятора має бути спроектований так, щоб забезпечувалася лінійність його характеристики не тільки в очікуваному діапазоні можливих змін рівня корисного сигналу, але також і на заваді. Застосування автоматичного регулювання підсилення лише частково вирішує цю проблему в тому сенсі, що вона дозволяє регулювати рівень підсилення сигналом, перешкодою або, нарешті, суміші сигналу і перешкоди. Оскільки потужність перешкоди часто у багато разів перевищує потужність корисного сигналу, то АРП за сумарною потужністю фактично працює як АРП за потужністю перешкоди.

Зазвичай прагнуть регулювати коефіцієнт посилення приймача за вихідним сигналом корелятора, оскільки в цьому випадку можна знехтувати впливом перешкоди на процес регулювання посилення. В іншому випадку, постановник перешкоди міг би регулювати рівень сигналу і навіть здійснювати його модуляцію шляхом зміни рівня потужності перешкоди. Після встановлення керованого рівня сигналу в кожному з каскадів приймача, через які разом проходять і сигнал, і перешкода, повинна підтримуватися лінійна характеристика. З цієї причини в більшості випадків корелятор у приймачі широкосмугових сигналів бажано включати якомога ближче до його входу, так щоб перед корелятором розташовувалося якнайменше каскадів з високим рівнем вихідних сигналів. Це також призводить до зменшення необхідного рівня опорного сигналу приймача.

У випадку, коли приймач повинен працювати в широкому діапазоні робочих частот, часто виникає необхідність використовувати вхідні широкосмугові каскади, які повністю перекривають всю смугу частот або, принаймні, максимально можливу частину необхідної смуги. У цьому випадку перебудова приймача здійснюється за допомогою гетеродина, що перебудовується, сигнал якого змішується в змішувачі з прийнятим сигналом, і в результаті на виході утворюється складова сигналу фіксованої проміжної частоти. У сучасній радіоапаратурі замість гетеродин все частіше застосовують цифровий синтезатор частоти. Такий підхід у деяких випадках є розумним і навіть бажаним. Однак у широкосмугових системах з підвищеною завадостійкістю він використовується мало. Припустимо, наприклад, що джерело перешкоди може випромінювати тільки два сигнали, зміщених частотою на величину, рівну проміжній частоті приймача. У цьому випадку не має значення, яка робоча частота приймача, оскільки сигнал на виході першого змішувача або корелятора міститиме складову проміжної частоти. Це, в свою чергу, може призвести до істотного зниження завадостійкості. Аналогічним чином за наявності широкосмугових вхідних каскадів приймача можливий прийом різними побічними каналами, наприклад дзеркальному, що також збільшує рівень перешкод.

Таким чином, у приймачах, спеціально призначених для систем з підвищеною завадостійкістю, видається вкрай небажаним потрапляння безпосередньо на вхід корелятора будь-якої перешкоди, яка відрізняється від тієї, на яку розрахована система. Тому зазвичай не рекомендується використовувати широкосмугове посилення (принаймні більше того, яке необхідне для корисного сигналу).

2.6 Способи блокування прийому сигналів.

Наведений вище аналіз принципів формування, приймання та обробки сигналів в системах передачі інформації з прямим розширення спектру дозволяє навести основні способи блокування прийому сигналів в приймачі. До них можна віднести наступні способи:

– загороджувальна шумова завада (blanket jamming);
– імітаційна перешкода;
– потужна монохромна завада частини спектру де присутня несуча сигналу.

Загороджувальна завада є формою електронної перешкоди. Цей метод часто використовується в електронній боротьбі, коли необхідно створити інтенсивні перешкоди для блокування або порушення нормальної роботи комунікаційних систем. Ця перешкода може застосовуватися для впливу на весь діапазон частот, включаючи різні стандарти бездротового зв'язку, радіолокацію та інші системи. Наявність загороджувальної завади може суттєво погіршити або навіть повністю блокувати передачу та прийом радіосигналів.

Імітаційна перешкода це метод в електронній боротьбі, який полягає у створенні та передачі підроблених (імітаційних) розширених спектрів з метою порушення або приведення в оману системи, що використовують DSSS-модуляцію. Вплив помилкових чіп-послідовностей перешкоджає нормальній роботі приймача, сприяє збільшенню часу синхронізації та, в окремих випадках, може призводити до встановлення хибної синхронізації. Найбільш небезпечними є ситуації, коли зловмиснику стають відомі тактова частота та довжина кодової послідовності, що використовується системою.

У випадках, коли зловмисник не має достатньої інформації про сигнали комунікаційної системи, зазвичай вдаються до використання «грубої сили», а саме до блокування приймача потужною монохромною завадою сконцентрованою в вузькому діапазоні частот, де присутня несуча.

Більш детально методи протидії системам з DSSS, а також методи їх захисту будуть проаналізовані в наступних розділах.

3 ДОСЛІДЖЕННЯ МЕТОДІВ ПРОТИДІЇ СИСТЕМАМ ПЕРЕДАЧІ З ПРЯМИМ РОЗШИРЕННЯМ СПЕКТРА

В даному розділі наведено дослідження найбільш поширених технологій протидії системам передачі з прямим розширенням спектра. Більшість з наведених технологій діють шляхом навмисної передачі інтерференційних сигналів в безпроводовому каналі. Зазначені сигнали можуть ускладнювати та навіть блокувати роботу призначених приймачів, вводити їх в оману шляхом передачі подібного, хибного сигналу або роблять неможливим вилучення значущих даних. Далі проаналізовано вплив засобів протидії на роботу комунікаційних систем з прямим розширенням спектру та їх ефективність при різних умовах. І, на завершення, запропоновані рекомендації для захисту систем з DSSS від кожного типу протидії.

3.1 Методи протидії системам з DSSS

Для зручності дослідження методів протидії системам зв’язку з прямим розширенням спектру, автор роботи пропонує класифікувати ці методи з точки зору спрямованості їх потенційних загроз, а саме спрямованості на втрати конфіденційності, цілісності та доступності даних.

Під методами протидії системам з DSSS спрямованими на загрозу втрати конфіденційності будемо розуміти методи, що ставлять за мету отримання несанкціонованого доступу до інформації, яка передається від однієї системи до іншої. Загроза порушення конфіденційності полягає в тому, що інформація яка передається стає відомою особі або групі осіб, які не володіють повноваженнями доступу до неї. Цілком логічно, що порушення конфіденційності для будь-якої комунікаційної системи є перехоплення інформації, що передається. Ефективність перехоплення інформації в системах з DSSS буде розглянута нижче але, забігаючи наперед, можна відзначити, що цей спосіб протидії не є надто актуальним для сучасних систем з прямим розширенням спектру.

Наступна група методів протидії комунікаційним системам з прямим розширенням спектру – це методи спрямовані на використання імітаційних перешкод, а саме на створення та передачу імітаційних розширених спектрів (імітаційних сигналів) з метою приведення в оману систем, що використовують

DSSS-модуляцію. Система зв’язку сприймає підроблений сигнал за справжній, що перешкоджає нормальній роботі приймача та може призводити до збільшенню часу синхронізації або навіть до встановлення хибної синхронізації та отримання невірних даних. Атаки з використанням імітаційних перешкод здійснюються під час роботи приймача в найбільш уразливому режимі – режимі встановлення синхронізації. Найбільші обмеження і складність застосування цих методів полягають у тому, що потрібна ультраточність синхронізації, а також значні апріорні знання структури цільового сигналу (тактової частоти та довжини кодової послідовності). Дані методи протидії можна віднести до методів, що становлять загрозу цілісності передачі даних через те, що імітаційний сигнал може містити невірні дані, які будуть отримані після обробки імітаційного сигналу.

Третя група методів протидії є найпоширенішою та найпростішою з точки зору практичної реалізації. Зазначені методи спрямовані на постанову завад та глушіння (Jamming) шляхом навмисної передачі інтерференційних сигналів в безпроводовому каналі, які в свою чергу, ускладнюють або роблять неможливим для призначених приймачів вилучення значущих даних. Через те, що постановка завад та глушіння ускладнюють або навіть унеможливлюють передачу даних, можна сказати, що ці методи створюють загрози доступності даних.

Проаналізуємо найбільш поширенні технології протидії системам передачі з прямим розширенням спектра шляхом. Відповідно до [5, 9], системи з DSSS схильні до впливу наступних Jamming технологій:

– шумове глушіння;
– імпульсне глушіння;
– глушіння тонами.

Розглянемо поверхнево кожну з зазначених технологій, з більш детальним описом можна ознайомитися в [5] та [9].

Для глушіння шумом сигнал несучої глушіння модулюється випадковою формою хвилі шуму. Мета полягає в тому, щоб порушити форму сигналу зв’язку шляхом введення шуму в приймач. Смуга пропускання сигналу може бути такою ж широкою, як і вся ширина спектру, що використовується системою комунікацій (BBN Jamming – Broadband Noise Jamming), або набагато вужчою, займаючи лише один канал чи декілька каналів (PBN Jamming – Partial-Band Noise Jamming).

BBN Jamming, або перешкоди широкосмуговим шумом, розподіляють енергію шуму по всій ширині частотного спектру, який використовується

цільовими системами зв’язку. Його також називають повносмуговим глушінням, а іноді називають загороджувальним глушінням (це останнє найменування також стосується випадків, коли глушиться менше, ніж повна смуга).

Цей тип перешкод є ефективним проти всіх форм зв'язку з ШШС. Також перешкоди широкосмуговим шумом можуть бути корисними при покритті області з метою скринінгу. В цьому випадку, пристрій перешкод виступає у ролі електронного захисту і розміщується між електронною системою підтримки супротивника та дружнім зв’язком. Звичайно, спрямовані антени, повинні бути спрямовані в напрямку електронних систем підтримки. При правильному використанні ці дії запобігають перехопленню дружніх комунікацій противником.

BBN Jamming проілюстровано на рисунку 3.1. За замовченням передбачається, що центральна частота сигналу перешкод є такою ж, як у цільової DSSS системи.

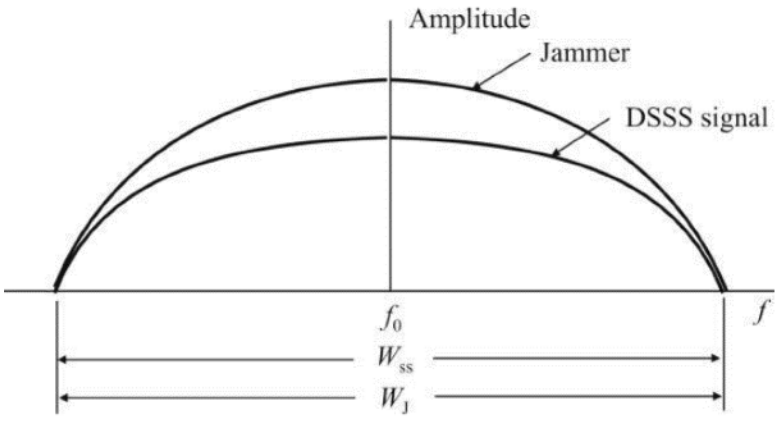

Рисунок 3.1 – Глушіння сигналу з прямим розширенням широкосмуговим шумом

На цільовому приймачі DSSS ми знаємо, що вихідне співвідношення сигнал/шум детектора (SNR_0), збільшується на виграш обробки – G. Рівень вихідного сигналу збільшується на G, а вихідний шум – ні. Процес декореляції не впливає на шум, і будь-який шум, який існує на вході, буде існувати і на виході детектора.

Таким чином, щоб використовувати BBN як техніку глушіння, необхідно подолати приріст обробки, щоб створити достатньо шуму на виході детектора та вплинути на процес виявлення. Ефективність глушіння DSSS системи також залежить від того, чи є сигнал DSSS закодованим для захисту від помилок чи ні.

PBN Jamming, або перешкоди частково-смуговим шумом, розподіляють енергію глушіння шуму на кілька, але не на всі канали в спектрі, який використовують цільові системи зв’язку. Ці канали можуть бути суміжними або ні.

Рисунок 3.2 ілюструє спектри глушіння частково-смуговим шумом сигналів DSSS. Сигнал перешкод може бути зосереджений на центральній частоті сигналу, як показано на рис. 3.2 а, або він може бути зміщений, як показано на рис. 3.2 б.

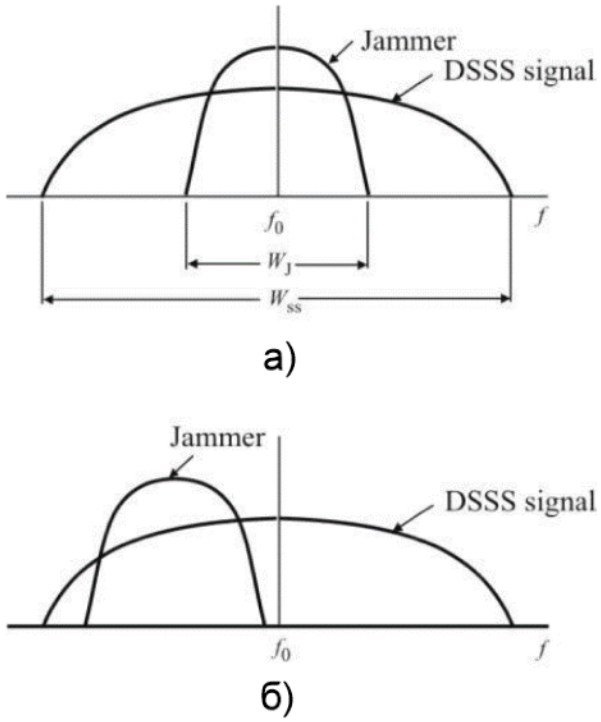

Рисунок 3.2 – Глушіння сигналу частково-смуговим шумом
а) сигнал перешкод по центру, б) сигнал перешкод зміщений

Імпульсне глушіння подібне за концепцією до частково-смугового шумового глушіння. Частка γ, у цьому випадку відповідає частині часу, протягом якого глушник увімкнений відносно вимкненого, тоді як для глушіння PBN частка відповідає частині спектра, охопленої одночасно. Однак статистика виявляється однаковою. Короткі імпульси мають широкий спектральний вміст і тому схожі на широкосмуговий шум, коли вони включені.

Імпульсне глушіння може мати нижчу середню потужність, ніж деякі з інших методів глушіння, розглянутих тут, і мати таку саму або більшу ефективність. Робочий цикл визначає співвідношення між середньою та піковою

потужностями. Ефекти перешкод залежать від пікової потужності та частоти повернення сигналу до приймача.

Для глушіння тонами використовується одна з найпростіших форм сигналу з точки зору створення та використання. На відміну від глушіння BBN і PBN, яке обговорювалося раніше, глушіння тонами мінімізує вплив на дружні пристрої, тому використання цієї технології в деяких випадках буде більш раціональним.

Загальний сигнал перешкод на приймачі при глушінні тонами визначається як:

$$j(t)=\sum_{n=1}^{N_j}\sqrt{2J_n}\cos\left(\omega_n t+\phi_n\right), \qquad (3.1)$$

де J_n – середня потужність n-го тону;

ω_n – частота n-го тону;

ϕ_n – його фазовий зсув відносно цільового сигналу, який рівномірно розподілений на $(0, 2\pi]$;

N_j – кількість тонів ($N_j \geq 1$).

При заглушенні за допомогою тонів можуть використовуватися один або декілька тонів. Спектр, коли використовується один тон, проілюстровано на рисунку 3.3, тоді як спектр у випадку глушіння мульти-тонами проілюстровано на рисунку 3.4. Тони перешкод можна розташовувати довільно, але деякі варіанти розташування дають кращі результати, ніж інші. Наприклад, при глушінні одним тоном, потужний CW (Continuous Wave) тон розміщується у певному місці в частотному спектрі. Цей стійкий сигнал не несе ніякої інформації в своїй амплітуді чи частоті. Це місце, як правило, залежить від поточної цілі, і мета полягає в тому, щоб оптимізувати це розміщення на користь глушника.

У випадку використання кількох CW тонів, потужність перешкод розподіляється на певну кількість каналів, і через це потужність на кожний окремий канал зменшується.

Найкраща ефективність перешкод досягається шляхом розміщення кількох тонів у цілих числах, кратних швидкості передачі даних. Тонове глушіння, незалежно від того, використовується один або кілька тонів, відносно неефективне

навіть для помірних значень SNR, коли тон розташований поза межами несучої частоти системи з DSSS.

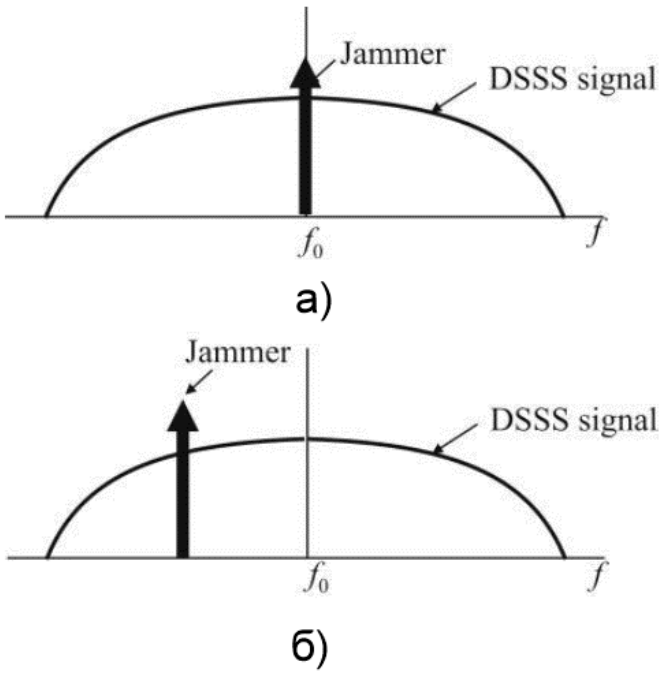

Рисунок 3.3 – Глушіння широкосмугового сигналу одним тоном
а) тон по центру спектра, б) тон перешкоди зміщений

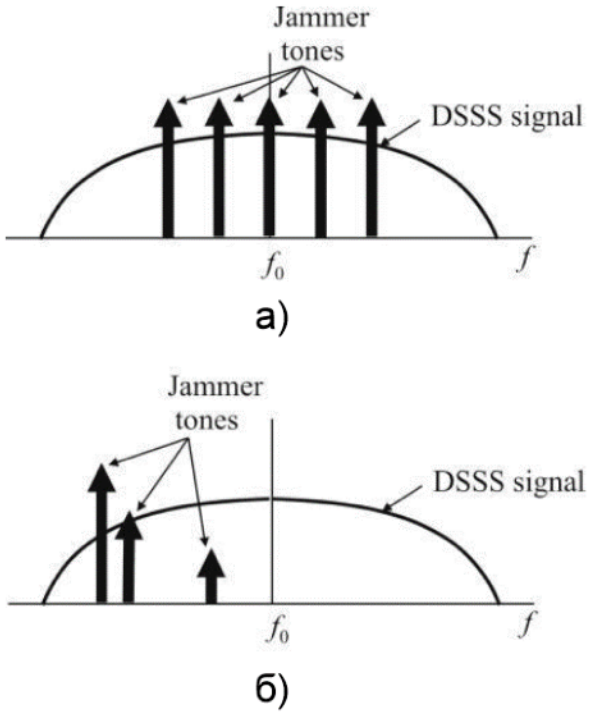

Рисунок 3.4 – Глушіння широкосмугового сигналу мульти-тонами
а) тони рівної амплітуди, рівномірно розподілені і відцентровані у спектрі, б) тони різної амплітуди з нерівномірним розподіленням по спектру сигналу

2. Ефективність методів протидії системам з DSSS при різних умовах

Ефективність методів протидії, що спрямовані на перехоплення інформації, є доволі низькою для сучасних систем з DSSS через декілька факторів:

– важкість детектування розширених сигналів (широкосмугові сигнали характеризуються дуже малою нормованою за частотою щільністю потужності (ват/герц), часто ці сигнали знаходяться нижче рівня шуму);

– кодування забезпечує захист інформації, що передається від підслуховування («чужий» DSSS-приймач використовує іншу кодову послідовність і не зможе декодувати інформацію не від свого передавача).

Звісно, зашифровану кодову послідовність можна визначити з використанням методу спроб та помилок. Однак, дана задача суттєво ускладняється збільшенням довжини PN-коду. Чим довша послідовність, тим більше в ній зашифрованих кодових комбінацій, розгадка котрих буде займати все більше і більше часу та обчислюваних ресурсів.

На протязі останнього десятиріччя можливості імітонападіння значно розширилися. Процес впливу значно змінився на канальному, сервісному та апаратному рівнях. Як показали проведені дослідження, методи засновані на використанні імітаційних завад за певних умов можуть станови істотні загрози для комунікаційних систем з прямим розширенням спектру.

Виділяють два типи імітаційних завад для впливу на автоматизований радіоканал [6]:

– перший тип – імітозавади, діючі на радіоканалі чергового прийому;

– другий тип – імітаційні перешкоди, діючі в момент передачі повідомлення (під час сеансу зв’язку).

Можливість застосування імітаційної завади того чи іншого типу визначається часом, затраченим на виявлення сигналу, тривалістю передачі сигналу та інерційністю систем радіоспостереження (РС) та радіоелектронного впливу (РЕВ).

У зв'язку з цим виділяють поняття «імітаційна стійкість системи зв'язку». Система є стійкою до дії імітаційної перешкоди, якщо завдання підбору імітаційної завади вимагає більше часу, ніж тривалість передачі сигналу в каналі зв'язку.

В роботі [6] наведені результати оцінки стійкості широкосмугових сигналів до імітаційних перешкод. Для проведення розрахункових досліджень

використовувалися математичні моделі, наведені в [5, 6]. Методика оцінки стійкості базується на визначенні часу безпечної роботи комунікаційної системи:

$$t_s = \frac{1}{2} Z \bullet t_{im}, \tag{3.2}$$

де t_s – математичне очікування часу статистичного випробування всіляких варіантів нав'язування супротивником сигналу з використанням всього простору {Z} складних сигналів;

t_{im} – час передачі імітаційного сигналу, що є величиною зворотньо пропорційною швидкості імітаційного впливу.

Результати розрахункових досліджень наведені в таблиці 3.1.

Таблиця 3.1 – Стійкість різних сигналів до імітаційних перешкод

Алгоритм формування	Безпечний час роботи для довжини ПВП, с, біт						Вірогідність нав’язування
	32	64	128	256	512	1024	
Вузькосмуговий фазомодульований сигнал	-	-	-	-	-	-	1
Широкосмуговий фазомодульований сигнал	3,1E-4	6,3E-4	1,3E-3	2,5E-3	5E-3	0,01	0,16
Широкосмуговий вейвлет-модульований сигнал	4,69	9,53	19,2	38,6	77,3	155	1,1E-5

Проаналізувавши дані, наведені в таблиці 3.1, можна зробити висновок про те, що найбільшою імітаційною стійкістю, і відповідно, найкращою здатністю протистояти імітаційним перешкодам має вейвлет-модульований широкосмуговий сигнал з фіксованим значеннями параметрів модулюючої функції. Наприклад, застосування даного алгоритму формування сигналу дозволяє збільшити безпечний час передачі інформаційної послідовності на 4,69 с для довжини ПВП 32 біта. Тоді як широкосмуговий фазомодульований сигнал збільшує безпечний час передачі лише на 3,1E-4 с для аналогічної довжини ПВП. А використання

вузькосмугового фазомодульованого сигналу ніяк не впливає на зміну безпечного часу передачі, оскільки можливість його нав'язування дорівнює 100 %.

Далі розглянемо ефективність впливу різноманітних методів глушіння на роботу комунікаційних систем з прямим розширенням спектру. Зазначені методи протидії спрямовані на ускладнення або унеможливлення передачі даних. Для кількісного оцінювання ефективності глушіння, будемо використовувати коефіцієнт BER. Так, якщо значення коефіцієнту BER досягає або перевищує рівень 10^{-1} (в середньому один біт помилки з 10), то можна зробити висновок щодо успішного глушіння комунікацій.

BBN Jamming, або перешкоди широкосмуговим шумом, є доволі ефективним методом протидії всім формам зв'язку з ШШС. Частота бітових помилок для BPSK і QPSK модуляцій в адитивному білому гаусівському шумі буде однакова. Потужність на символ для QPSK модуляції буде вдвічі менша, ніж для BPSK, тоді як тривалість символу вдвічі більша, що гарантує однакову енергію на біт для обох підходів. Для прямокутної форми імпульсу та повносмугового глушіння системи з DSSS незалежно від модуляції (BPSK або QPSK) коефіцієнт BER визначається як:

$$P_e=Q\left(\sqrt{\frac{2G_p}{\frac{1}{u}+\varepsilon}}\right), \tag{3.3}$$

де G_p – виграш обробки;

u – відношення сигнал/шум (SNR);

ε – відношення завада/сигнал (JSR);

Q – функція Гауса, задана у вигляді додаткової функції похибок.

$$Q(x)=\frac{1}{2}\operatorname{erfc}\left(\frac{x}{\sqrt{2}}\right). \tag{3.4}$$

На рисунку 3.5 наведено графікі залежностей BER від JSR для значень SNR -10, -15 та -20 дБ та фіксованого значення G_p=100 (20 дБ) [5]. З рисунка видно, що широкосмугова завада залишається відносно неефективною, доки її величина

(JSR) не подолає виграш обробки (N = 100, 20 дБ). Однак, цей момент, коли $P_e \approx 10^{-1}$ або вище, досягається майже одночасно для всіх наведених кривих, незалежно від рівня SNR.

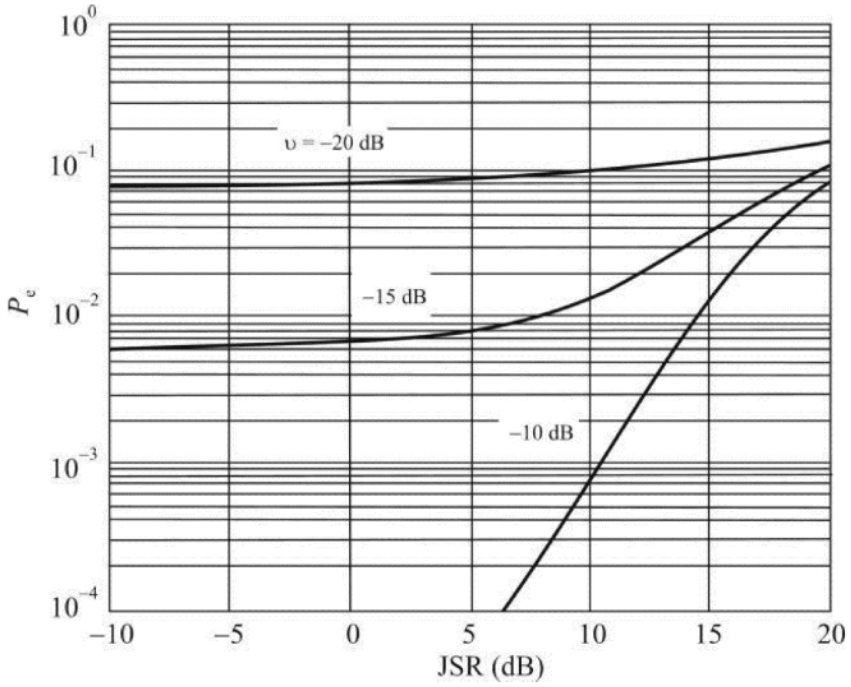

Рисунок 3.5 – Ефективність широкосмугового глушіння некодованих систем з DSSS з BPSK або QPSK модуляцією, G_p=100

Ефективність широкосмугового глушіння, коли виграш обробки змінюється від 10 до 1000, показана на рисунку 3.6 для SNR=-20 дБ. Збільшення JSR на 10 дБ покращує ефективність глушіння, виміряну подоланим коефіцієнтом посилення обробки, приблизно на 3 дБ при $P_e=10^{-1}$.

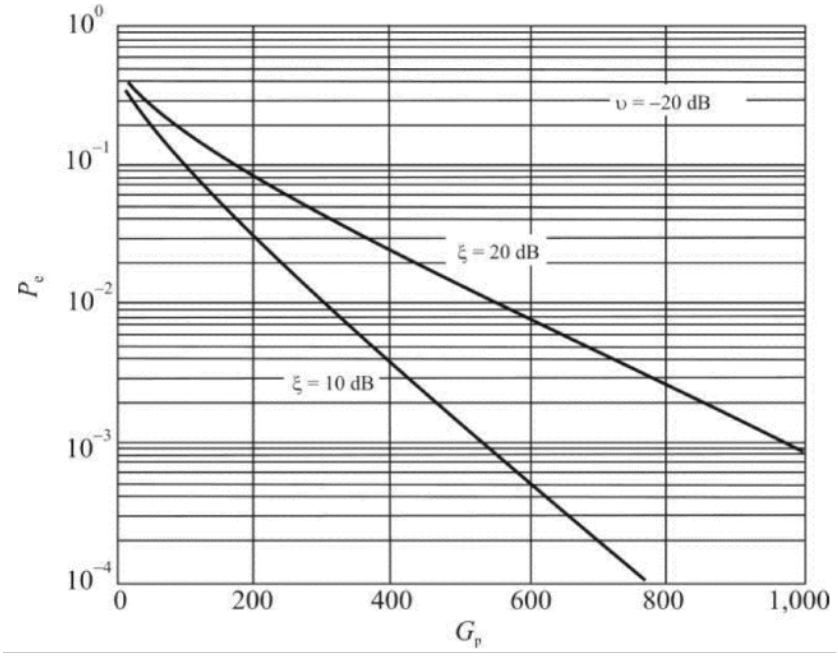

Рисунок 3.6 – Ефективність широкосмугового глушіння некодованих систем з DSSS з QPSK модуляцією, для різних рівнів JSR та SNR -20 дБ

Таким чином, щоб використовувати BBN як техніку глушіння, необхідно подолати приріст обробки, щоб створити достатньо шуму на виході детектора та вплинути на процес виявлення. Ефективність глушіння DSSS системи також залежить від того, чи є сигнал DSSS закодованим для захисту від помилок чи ні.

PBN Jamming, або перешкоди частково-смуговим шумом, розподіляють енергію глушіння шуму на кілька, але не на всі канали в спектрі, який використовують цільові системи зв’язку. У випадку протидії частково-смуговим шумом, функцію BER для некодованої системи з DSSS незалежно від модуляції (BPSK або QPSK) можна представити як:

$$P_e = Q\left(\sqrt{\frac{2G_p}{\frac{1}{\upsilon}+2\varepsilon}}\right). \qquad (3.5)$$

Ця функція зображена на рисунку 3.7 в залежності від коефіцієнта обробки, G_p. Графіки побудовано для випадку, коли перешкода покриває 10 % спектру широкосмугового сигналу, тобто

$$\gamma = \frac{W_J}{W_{ss}} = 0{,}1\ . \qquad (3.6)$$

З графіків зрозуміло, що якщо пристрій перешкод може подолати приріст обробки системи DSSS, у приймачі можуть виникнути значні шкідливі ефекти. Коли відношення сигнал/шум дорівнює -10 дБ для відношення завада/сигнал 10 дБ, спостерігаємо приріст кодування менше 13 дБ, тоді як якщо JSR складає 20 дБ, приріст кодування понад 20 дБ все ще є ефективним (P_e <10^{-1}).

Порівняння наведених графіків для широкосмугового та частково-смугового глушіння показує, що отримані результати не дуже чутливі до рівня SNR на розглянутих рівнях JSR. Виграш обробки DSSS при використанні сигналів BPSK або QPSK для глушіння PBN на 3 дБ менше, ніж для глушіння BBN. Таким чином, глушіння PBN є більш ефективним проти цих типів сигналу.

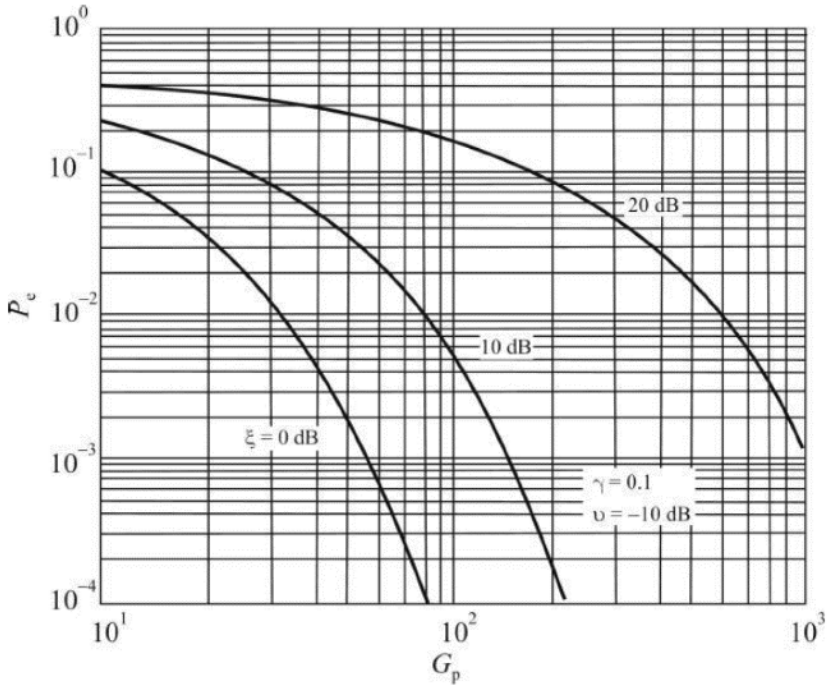

Рисунок 3.7 – Ефективність частково-смугового глушіння некодованих систем з DSSS з QPSK модуляцією, для різних рівнів JSR та SNR -10 дБ

Також, слід зазначити, що при використанні PBN глушіння, оптимальним варіантом є розміщення перешкоди в центрі DSSS сигналу.

Імпульсне глушіння подібне за концепцією до частково-смугового шумового глушіння. Частка γ, у цьому випадку відповідає частині часу, протягом якого глушник увімкнений відносно вимкненого, тоді як для глушіння PBN частка

відповідає частині спектра, охопленої одночасно. У даному випадку усереднену функцію BER для некодованої системи з DSSS незалежно від модуляції (BPSK або QPSK) можна представити в наступному вигляді:

$$P_e=(1-\gamma)Q(\sqrt{2G_p u})+\gamma Q\left(\sqrt{\frac{2\gamma G_p}{\frac{\gamma}{u}+2\varepsilon}}\right). \qquad (3.7)$$

З іншого боку, при використанні імпульсного глушіння, найбільш шкідливий ефект на комунікаційну систему досягається при певних значеннях γ – γ^*:

$$\gamma^*=\begin{cases}\dfrac{0{,}709}{E_S/N_T}, & E_S/N_T>0{,}709\\ 1\ , & E_S/N_T\le 0{,}709,\end{cases} \qquad (3.8)$$

де E_S – енергія на символ даних;

N_T – щільність шуму, коли генератор шуму активний.

Відповідне максимальне значення BER [5]:

$$P_e^*=\begin{cases}\dfrac{0{,}083}{E_S/N_T}, & E_S/N_T>0{,}709\\ Q\left(\sqrt{\dfrac{2E_s}{N_T}}\right), & E_S/N_T\le 0{,}709.\end{cases} \qquad (3.9)$$

Ця функція зображена на рисунку 3.8, який ілюструє переваги імпульсного широкосмугового глушіння над безперервним широкосмуговим глушінням незакодованих систем BPSK DSSS. Імпульсний глушитель має перевагу приблизно на 20 дБ над загороджувальним BBN глушінням при BER=10^{-4}. При відношенні E_S/N_T=-3 дБ і менше обидва методи глушіння дають приблизно однакові результати.

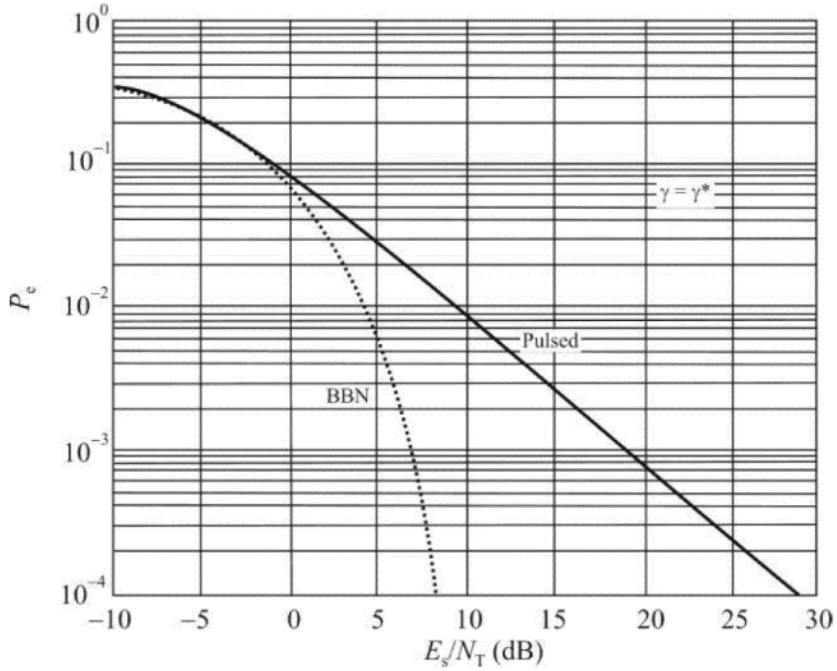

Рисунок 3.8 – Ефективність імпульсного глушіння при γ* некодованих систем з DSSS з BPSK модуляцією в порівнянні з широкосмуговим глушінням

На ефективність тонового глушіння впливають багато факторів серед яких можна виділити параметри сигналу/сигналів тонового глушіння, а також параметри системи зв’язку з прямим розширенням спектру. До зазначених параметрів глушіння можна віднести: розташування тонів в розширеному спектрі, кількість тонів, їх амплітуди, потужність, частотний зсув відносно цільового сигналу та інші. До параметрів системи зв’язку, які впливають на стійкість до глушіння тонами, можна віднести наступні: довжина PN-коду, метод модуляції несучої частоти (BPSK, QPSK), розподіл бітів (двофазний або чотирьох фазний) та інші. Через зазначене різноманіття конфігурацій, дослідження ефективності тонового глушіння є більш складною задачею і за обсягом цілком може бути виділено в окрему роботу. Тому в даній роботі коротко розглянемо вплив декількох із зазначених параметрів на ефективність тонового глушіння.

Математичне моделювання впливу тонового глушіння на системи з DSSS є більш складним через необхідність врахування багатьох факторів. В роботі [5] отримані аналітичні залежності для розрахунку функції BER для різних конфігурацій комунікаційних систем та тонового глушіння, а також наведені чисельні графічні зображення функції BER при різних умовах. Аналіз наведених матеріалів дозволив зробити ряд висновків щодо ефективності тонового глушіння

при різних умовах. Для зручності результати дослідження ефективності глушіння одним тоном зведені в таблицю 3.2.

Таблиця 3.2 – Ефективність глушіння одним тоном в різних умовах та з різними конфігураціями DSSS сигналів

<table>
<tr><td colspan="2">Двофазний розподіл бітів послідовності та BPSK модуляція</td></tr>
<tr><td>Довга кодова послідовність</td><td>Коротка кодова послідовність</td></tr>
<tr><td>Якщо тон глушіння не співпадає по частоті з сигналом ($\Delta\omega \neq 0$), для виграшу обробки 13 дБ, ефективність глушіння зменшується при віддаленні тону від центру спектра (f_0). Для виграшу 20 дБ, продуктивність глушіння залишається відносно постійною, незалежно від того, наскільки далеко розташований тон.
Ефективність впливу глушіння тоном залежить від відносної фази між перешкодами та сигналом, навіть якщо $\Delta\omega=0$ і довжина послідовності $L\to\infty$. Наприклад, для $\Delta\omega=0$ і $L\to\infty$, з різницею фаз $\theta=90°$ ефект перешкод повністю зникає, тоді як при $\theta=0°$ маємо найкращу продуктивність перешкод.</td><td>В даному випадку, розташування тону глушіння на одній частоті з сигналом DSSS ($\Delta\omega\to0$) не є найкращим рішенням через значне затухання тону. Набагато вигідніше розмістити перешкоду на частоті вище або нижче від несучої частоти на $1/T_s$ (де T_s – тривалість символу даних).
Коли код розширення стає довшим, глушіння стає складнішим і вимагає більшої потужності перешкод. Відносно легко досягти BER=10^{-2}, при N=4, тоді як для N=128 потрібно збільшити потужність перешкоди приблизно на 15 дБ.</td></tr>
<tr><td colspan="2">Чотирьох фазовий розподіл бітів послідовності та QPSK модуляція</td></tr>
<tr><td>Довга кодова послідовність</td><td>Коротка кодова послідовність</td></tr>
<tr><td>Коли L >> N, тип розширення для модуляції даних не має значення. Тому показники завадостійкості до глушіння одним тоном при QPSK такі ж, як і для BPSK модуляції.</td><td></td></tr>
</table>

Продовження таблиці 3.2

Чотирьох фазовий розподіл бітів послідовності та BPSK модуляція	
Довга кодова послідовність	Коротка кодова послідовність
При низьких JSR та BPSK модуляції даних, однотонове глушіння є більш ефективним при двофазному розширенні, ніж при чотирьох фазному розширенні. Однак, коли відношення завада/сигнал приблизно дорівнює G_p, глушіння одним тоном стає більш ефективним проти чотирьох фазового розширення. Крім того, при цьому рівні SNR, а також при нижчих значеннях, BER ≈ 10^{-1}, коли ε ≈ Gp. При високих JSR (ε>10 дБ) ефективність глушіння майже не залежить від SNR. Коли Δω ≠ 0, наслідки зміни зсуву частоти тону відносно несучої частоти DSSS такі ж, як і для двофазного розширення.	Якщо BER усереднено за θ [0, 2π), то двофазне та чотирьох фазне розширення забезпечують однакову завадостійкість при BPSK модуляції даних. З іншого боку, для когерентного джерела перешкод (θ = 0°) чотирьох фазне розповсюдження має перевагу на 3 дБ над двофазним. Якщо ми приймемо Pe≥10^{-2} як нашу міру успішного впливу глушіння, то для N≤32 дана конфігурація системи зв'язку з DSSS практично не забезпечує захисту від однотонової перешкоди.
Двофазний розподіл бітів послідовності та QPSK модуляція	
Довга кодова послідовність	Коротка кодова послідовність
Ефекти зміщення тону перешкод відносно центральної частоти DSSS у цьому випадку незначні. Криві значення функції BER майже ідентичні відповідним значенням для BPSK модуляції. Невелика різниця помітна для значень JSR вище 25 дБ. При Δω ≠ 0 глушник є настільки ж ефективним проти двофазного розширення/BPSK як і проти конфігурації двофазне розширення/ QPSK, коли L >> N.	

Ефективність глушіння широкосмугового сигналу мульти-тонами однакова для BPSK і QPSK модуляцій при використанні довгоперіодичних послідовностей. Чотирьох фазне розподілення бітів забезпечує на 2-3 дБ кращу продуктивність, ніж двофазне розподілення для довгих послідовностей.

Як показали проведені дослідження, одним з основних параметрів систем з прямим розширенням спектру, що визначає рівень її завадостійкості є довжина коду розширення. Довжина коду розширення в системі з DSSS впливає на можливість глушіння. Короткі коди, які повторюються після одного або кількох бітів даних, досить вразливі до спроб з'ясувати послідовність основного коду. Довгі коди, які повторюються після багатьох бітів даних, є менш вразливими. Для послідовностей середньої довжини BER залежить від конкретної послідовності розширення та буде різним для різних послідовностей розширення.

Також, для деяких технологій глушіння, критичним є розміщення перешкоди в розширеному спектрі, що використовується комунікаційною системою. Так, для PBN оптимальним є розміщення центру смуги з перешкодами в центрі сигналу DSSS; прямо протилежне розміщення оптимальне для глушіння мультитоном. CW тон, розміщений на центральній частоті розширеного спектра, зазнає серйозного затухання в процесі декореляції.

Слід зауважити, що відхилення сигналів вузькосмугових перешкод можливо за допомогою одного або кількох фільтрів відхилення (rejection filters) в приймачі, які є особливо ефективними проти мульти-тонових перешкод. Однак доволі важко відхилити сигнали глушіння BBN і PBN, оскільки це вимагає вирізання значних частин спектру, і зв'язок в цьому випадку був би ускладнений.

3.3 Методи захисту та підвищення завадостійкості систем з прямим розширення спектру

Перш ніж навести можливі методи мінімізації уразливості систем передачі з прямим розширенням спектру від різного роду завад та перехоплення, варто нагади, що технології передачі з використанням розширених шумоподібних спектрів були покликані для підвищення рівня захищеності безпроводової передачі даних. В деяких джерелах, подібні системи називають AJ (Antijam) системами [5]. Слід зазначити, що рівень захищеності систем з DSSS знаходиться на іншому якісному рівні в порівнянні з системами, що використовують вузькосмугові сигнали.

Виходячи з проведених в рамках виконання поточної магістерської роботи досліджень, сформулюємо можливі заходи мінімізації ризиків втрати конфіденційності, цілісності та доступності даних при їх передачі в системах з DSSS.

1) Одним з основних параметрів систем з прямим розширенням спектру, що визначає рівень її захищеності є довжина коду розширення. Довжина коду розширення в системі з DSSS впливає на можливість і ефективність глушіння, перехоплення та застосування імотозавад.

Так, в попередніх розділах показано, що при збільшення довжини коду розширення підтримання значення BER на тому ж рівні вимагає збільшення потужності перешкод.

З точки зору забезпечення конфіденційності і цілісності передачі інформації, збільшення довжини ПВП підвищує енергетичну скритність широкосмугових сигналів, значно ускладнює дешифрування та збільшує час безпечної роботи системи.

2) Суттєвий вплив на характеристики систем з DSSS мають кореляційні властивості ПВП, які в свою чергу залежать від типу кодової послідовності, частоти проходження її символів та довжини коду. У випадках, коли велика кількість передавачів, що використовують різні коди, має працювати в одному частотному діапазоні, такі послідовності треба обирати так, щоб уникати взаємних перешкод між користувачами. Висока ступінь кореляції між опорною кодовою послідовністю приймача та кодовою послідовністю перешкоджаючої станції призводить до збільшення вірогідності хибного виявлення в приймачі і в деяких обставинах навіть до встановлення хибної синхронізації приймача.

3) Заходи спрямовані на поліпшення процесу синхронізації та зменшення часу роботи системи в режимі пошуку сигналу та синхронізації.

Під час синхронізації існує ризик встановлення хибної синхронізація, яка, в свою чергу, може виникати через завантажений радіоефір, а може бути результатом нав’язування імітаційних перешкод зловмисником. Саме тому середній час досягнення синхронізації може вважатися одним із критерієм якості системи зв’язку з прямим розширенням спектру.

Вибір методу синхронізації, залежить від призначення системи, часу, що відводиться для встановлення синхронізації, а також розмірів області невизначеності параметрів сигналів що приймаються.

4) Вибір фазової модуляції з урахуванням призначення та умов експлуатації системи. Наприклад, фазова модуляція QPSK має переваги щодо зайнятості спектру порівняно з BPSK модуляцією, однак характеристики системи зв’язку з QPSK більш чутливі до шуму та перешкод.

5) Використання сучасних методів криптографії сприяє вирішенню задач забезпечення конфіденційності даних. Цей підхід в комбінації зі збільшенням довжини ПВП та підвищенням параметричної скритності сигналів фактично унеможливлює перехоплення значущої інформації.

6) При побудові приймального тракту системи з прямим розширенням спектру, необхідно вирішувати задачі та враховувати рекомендації зазначені в розділі 2.5 поточної роботи.

7) Для покращення загального рівня завадостійкості системи, рекомендується використовувати спеціальні коди для виявлення та корекції помилок в передачі даних. Наприклад, в роботі [9] наведені результати покращення завадостійкості та зниження рівня BER систем з широкосмуговими сигналами завдяки застосуванню блочного кодування (block coding) та кодування з використанням конволюційних кодів (convolutional coding).

8) Застосування адаптивної обробки сигналів для підвищення продуктивності і стабільності роботи систем з DSSS у різних умовах експлуатації [3, 11].

Адаптивна обробка сигналів означає зміну характеристик приймача відповідно до діючої сигнально-перешкодової обстановки. Тобто корекція параметрів пристрою обробки відбувається на підставі інформації, що отримується в процесі функціонування системи зв’язку. Загалом адаптивна система являє собою замкнутий контур, що містить об'єкт управління, пристрій контролю/ідентифікації, вирішальний пристрій та пристрій управління.

Адаптивна обробка сигналів може включати наступні заходи:

– застосування адаптивних фільтрів для підсилення або приглушення конкретних частот або шумів у сигналі DSSS;

– адаптивні алгоритми корекції помилок, які використовуються для виправлення спотворень в каналі зв'язку;

– керування потужністю;

– адаптивну синхронізацію для вирівнювання часових та частотних параметрів сигналу;

– спектральну адаптацію, що допомагає системі підлаштовувати ширину смуги та спектральні характеристики.

9) Дуже важливим заходом, спрямованим на захист систем з DSSS є забезпечення параметричної скритності системи. Під параметричною скритністю розуміється запобігання витоку наступної інформації про параметри системи зв’язку та її сигнали:

– тип кодової послідовності та її довжина;

– спосіб модуляції;

– частота центрального сигналу та ширина смуги, що використовуються системою;

– характеристики шуму та завад в каналі;

– техніка управління потужністю та інше.

Як показали проведені дослідження, знання зловмисником зазначеної інформації значно полегшують процеси перехоплення даних, постанови імітаційних завад та глушіння систем з прямим розширенням спектра.

Забезпечення параметричної секретності в системах DSSS вимагає комплексного підходу, який включає технічні, криптографічні та фізичні заходи безпеки. Системи повинні бути проектовані та конфігуруванні з урахуванням сучасних стандартів безпеки для забезпечення високого рівня захисту.

Розглянуті методи дозволяють істотно підвищити стійкість систем з прямим розширенням спектру до різних типів протидії, але підвищення стійкості зазвичай супроводжуються підвищенням складності та вартості комунікаційної мережі. Тому, при проектуванні реальних систем, треба враховувати доцільність застосування заходів підвищення завадостійкості. Так, можна прийняти деякі компромісні безпекові рішення при створенні громадських комунікаційних безпроводових мереж, а натомість отримати прийнятну вартість розгортання мережі та її підтримки. Але в деяких випадках, наприклад в військовій або аерокосмічний сферах, потрібен максимальний рівень захищеності процесу передачі даних.

4 АНАЛІЗ ПРОБЛЕМ У БЕЗПРОВОДОВИХ МЕРЕЖАХ СТАНДАРТІВ IEEE 802.11 ТА IEEE 802.15.4

В залежності від розміру зони дії безпроводової мережі виділяють чотири групи безпроводових мереж, які зображено на рисунку 4.1.

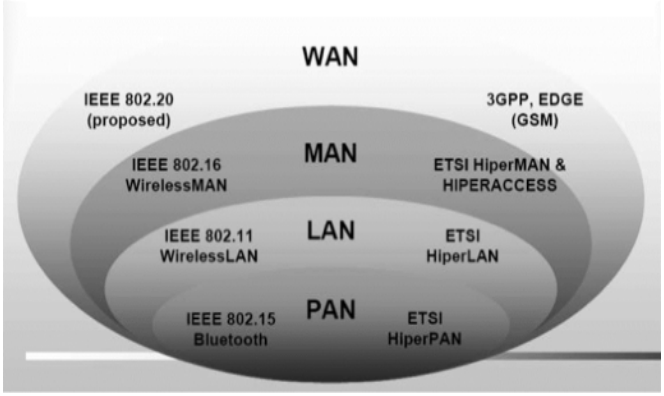

Рисунок 4.1 – Класифікація безпроводових мереж передачі даних

Розглянемо деякі особливості функціонування груп нижніх рівнів WPAN (Wireless Personal Area Network) та WLAN (Wireless Local Area Network) створених, відповідно, на основі стандарту IEEE 802.15.4 та сімейства стандартів IEEE 802.11.

4.1 Безпроводові мережі стандарту IEEE 802.15.4

Персональні безпроводові мережі (WPAN) функціонують приблизно в радіусі 10 м та орієнтовані, головним чином, на використання в якості засобів зв'язку між автономними приладами та обладнанням. У корпоративному секторі це можуть бути, наприклад, складські системи, системи автоматизації виробництва, різні датчики, сенсори, сервоприводи, електронні мітки, а в домашніх умовах – комп’ютери, ігрові приставки, системи безпеки, освітлення, кондиціювання, радіофіковані іграшки та навіть пульти дистанційного керування.

Основна ідея використання цієї технології полягає у зниженні вартості, малому споживанні при передачі даних на короткі відстані. Цей стандарт є основою для ряду специфікацій, таких як ZigBee, WirelessHART, MiWi, ISA100.11a, 6LoWPAN тощо. Враховуючі низьку вартість розгортання таких мереж, низький півень енергоспоживання та низькі швидкості передачі даних,

протокол IEEE 802.15.4 також ідеально підходить до розгортання безпроводових сенсорних мереж – WSN (Wireless Sensor Network) [12].

В залежності від дати виходу специфікації стандарту IEEE 802.15.4 в системах WPAN може бути різні набори каналів, частотні діапазони, метод модуляції та розширення спектру. В більшості випадків використовується пряме розширення спектру з BPSK або QPSK модуляцією. Доволі поширені є версії WPAN мереж з DSSS, що працюють в діапазоні 2,4 ГГц. Частотні канали в діапазоні 2,4 ГГц, що використовуються стандартом 802.15.4 зображено в верхній частині рисунка 4.2.

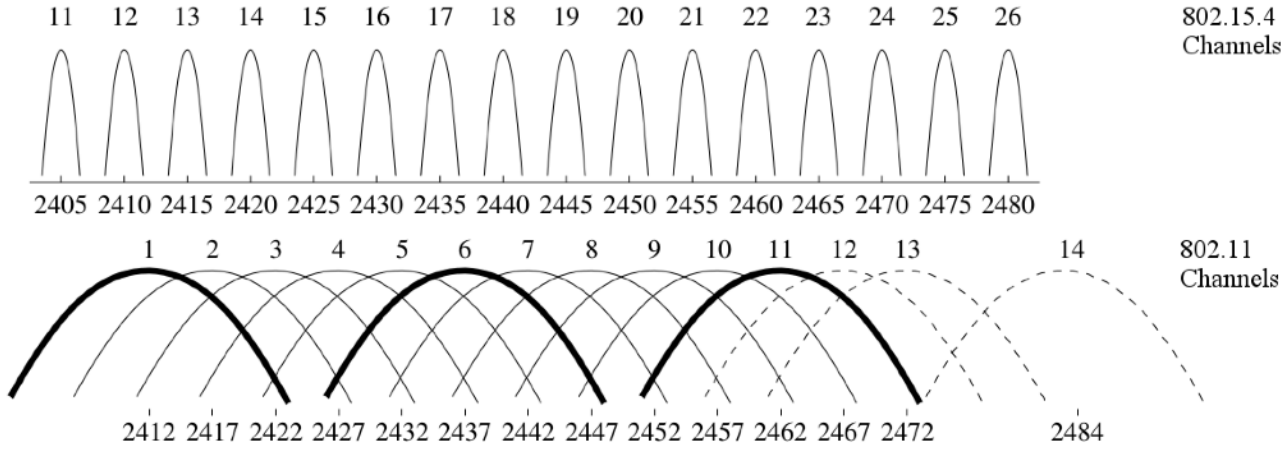

Рисунок 4.2 – Частотні канали в діапазоні 2,4 ГГц, що використовуються технологіями 802.11 та 802.15.4

Слід зазначити, що для мереж WPAN, побудованих на основі стандарту IEEE 802.15.4 з прямим розширенням спектру будуть справедливими всі висновки щодо вразливостей до різного роду перешкод, наведені в попередній частині роботи.

Мережі WPAN є вразливими для атак пасивного прослуховування, і навіть для атак активної фальсифікації, оскільки для участі у інформаційному обміні тут не потрібно мати фізичного підключення до проводів. Характерні особливості цих мереж роблять їх навіть дещо вразливішими. Пристрої є дешевими та мають обмежену обчислювальну потужність, оперативну пам'ять і не можуть забезпечити навіть високий рівень роботи генератора випадкових чисел. Ці обмеження обмежують переваги від розширення спектру, можуть серйозно звузити вибір криптографічних алгоритмів та протоколів, а також вплинути на структуру безпеки. Крім того, час життя автономних джерел живлення і вартісні обмеження встановлюють жорсткі границі на надмірність, пов'язану з безпекою.

При цьому вважається, що більшість архітектурних елементів безпеки мають бути реалізовані на вищих мережевих рівнях.

Криптографічний механізм даного стандарту базується на симетричній ключовій схемі і використовує ключі, що поставляються вищерозташованим мережевим рівнем. Робота з кріптоключами знаходиться за межами цього стандарту. Криптографічний механізм забезпечує певні комбінації таких послуг безпеки як конфіденційність та цілісність [13].

4.2 Безпроводові мережі сімейства стандартів IEEE 802.11

Наступна група бездротових мереж WLAN базується на специфікаціях основного стандарту IEEE 802.11. Сімейство складається зі стандартів IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac, IEEE 802.11ax та IEEE 802.11be. Це найбільш широко використовувані мережеві стандарти, мережі побудовані на їх основі більш відомі як Wi-Fi мережі.

В залежності від версії стандарту, можуть різнитися частотний діапазон (2,4 та 5 ГГц), пропускна здатність, ширина каналу, дальність передачі, тип модуляції, наявність та відсутність різних технологій, захисту та інше. Більш детально ознайомитися зі специфікаціями різних версій стандарту можна за посиланням [14].

WLAN мережі використовують пряме розширення спектру але на відміну від WPAN мереж мають набагато більшу енергетичну потужність та оперують більш широкими діапазонами розширення спектру, що позитивно позначується на їх завадостійкості на відміну від WPAN. При цьому, безпекові ризики, зазначені для WPAN систем є актуальними і для WLAN.

Як показано в [15], для передачі широкосмугових сигналів з технологією DSSS в діапазоні 2,4 ГГц передбачено використання смуги частот 83 МГц від 2,400 ГГц до 2,483 ГГц, який поділений на 13 каналів та додатковий 14-й канал (рисунок 4.2). В більшості країн дозволено до використання 13 каналів, 11 – в США та Канаді, 14 – тільки в Японії. Наприклад, перший канал працює в смузі 2,401…2,423 ГГц, тобто 2,412 ГГц±11 МГц. Рознесення між центральними частотами сусідніх каналів в цьому діапазоні складає 5 МГц.

Для виключення взаємних завад між каналами необхідно, щоб їх смуги не перекривалися, тобто мали рознесення 25 МГц. Тобто в одній зоні одночасно

можуть використовуватися тільки три канали, які не перекриваються. Наприклад, канали з номерами 1, 6, 11, або 2, 7, 12, або 3, 8, 13 (рисунок 4.2.).

Для забезпечення безпеки в WLAN мережах використовують наступні засоби:

– протоколи шифрування (WEP, WPA, WPA2);
– протоколи автентифікації (802.1x, RADIUS, EAP);
– віртуальні приватні мережі (VPN);
– відключення розсилки ідентифікатора мережі (SSID);
– контроль за підключенням до точки доступу на основі MAC-адресів;
– винесення безпроводової мережі за міжмережевий екран;
– використання спеціального програмного забезпечення (наприклад, AirDefense Guard, AirMagnet тощо).

4.3 Співіснування мереж стандартів IEEE 802.11 та IEEE 802.15.4 в частотному діапазоні 2,4 ГГц

Як було показано вище, бездротові технології IEEE 802.11 (Wi-Fi) та IEEE 802.15.4 (Zigbee) доволі часто працюють в одному діапазоні частот – 2,4 ГГц. В свою чергу, мережі Zigbee мають дуже низький рівень потужності передачі та є менш завадостійкими. Відносно потужні сигнали пристроїв на основі стандарту IEEE 802.11 перекривають спільні канали і через це створюються додаткові радіоперешкоди. Дана ситуація проілюстрована на рисунку 4.3.

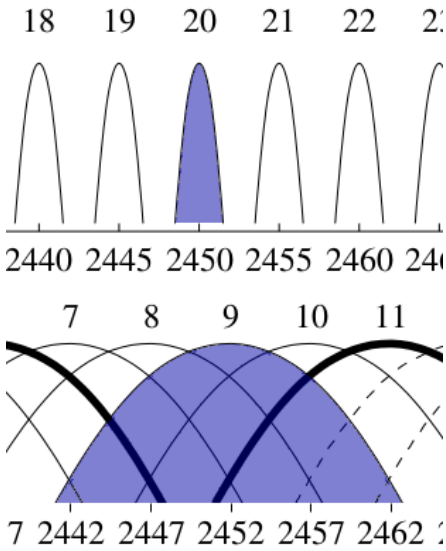

Рисунок 4.3 – Перекриття спектрів передачі Wi-Fi та WPAN

Цікаві дослідження, присвячені проблемі співіснування стандартів IEEE 802.11 та IEEE 802.15.4 в частотному діапазоні 2,4 ГГц були проведені в роботі [16]. Було показано, що перешкоджаючі сигнали IEEE 802.11b/g/n менше впливали на канали IEEE 802.15.4 в випадках, коли центральні частоти цих каналів не співпадали з центральними частотами каналів WLAN, що використовувалися.

Якщо зсув центральних частот між обраним каналом WLAN і стандартним каналом IEEE 802.15.4 перевищує 12 МГц, тоді середній прийом пакетів, записаний у трафіку на основі стандарту IEEE 802.11b/g, становить близько 85-95 %. Таким чином, для успішного співіснування рекомендований зсув центральних частот каналів має перевищувати 12 МГц. Перешкоди стають майже непомітними, якщо зсув між центральними частотами становить 20 МГц.

Також було помічено, що перекриття каналів призводило до збільшення затримки в мережі IEEE 802.15.4.

5 МОДЕЛЮВАННЯ СИСТЕМИ З DSSS В УМОВАХ ДІЇ ОДНОТОНОВОЇ ПЕРЕШКОДИ ТА АДИТИВНОГО БІЛОГО ГАУСІВСЬКОГО ШУМУ

В даному розділі наведено короткий опис розробленої моделі та результати моделювання в графічному вигляді.

5.1 Опис імітаційної моделі

Розроблена модель симулює роботу системи зв'язку з DSSS в умовах наявності АБГШ та однотонового перешкоджаючого сигналу. Додавання АБГШ дозволяє провести оцінку характеристик системи зв’язку в умовах, максимально наближених до реальних умов функціонування системи через те, що в ефірі, на всіх частотах, завжди присутній певний рівень шуму. Для практичної реалізації моделі використовувалася середа MATLAB.

При створенні імітаційної моделі системи з DSSS була використана блок-схема [17], наведена на рисунку 5.1. На базі цієї блок-схеми був написаний програмний код в середовищі MATLAB. Як видно з рисунка 5.1, модель включає наступні складові:

– передавач, що включає випадкове двійкове інформаційне джерело та повторювач, що повторює інформаційний потік G_p раз (G_p – виграш обробки);
– генератор ПВП (блок «PRBS generator» на схемі);
– генератор однотонової перешкоди для заданого значення JSR (блок «Jammer»);
– генератор АБГШ (блок «AWGN»);
– приймач, який включає суматор отриманих шумових сигналів та псевдо-випадкового сигналу, приймач кореляційного типу та блок виявлення порогових значень.

В моделі системи з DSSS була застосована стандартна двійкова фазова модуляція (BPSK) та m-послідовності для розширення спектра інформаційного сигналу.

Однотоновий інтерференційний сигнал був змодельований з використанням синусоїди. Слід зазначити, що однотоновий сигнал перешкоди є найпростішим для генерування. Дискретне рівняння за часом для генерації однотонової

перешкоди, яке було використано в процесі побудови моделі, визначається наступним рівнянням:

$$J(t)=\sqrt{2P_j}\sin\left(2\pi f_j t+\theta_j\right), \tag{5.1}$$

де P_j – середня потужність j-го тону;

f_j – частота j-го тону;

θ_j – його фазовий зсув відносно цільового сигналу, який рівномірно розподілений на (0, 2π].

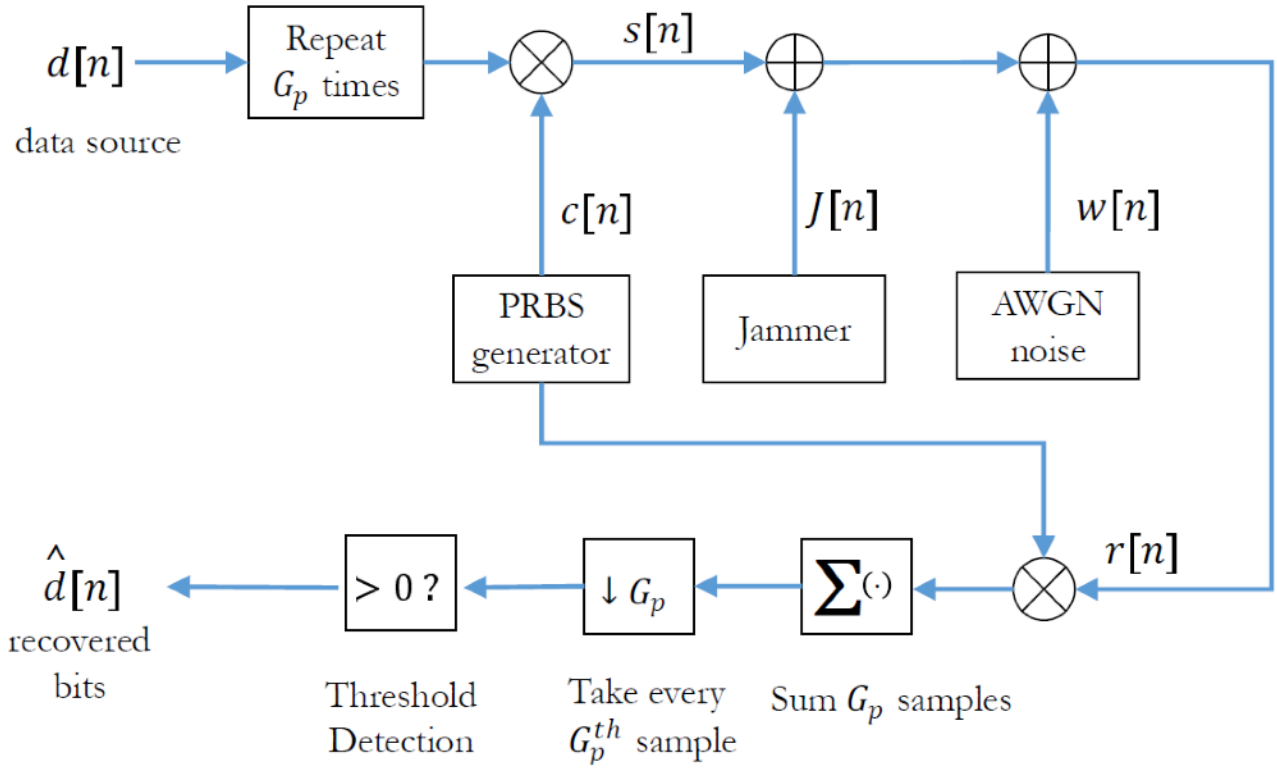

Рисунок 5.1 – Блок-схема імітаційної моделі системи з DSSS та з BPSK модуляцією під впливом АБГШ та тональних перешкод

Слід зазначити, що застосування моделі може бути поширено на випадки мульти-тонового впливу завдяки модифікації виразу (5.1) наступним чином:

$$J(t)=\sum_{i=1}^{N}\sqrt{\frac{2P_j}{N}}\sin\left(2\pi f_{ji} t+\theta_{ji}\right), \tag{5.2}$$

де N– кількість тонів (N≥1).

Для кількісного оцінювання ефективності глушіння використовується коефіцієнт BER.

5.2 Результати чисельного модулювання

Розроблена модель дозволяє дослідити вплив АБГШ та однотонової перешкоди на BER системи зв'язку з DSSS та BPSK модуляцією. Вихідні дані, що використовувалися в процесі розрахункових досліджень, наведені в таблиці 5.1.

Таблиця 5.1 – Вихідні дані

Параметр	Значення
Виграш обробки	31
Кількість бітів даних для передачі	10E5
Відношення потужності сигналу до АБГШ (E_b/N_0), дБ	-4, -2, 0,…,12
JSR, дБ	-100;-5; 0; 2; 5
Зміщення частоти перешкод відносно центральної частоти сигналу	1E-4

Результати чисельного моделювання для різних рівнів JSR наведені на рисунках 5.1 – 5.5.

Значення JSR (JSR>0, дБ) відповідають випадкам, коли сигнал однотонової перешкоди сильніший за широкосмуговий сигнал системи зв’язку. Негативні значення JSR (JSR<0, дБ) відображують ситуацію, коли сигнал системи зв’язку більш потужний за сигнал глушіння.

На рисунку 5.1 зображено функцію BER для випадку, коли відношення JSR=-100 дБ. При таких значення JSR можна сказати, що потужність однотонового глушника настільки мала, що система зв’язку не відчуває цього впливу і працює за умов впливу лише АБГШ.

З графіків, зображених на рисунках 5.2 – 5.5 видно, що поступове збільшення потужності однотонової завади призводить до збільшення значень коефіцієнту BER при фіксованих значеннях відношення енергії широкосмугового

сигналу до потужності АБГШ – E_b/N_0 (в даному випадку, фактично є відношенням SNR). Така поведінка моделі є цілком фізичною.

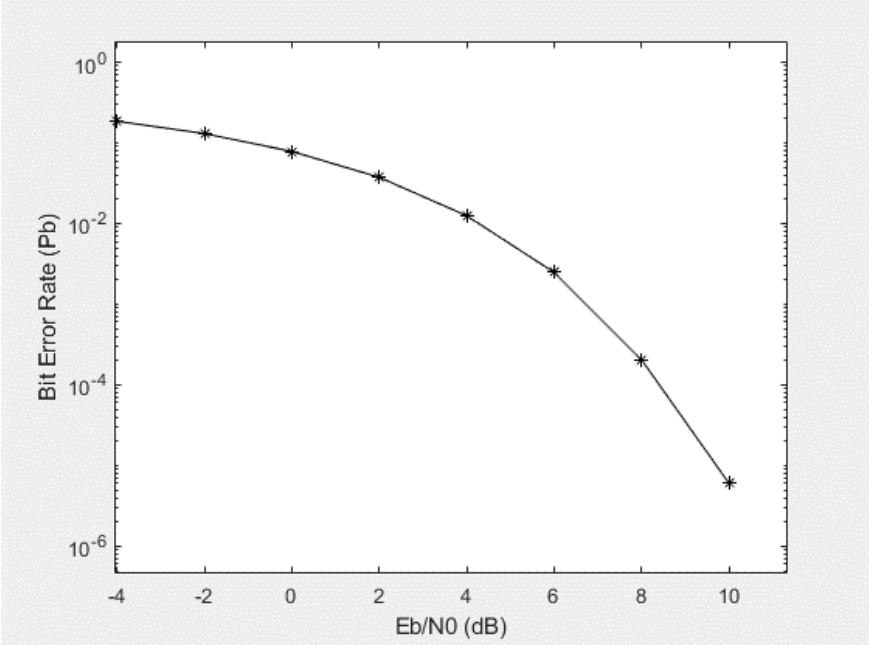

Рисунок 5.1 – Ефективність глушіння системи з DSSS та з BPSK модуляцією однотоновою перешкодою JSR -100 дБ в середі з АБГШ різної спектральної щільності

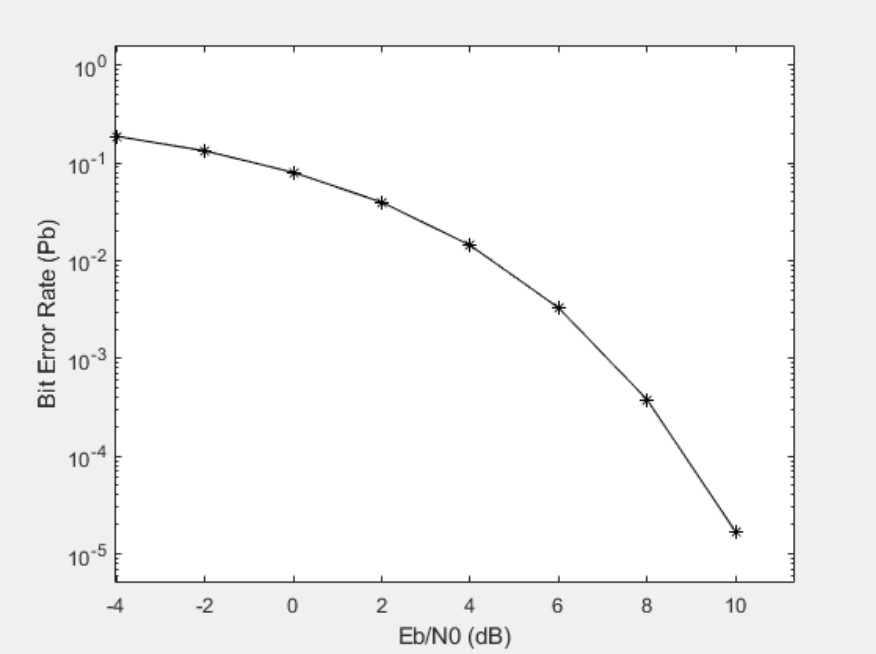

Рисунок 5.2 – Ефективність глушіння системи з DSSS та з BPSK модуляцією однотоновою перешкодою JSR -5 дБ в середі з АБГШ різної спектральної щільності

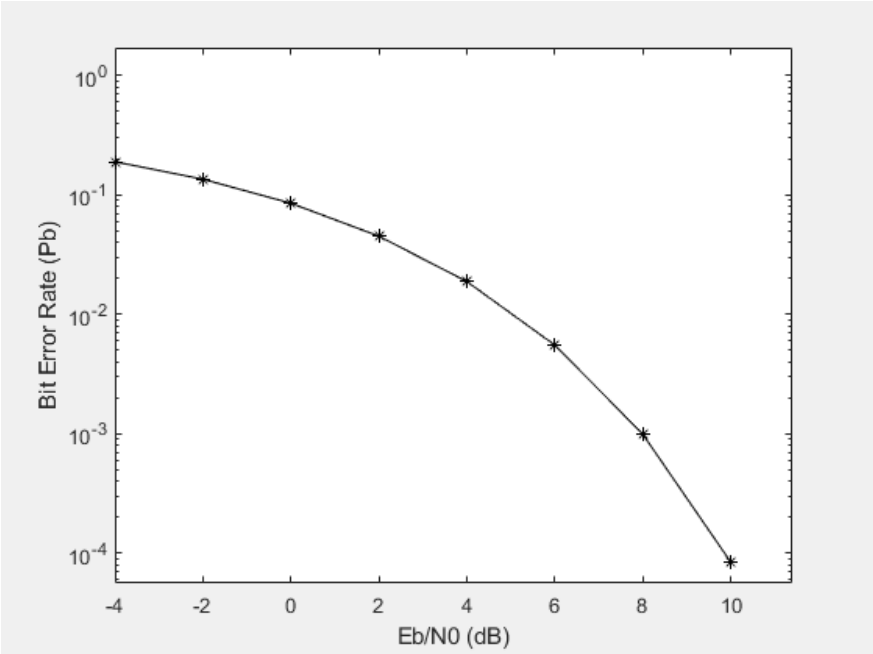

Рисунок 5.3 – Ефективність глушіння системи з DSSS та з BPSK модуляцією однотоновою перешкодою JSR 0 дБ в середі з АБГШ різної спектральної щільності

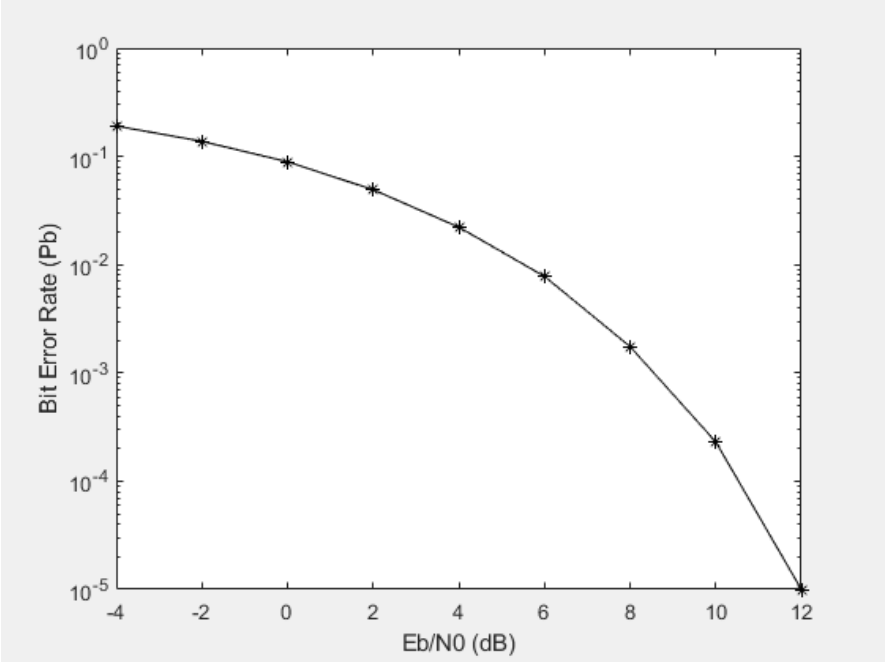

Рисунок 5.4 – Ефективність глушіння системи з DSSS та з BPSK модуляцією однотоновою перешкодою JSR 2 дБ в середі з АБГШ різної спектральної щільності

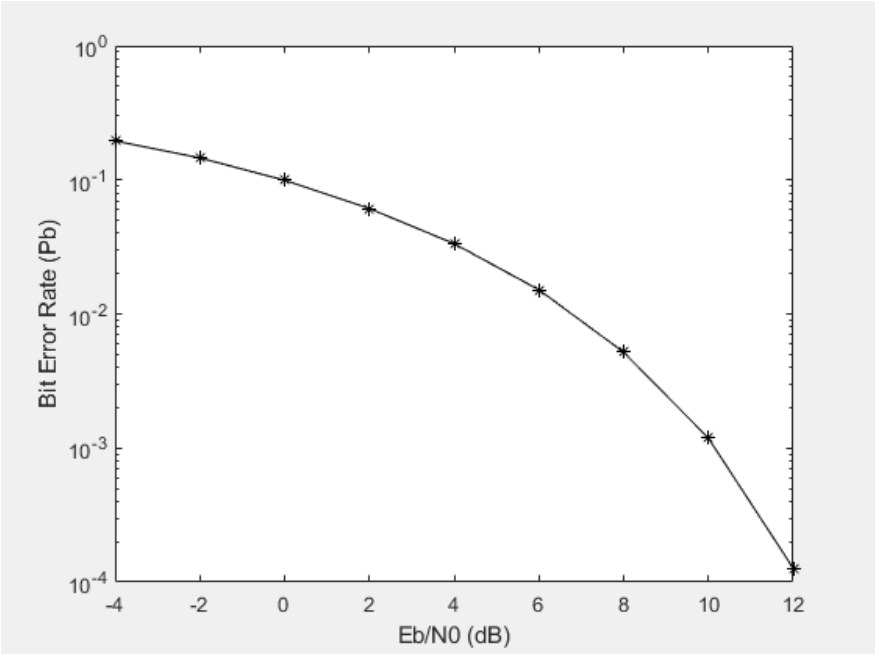

Рисунок 5.5 – Ефективність глушіння системи з DSSS та з BPSK модуляцією однотоновою перешкодою JSR 5 дБ в середі з АБГШ різної спектральної щільності

Суттєву різницю між значеннями BER для різних значень JSR можна спостерігати при високих значеннях E_b/N_0. Наприклад, при E_b/N_0=10 дБ BER для JSR=-5 дБ складає 2,2E-5, а для JSR=5 дБ BER дорівнює 1,213E-3. При підвищені рівня АБГШ та відповідному зменшенні E_b/N_0 зазначена різниця значень BER зменшується і майже повністю нівелюється при значенні E_b/N_0=-2 дБ.

Порогове значення коефіцієнта BER (10E-1) для всіх розглянутих випадків досягається при $E_b/N_0\approx$-1 дБ і це більше пов’язано з впливом АБГШ.

В попередньому розділі при розгляді впливу однотонової завади на систему з DSSS було зазначено, що ефективність впливу завади залежіть від розташування тонової перешкоди в частотному діапазоні широкосмугового сигналу. Запропонована імітаційна модель дозволяє розміщувати тоновий сигнал в будь-якому місці в рамках спектру широкосмугового сигналу, тобто f_j в виразі (5.1) може приймати значення в діапазоні (-0,5; 0,5), при цьому значення f_j=0 відповідає розміщенню тону в середині спектру широкосмугового сигналу. Нижче, на рисунку 5.5, представлені результати розрахункових досліджень впливу зміщення частоти однотонової перешкоди відносно центральної частоти сигналу при JSR=-2 дБ та наявності АБГШ.

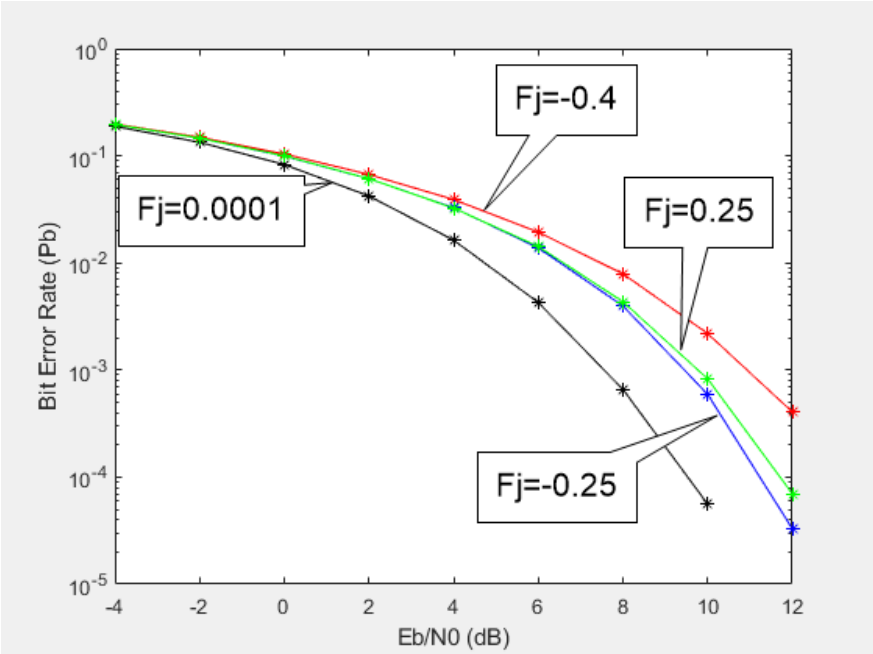

Рисунок 5.5 – BER системи з BPSK DSSS для різних значень зміщення частоти однотонової перешкоди відносно центральної частоти сигналу при JSR=-2 дБ

Аналіз результатів, зображених на рисунку 5.5, дає змогу стверджувати, що в даному випадку (для даної конфігурації і даного набору параметрів моделі) зміщення частоти розташування однотонової перешкоди в будь-яку сторону від центра спектру широкосмугового сигналу призводить до збільшення значень коефіцієнту BER і, відповідно, до підвищення ефективності однотонової завади. Для більших значень відношення енергії широкосмугового сигналу до потужності АБГШ (E_b/N_0) можна спостерігати більший ефект від зміщення частоти. І навпаки, при низьких значеннях E_b/N_0, коли рівень АБГШ істотно перевищує енергію сигналу, цей ефект зникає.

На завершення можна сформулювати деякі висновки стосовно запропонованої моделі.

1) Результати розрахункових досліджень підтвердили адекватність імітаційної моделі, отримані залежності не суперечать фізичним явищам, що мають місце в системах з DSSS при протидії однотоновою перешкодою.

2) Дана модель може використовуватися для різного роду досліджень та може бути використана в якості бази для розробки більш складної імітаційної моделі (з використанням різних ПВП для розширення сигналу, обробки мульти-тонових перешкод, додавання інших типів інтерференційних сигналів та інше).

3) Через відсутність експериментальних даних або достовірних даних отриманих іншим шляхом, дана модель не була провалідована. Надання кількісних оцінок тільки на основі результатів, отриманих за допомогою розглянутої моделі не може бути рекомендованим.

ВИСНОВКИ

Завдання на кваліфікаційну роботу виконано у повному обсязі.

Проведені дослідження принципів побудови систем передачі даних з DSSS дозволили визначити параметри систем, які впливають на ступінь захищеності від перехоплення та різного роду завад. Подальший аналіз дозволив сформулювати ряд рекомендацій, що мають бути прийняті до уваги при створенні комунікаційних систем які працюють в складних завадових умовах або оперують важливими даними. Зазначені рекомендації спрямовані на зниження ризиків, пов'язаних з загрозами втрати конфіденційності, цілісності та доступності даних в процесі їх передачі через бездротові мережі. Звісно, що найбільш ефективним є комплексне застосування наведених рекомендацій, а також застосування адаптивної обробки сигналів, основні складові якої наведені в розділі 3.3.

Також в процесі роботи була розглянута ефективність різних методів протидії функціонуванню системам з DSSS за різних умов. До найбільш ефективних технологій протидії системам зв'язку з прямим розширення спектру можна віднести імітаційні завади, а також глушіння PNB, імпульсними та тоновими завадами. Ефективність зазначених методів залежить як від параметрів та конфігурації системи комунікацій, так і параметрів реалізації протидії.

Реалізована імітаційна модель системи з DSSS та BPSK модуляцією дозволяє досліджувати вплив тонової перешкоди варійованої потужності в середовищі з АБГШ. Результати чисельного моделювання підтвердили адекватність моделі, отримані графічні залежності не суперечать фізичним процесам, що мають місце при протидії тоновою перешкодою. Для практичного застосування модель має бути піддана валідаційній процедурі, що не було виконано в даній роботі через відсутність експериментальних даних.

Окремі результати роботи доповідались на двох міжнародних наукових конференціях [1, 2].

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Руденко О. С. Дослідження технологій протидії системам передачі з прямим розширенням спектра. *Електронні та мехатронні системи: теорія, інновації, практика* : зб. наук. праць за матеріалами IX Всеукраїнської наук.-практ. конф., м. Полтава, 10 лист. 2023 р. Полтава, 2023. С. 14–15.
2. Руденко О. С. Дослідження методів мінімізації уразливості систем передачі з прямим розширенням спектра. *Сучасні аспекти та перспективні напрямки розвитку науки* : зб. за матеріалами VI Міжнар. студентської наук. конф., м. Харків, 19 січ. 2024 р. Харків, 2024. С. 249–251.
3. Харитонов А.С. Анализ и синтез адаптивных устройств помехозащиты в радиолиниях с широкополосными шумоподобными сигналами, входящих в состав радиолокационных комплексов : дисс. ... канд. техн. наук : 05.12.14. Москва: МГТУ, 2011. 110 с.
4. Кабак В.С., Уваров Р.В. Функціональні пристрої телефонів мобільного зв’язку : навч. посібник. Запоріжжя : ЗНТУ, 2007. 375 с.
5. Poisel R. Modern Communications Jamming Principles and Techniques, Second Edition. USA: Artech House, 2011. 870 p.
6. Кузовников А. В., Сомов В. Г., Черноусов А. В. Оценка устойчивости широкополосных сигналов к имитационным помехам. *Вестник СибГАУ.* Красноярск, 2013. №4(50). С. 81-84.
7. Галкин В.А. Мобильные системы радиосвязи. Радиоканал : учебное пособие. Москва: МИЭТ, 2003. 300 с.
8. Диксон Р.К. Широкополосные системы: пер. с англ. / под ред. В.И. Журавлёва. Москва: Связь, 1979. 304 с.
9. Ziemer R. E. Fundamentals of Spread Spectrum Modulation. USA: Morgan and Claypool Publishers, 2007. 78 p.
10. Torrieri D. Principles of spread-spectrum communication systems. USA: Spinger, 2005. 444 p.
11. Варакин Л.Е. Системы связи с шумоподобными сигналами. Москва: Радио и связь, 1985. 384 с.
12. Сети стандарта IEEE 802.15.4. URL: https://www.rovdo.com/ieee-802-15-4-networks (дата звернення: 22.12.2023).

13. Беспроводные сети ZigBee и IEEE 802.15.4. URL: http://book.itep.ru/4/41/zigbee.htm (дата звернення: 22.12.2023).

14. IEEE 802.11™ Wireless Local Area Networks. The working group for WLAN standards. URL: https://www.ieee802.org/11/ (дата звернення: 23.12.2023).

15. Головін Ю.О. Основи радіозв'язку з рухомими об'єктами: навч. посіб. Київ: ІСЗЗІ НТУУ КПІ, 2016. 322 с.

16. Verma R. Assessing coexistence of IEEE 802.15.4 networks and IEEE 802.11b/g/n networks – A study of interference effects : master degree project : 2019. Ames IA: Iowa State University, 2019. 35 p.

17. Mathuranathan Viswanathan, Wireless Communication Systems in Matlab, Second Edition. Independently Published, 2020. 368 p.