

Міністерство освіти і науки України  
Національний технічний університет  
«Дніпровська політехніка»

---

---

Інститут електроенергетики  
Факультет інформаційних технологій  
Кафедра безпеки інформації та телекомунікацій

**ПОЯСНЮВАЛЬНА ЗАПИСКА**  
кваліфікаційної роботи ступеня магістра

студента Ковтуна Кирила Андрійовича

академічної групи 125м-19-1

напряму підготовки 125 Кібербезпека

спеціалізації<sup>1</sup>

за освітньо-професійною програмою

на тему «Забезпечення конфіденційності при передачі інформації в системах  
зв'язку з фазоманіпульованими сигналами»

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н. доц. Герасіна О.В.			
розділів:				
спеціальний	к.т.н. доц. Герасіна О.В.			
економічний	к.е.н., доц. Пілова Д.П.			

Рецензент				
-----------	--	--	--	--

Нормоконтролер	ст. викл. Мешков В.І.			
----------------	-----------------------	--	--	--

Дніпро

2020

**ЗАТВЕРДЖЕНО:**  
завідувач кафедри  
безпеки інформації та телекомунікацій  
\_\_\_\_\_ д.т.н., проф. Корнієнко В.І.

«\_\_\_\_\_» \_\_\_\_\_ 20\_\_ року

**ЗАВДАННЯ  
на кваліфікаційну роботу  
ступеня магістра**

студенту \_\_\_\_\_ академічної групи \_\_\_\_\_  
Ковтуну Кирилу Андрійовичу 125м-19-1  
(прізвище та ініціали) (шифр)

спеціальності \_\_\_\_\_  
125 Кібербезпека

на тему \_\_\_\_\_  
«Забезпечення конфіденційності при передачі інформації  
в системах зв'язку з фазоманіпульованими сигналами»

Затверджену наказом ректора НТУ «Дніпровська політехніка» від 22.10.2020 №888-с

Розділ	Зміст	Термін виконання
Розділ 1	Аналіз існуючих підходів до конфіденційної передачі інформації в системах зв'язку з фазоманіпульованими сигналами.	03.09.2020 – 10.10.2020
Розділ 2	Підхід до конфіденційної передачі інформації в системах зв'язку з фазоманіпульованими сигналами та оцінка його ефективності.	11.10.2020 – 24.11.2020
Розділ 3	Розрахунок трудомісткості та капітальних витрат організації системи зв'язку з фазоманіпульованими сигналами конфіденційної передачі інформації.	25.11.2020 – 04.12.2020

Завдання видано \_\_\_\_\_  
(підпис керівника)

\_\_\_\_\_ Герасіна О.В.  
(прізвище, ініціали)

Дата видачі завдання: \_\_\_\_\_

Дата подання до екзаменаційної комісії: \_\_\_\_\_

Прийнято до виконання

---

(підпис студента)

Ковтун К.А.

---

(прізвище, ініціали)

## РЕФЕРАТ

Пояснювальна записка: 92 с., 25 рис., 1 таблиця, 4 додатки, 23 джерела.

Об'єкт дослідження – система зв'язку з фазоманіпульованими сигналами для конфіденційної передачі інформації.

Мета кваліфікаційної роботи – підвищення завадостійкості систем зв'язку в умовах структурних завад при фіксованій базі фазоманіпульованого сигналу.

Методи розробки: спостереження, порівняння, аналіз, опис.

Наукова новизна результатів полягає в ускладненні і маскуванні структури сигналу, сформованого на передавальній стороні, та в забезпеченні розпізнавання цієї структури і поліпшення компенсації структурних завад на приймальній стороні.

У першому розділі проаналізовано основи застосування шумоподібних сигналів в системах зв'язку, а також існуючі підходи до конфіденційної передачі інформації в системах зв'язку з фазоманіпульованими сигналами, та їх недоліки.

У спеціальній частині роботи запропоновано підхід до підвищення структурної та інформаційної складових скритності, а також підвищенні завадостійкості відомої системи в умовах структурних завад при фіксованій базі фазоманіпульованого сигналу.

У економічному розділі виконані розрахунки трудомісткості та капітальних витрат на організацію запропонованої системи зв'язку з фазоманіпульованими сигналами для передачі конфіденційної інформації.

ФАЗОМАНІПУЛЬОВАНИЙ СИГНАЛ, ЗАВАДОСТІЙКІСТЬ, СКРИТНІСТЬ, ВІДНОШЕННЯ СИГНАЛ \ ШУМ, АВТОКОРЕЛЯЦІЙНА ФУНКЦІЯ.

## РЕФЕРАТ

Пояснительная записка: 92 с., 25 рис., 1 таблица, 4 приложения, 23 источника.

Объект исследования - система связи с фазоманипулированными сигналами для конфиденциальной передачи информации.

Цель квалификационной работы – повышения помехоустойчивости систем связи в условиях структурных помех при фиксированной базе фазоманипулированного сигнала.

Методы разработки: наблюдение, сравнение, анализ, описание.

Научная новизна заключается в усложнении и маскировке структуры сигнала, сформированного на передающей стороне, и в обеспечении распознавания этой структуры и улучшения компенсации структурных помех на приемной стороне.

В первом разделе проанализированы основы применения шумоподобных сигналов в системах связи, а также существующие подходы к конфиденциальной передаче информации в системах связи с фазоманипулированными сигналами, и их недостатки.

В специальной части работы предложен подход к повышению структурной и информационной составляющих скрытности, а также повышению помехоустойчивости известной системы в условиях структурных препятствий при фиксированной базе фазоманипулированного сигнала.

В экономическом разделе выполнены расчеты трудоемкости и капитальных затрат на организацию предложенной системы связи с фазоманипулированными сигналами для передачи конфиденциальной информации.

ФАЗОМАНИПУЛИРОВАННЫЙ СИГНАЛ, ПОМЕХОУСТОЙЧИВОСТЬ,  
СКРЫТНОСТЬ, ОТНОШЕНИЕ СИГНАЛ \ ШУМ, АВТОКОРРЕЛЯЦИОННАЯ  
ФУНКЦИЯ.

## ABSTRACT

Explanatory note: 92 p., 25 pictures, 1 table, 4 applications, 23 sources.

The object of research is a chaotic synchronization communication system for confidential transmission of information.

The purpose of the qualification work is an increasing the noise immunity of communication systems in conditions of structural interference with a fixed base of phase-shift keyed signals.

Development methods: observation, comparison, analysis, description.

The scientific novelty of the results lies in the complexity and masking of the structure signal generated on the transmitting side, and in ensuring the recognition of this structure and improving the compensation of structural interference on the receiving side.

The first section analyzes basics of application of noise-like signals in communication systems, as well as the existing approaches to confidential transmission of information in a chaotic synchronization communication system, and their disadvantages.

In a special part of the work, an approach is proposed to increase the structural and informational components of secrecy, as well as to increase the noise immunity of a known system in conditions of structural obstacles with a fixed base of chaotic synchronization communication system.

In the economic section, calculations of labor intensity and capital costs for organizing the proposed chaotic synchronization communication system for confidential transmission of information.

PHASE MANIPULATED SIGNAL, NOISE RESISTANCE, SECRET, SIGNAL / NOISE RATIO, AUTO CORRELATION FUNCTION.

## СПИСОК УМОВНИХ СКОРОЧЕНЬ

- ААСС – асинхронні адресні системи зв'язку
- АКФ – автокореляційна функція
- АЦП – аналогово-цифровий перетворювач
- ВКФ – взаємкореляційна функція
- ВФН – взаємна функція невизначеності
- ПАВ – поверхневі акустичні хвилі
- ПАХ – поверхневі акустичні хвилі
- ПЛІС – логічних інтегральних схем із можливістю програмування
- СВЧ – надвисокі частоти
- ССПС – стільникові системи рухомого зв'язку
- ФМН – фазоманіпульований
- ФМ-ЧМ – фазо-частотноманіпульований
- ФН – функція невизначеності
- ЧМ – частотно-маніпульований
- ШОУ – широкосмуговий підсилювач - обмежувач - узгоджений фільтр
- ШПС – шумоподібний сигнал
- DDS – схема прямого цифрового синтезу



ВСТУП.....	<b>Ошибка! Закладка не определена.</b>	9
1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ.....	<b>Ошибка! Закладка не определена.</b>	10
1.1 Основи застосування шумоподібних сигналів в системах зв'язку	<b>Ошибка! Закладка не определена.</b>	10
1.1.1 Визначення шумоподібних сигналів і широкосмугових систем зв'язку	<b>Ошибка! Закладка не определена.</b>	10
1.1.2 Завадостійкість .....	<b>Ошибка! Закладка не определена.</b>	11
1.1.3 Завадостійкість широкосмугових систем зв'язку .	<b>Ошибка! Закладка не определена.</b>	12
1.1.4 Скритність системи зв'язку.....	<b>Ошибка! Закладка не определена.</b>	13
1.1.5 Кодовий поділ абонентів .....	<b>Ошибка! Закладка не определена.</b>	15
1.1.6 Ефективність ААСС.....	<b>Ошибка! Закладка не определена.</b>	16
1.1.7 Основні структурні схеми широкосмугових систем зв'язку .....	<b>Ошибка! Закладка не определена.</b>	18
1.2. Шумоподібні сигнали .....		25
1.2.1 Сигнали і спектри.....	<b>Ошибка! Закладка не определена.</b>	25
1.2.2 Основи оптимальної обробки сигналів.....		28
1.2.3 Кореляційні функції сигналів .....		30
1.2.4 Фазоманіпульовані сигнали, як один з основних типів ШПС.....		32
1.3 Існуючі підходи до конфіденційної передачі інформації в системах зв'язку з фазоманіпульованими сигналами.....		34
1.4 Висновок. Постановка задачі .....		39
2 СПЕЦІАЛЬНИЙ РОЗДІЛ .....		41

2.1 Підхід до конфіденційної передачі інформації в системах зв'язку з фазоманіпульованими сигналами.....	41
2.2 Оцінка ефективності запропонованого підходу до конфіденційної передачі інформації в системах зв'язку з фазоманіпульованими сигналами.....	56
2.3 Висновок .....	70
3 ЕКОНОМІЧНИЙ РОЗДІЛ.....	72
3.1 Обґрунтування витрат на організацію запропонованої системи зв'язку з фазоманіпульованими сигналами.....	72
3.2 Визначення трудомісткості організації запропонованої системи зв'язку з фазоманіпульованими сигналами.....	72
3.3 Розрахунок капітальних витрат на організацію системи зв'язку для конфіденційної передачі інформації з використанням фазоманіпульованих сигналів.....	73
3.4 Розрахунок річних експлуатаційних витрат на утримання і обслуговування запропонованої системи передачі конфіденційної інформації .....	77
3.5 Оцінка величини можливого збитку від атаки.....	79
3.6 Загальний ефект від впровадження запропонованої системи зв'язку з фазоманіпульованими сигналами.....	81
3.7 Визначення та аналіз показників економічної ефективності запропонованої системи зв'язку з фазоманіпульованими сигналами.....	82
3.8 Висновок .....	83
ВИСНОВКИ.....	84
ПЕРЕЛІК ПОСИЛАНЬ .....	86
ДОДАТОК А. ВІДОМІСТЬ МАТЕРІАЛІВ КВАЛІФІКАЦІЙНОЇ РОБОТИ..	89
ДОДАТОК Б. ПЕРЕЛІК ДОКУМЕНТІВ НА ОПТИЧНОМУ НОСІЇ .....	90
ДОДАТОК В. ВІДГУК КЕРІВНИКА ЕКОНОМІЧНОГО РОЗДІЛУ .....	91

## ВСТУП

В останні роки тенденція глобального поширення різноманітних відкритих телекомунікаційних систем і різке зростання числа абонентів призводять до необхідності захисту інформації не тільки на рівні державних органів, спеціальних служб або ділових кіл, а й на рівні практично кожного індивідуального користувача. І в інформаційних мережах дана проблема пов'язана не тільки з закриттям інформації (криптографія), а й з втратами інформації через низьку завадостійкість різних каналів зв'язку.

Використання фазоманіпульованих сигналів (ФМН) з різними типами фазової модуляції або маніпуляції є однією із характерних рис сучасних і перспективних радіотехнічних систем прихованої передачі інформації. Сучасний розвиток радіотехнічних систем передачі конфіденційної інформації нового покоління заснований на використанні не тільки ФМН, але й хаотичних процесів і послідовностей.

Таким чином, розробка і вдосконалення підходів до підвищення скритності та завадостійкості систем зв'язку з фазоманіпульованими сигналами наразі є актуальною задачею.

Метою даної кваліфікаційної роботи є підвищення завадостійкості системи зв'язку в умовах структурних завад при фіксованій базі фазоманіпульованого сигналу.

Постановка задачі:

- проаналізувати основи застосування шумоподібних сигналів в системах зв'язку;

- провести аналіз існуючих підходів до конфіденційної передачі інформації в системах зв'язку з фазоманіпульованими сигналами;
- запропонувати підхід до конфіденційної передачі інформації в системах зв'язку з підвищеною скритністю та завадостійкістю при фіксованій базі фазоманіпульованого сигналу;
- оцінити ефективність запропонованого підходу.

## РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

### 1.1 Основи застосування шумоподібних сигналів в системах зв'язку

1.1.1 Визначення шумоподібних сигналів і широкосмугових систем зв'язку

Шумоподібними сигналами (ШПС) називають такі сигнали, у яких добуток ширини спектра  $F$  на тривалість  $T$  багато більше одиниці. Цей добуток називається базою сигналу і позначається  $B$ ,

$$B = F * T \quad (1.1)$$

У ШПС  $B \gg 1$ . Шумоподібні сигнали іноді називають складними на відміну від простих сигналів з  $B = 1$ . Оскільки у сигналів з обмеженою тривалістю спектр має необмежену протяжність, то для визначення ширини спектра використовують різні методи і прийоми. Для реальних ШПС, що складаються з кінцевого числа елементів, завжди можна однозначно визначити  $F$  і  $B$ .

У системах зв'язку з ШПС ширина спектра завжди багато більше ширини спектра переданого повідомлення. У цифрових системах зв'язку, що передають інформацію у вигляді двійкових символів, тривалість ШПС і швидкість передачі інформації  $R$  пов'язані співвідношенням  $T = 1/R$ . Тому база ШПС

$$B = F/R \quad (1.2)$$

характеризує розширення спектра ШПС відносно спектра повідомлення. В аналогових системах зв'язку, у яких верхня частота повідомлення дорівнює  $W$  і частота відліку дорівнює  $2W$ ,

$$B = F/2W \quad (1.3)$$

І якщо  $B \gg 1$ , то  $F \gg R$  і  $F \gg 2W$ . Саме тому системи зв'язку з ШПС в зарубіжній літературі отримали назву системи зв'язку з розширеним (або розподіленим) спектром, а у вітчизняній літературі - широкосмугові системи зв'язку. Надалі термін «широкосмугові системи зв'язку» буде ставитися тільки до систем зв'язку з ШПС.

Шумоподібні сигнали отримали застосування в широкосмугових системах зв'язку, так як: забезпечують високу завадостійкість систем зв'язку; дозволяють організувати одночасну роботу багатьох абонентів в загальній смузі частот при асинхронно - адресному принципі роботи системи зв'язку, заснованому на кодовому поділі абонентів; дозволяють успішно боротися з багатопроменевим поширенням радіохвиль шляхом поділу променів; забезпечують сумісність передачі інформації з виміром параметрів руху об'єкта в системах рухомого зв'язку; забезпечують електромагнітну сумісність з вузькосмуговими системами радіозв'язку і радіомовлення, системами телевізійного мовлення, забезпечують краще використання спектра частот на обмеженій території в порівнянні з вузькосмуговими системами зв'язку.

### 1.1.2 Завадостійкість

Це здатність системи зв'язку протистояти впливу потужних завад. Завадостійкість включає в себе скритність системи зв'язку і її стійкість, так як

для створення потужних завад треба спочатку виявити систему зв'язку і виміряти основні параметри її сигналів, а потім організувати потужну, найбільш сильнодіючу заваду. Чим вище скритність і стійкість перед завадами, тим вище завадостійкість системи зв'язку.

### 1.1.3 Завадостійкість широкосмугових систем зв'язку

Вона визначається широко відомим співвідношенням, що зв'язує відношення сигнал-завада на виході приймача (на виході узгодженого фільтра або коррелятора)  $q^2$  з відношенням сигнал-завада на вході приймача  $\rho^2$ :

$$q^2 = 2 * \rho^2 * B \quad (1.4)$$

де  $\rho^2$  – відношення потужностей сигналу  $P_c$  і завади  $P_n$  на вході приймача  $\rho^2 = \frac{P_c}{P_n}$ ,  $q^2 = 2E/N_n$ ,  $E$  – енергія ШПС,  $N_n$  – спектральна щільність потужності завади в смузі ШПС. Відповідно  $E = P_c * T$ , а  $N_n = P_n/F$ ,  $B$  – база ШПС (1.2), (1.3). Відношення сигнал-завада на виході  $q^2$  визначає робочі характеристики прийому ШПС, а відношення сигнал-завада на вході  $\rho^2$  - енергетику сигналу і завади. Величина  $q^2$  може бути отримана відповідно до вимог до системи (10...30 дБ) навіть якщо  $\rho^2 \ll 1$ . Для цього достатньо вибрати ШПС з необхідною базою  $B$ , що задовольняє (1.4). Як видно зі співвідношення (1.4), прийом ШПС узгодженим фільтром або коррелятором супроводжується посиленням сигналу (або придушенням завади) в  $2B$  раз. Саме тому величину

$$K_{шпс} = q^2 / \rho^2 \quad (1.5)$$

називають коефіцієнтом посилення ШПС при обробці або просто посиленням обробки. З (1.4), (1.5) випливає, що посилення обробки  $K_{\text{шпс}} = 2B$ . В широкосмугових системах прийом інформації характеризується відношенням сигнал-завада  $h^2 = \frac{q^2}{2}$ , тобто

$$h^2 = B * \rho^2 \quad (1.6)$$

Співвідношення (1.4), (1.6) є фундаментальними в теорії систем зв'язку з ШПС. Вони отримані для завади у вигляді білого шуму з рівномірною спектральною щільністю потужності в межах смуги частот, ширина якої дорівнює ширині спектра ШПС. Разом з тим ці співвідношення справедливі для широкого кола завад (вузькосмугових, імпульсних, структурних), що і визначає їх фундаментальне значення. У загальному випадку, посилення обробки ШПС для довільних завад

$$K_{\text{шпс}} \approx 2 * B \quad (1.7)$$

де ступінь наближення залежить як від виду завад, так і від бази ШПС.

#### 1.1.4 Скритність системи зв'язку

Це здатність протистояти виявленню і вимірюванню параметрів. Скритність - поняття дуже ємне, так як включає в себе безліч особливостей виявлення ШПС і вимірювання їх параметрів. Оскільки виявлення ШПС і вимірювання параметрів можливі при різній початковій поінформованості (апріорній невизначеності) про систему зв'язку, то можна вказати тільки основні співвідношення, що характеризують скритність. Коли відомо, що в даному діапазоні частот може працювати система зв'язку, але параметри її невідомі, то в цьому випадку можна говорити про енергетичну скритності

системи зв'язку, так як її виявлення можливо за допомогою аналізу спектру (енергетичне виявлення). Характеристика виявлення (ймовірності помилкової тривоги і пропуску сигналу) повністю визначається відношенням сигнал-завада на вході приймача-аналізатора  $\rho^2 = \frac{P_c}{P_n}$ , де завада являє собою власний шум приймача  $P_n = k * T_0 * (N_{ш} - 1) * F$ , де  $k$  - постійна Больцмана,  $T_0$  - температура навколишнього середовища,  $N_{ш}$  - коефіцієнт шуму приймача. Час виявлення ШПС за умови  $\rho^2 \ll 1$  наближено визначається співвідношенням  $T_{обн} \approx F^{-1} * (\rho^2)^{-2} * 2q^4$  або

$$T_{обн} \approx a * F \quad (1.8)$$

де розмірна постійна  $a = 2 * [q^2 * k * T_0 * (N_{ш} - 1) / P_c]^2$  залежить як від шумових властивостей приймача, потужності сигналу на вході, так і від необхідного відношення сигнал-завада на виході  $q^2$ . Таким чином, чим ширше ширина спектра ШПС, тим більше час виявлення, тим вище енергетична скритність системи зв'язку.

Якщо ШПС системи зв'язку відтворюються приймачем-аналізатором впевнено, то час аналізу наближено визначається співвідношенням, аналогічним по виду співвідношенню (1.8), але  $a = b * T * [k * T_0 * (N_{ш} - 1) / P_c]$ ,  $b$  - постійна величина. Чим ширше спектр ШПС, тим більше база, тим більше час аналізу, тим вище параметрична скритність системи зв'язку.

Таким чином, чим ширше спектр ШПС і чим більше його база, тим вище як енергетична, так і параметрична скритність. Для боротьби з радіорозвідкою в завадозахищених системах зв'язку застосовують також зміну ШПС. Частота зміни ШПС, їх вибір з деякого ансамблю (системи сигналів) визначається багатьма вимогами до системи зв'язку і не може бути однозначно визначено. Однак вважають, що число сигналів в системі (або обсяг системи сигналів) має бути багато більше бази ШПС. Можна припустити, що для завадозахищених систем зв'язку обсяг системи сигналів  $L$  визначається степеневим законом:



$$L \sim B^m \quad (1.9)$$

де  $m$  – деяке число, що задовольняє умові  $m \geq 2$ , хоча для роботи може використовуватися набагато менше число ШПС.

Отже, використання ШПС підвищує стійкість і скритність системи зв'язку, тобто її завадостійкість. Як випливає з матеріалів зарубіжній пресі, ШПС використовують в супутникових системах зв'язку, в авіаційних системах зв'язку, в радіорелейних лініях, в супутникових навігаційних системах. Мабуть, застосування ШПС в завадозахищених системах зв'язку буде розширюватися.

### 1.1.5 Кодовий поділ абонентів

Завадозахищені системи зв'язку є спеціальними, а не комерційними. Тому на ранньому етапі розвитку систем зв'язку з ШПС вважали, що ШПС не знайдуть широкого застосування в комерційних системах зв'язку. Однак з розвитком асинхронних адресних систем зв'язку впровадження ШПС в системи масової радіозв'язку стало можливим. Основу для цього становить кодовий поділ абонентів за рахунок ШПС, що відрізняються за формою.

При великих базах можна побудувати велику кількість різних ШПС. Наприклад, нехай ШПС являє собою фазоманіпулірований сигнал, що складається з радіоімпульсів, фази яких  $0$  або  $\pi$ , а кількість їх дорівнює  $B$ . Можна побудувати безліч сигналів (так званий повний код), число сигналів в якому дорівнює  $2^B$  а сигнали між собою відрізняються хоча б в одному імпульсі. Якщо покласти  $B = 100$  то маємо  $2^{100} \sim 10^{30}$  різних сигналів. З такої великої множини можна відібрати систему сигналів так, щоб кожному абоненту в системі зв'язку виділити свої власні сигнали. При цьому всі абоненти можуть працювати в загальній смузі частот, а поділ їх можливий за рахунок різниці ШПС за формою. Такий поділ абонентів називається кодовим. При цьому ШПС є за своєю сутністю адресою абонента і в цьому випадку принципово немає

необхідності в примусовій тимчасовій синхронізації абонентів. Тому подібні системи зв'язку отримали назву асинхронних адресних систем зв'язку (ААСС). Вони засновані на застосуванні ШПС і кодовому поділі абонентів.

У ААСС всі абоненти працюють в загальній смузі частот. Тому при передачі інформації ШПС різних абонентів, перекриваються за часом і по частоті і створюють взаємні завади. Однак при використанні ШПС з великими базами можливо звести рівень взаємних завад до необхідного, щоб забезпечити необхідну якість прийому інформації. Якщо припустити, що на вході одного з приймачів, системи зв'язку діє 1 ШПС, що заважають з однаковими потужностями, то відношення сигнал-завада на виході приймача

$$h^2 = B/l. \quad (1.10)$$

Таким чином, збільшуючи базу ШПС, завжди можна домогтися необхідної якості прийому інформації. На рис. 1.3 представлені залежності бази ШПС від числа активних абонентів, побудовані відповідно до (1.10).

### 1.1.6 Ефективність ААСС

Як впливає з (1.10), підвищення завадостійкості ААСС при заданому числі активних абонентів можливо тільки за рахунок збільшення бази ШПС. При заданій швидкості передачі інформації збільшення бази призводить до пропорційного розширення спектра ШПС відповідно до визначення (1.2). Виникає питання про ефективність використання радіоспектра в системах зв'язку з ШПС. У системах зв'язку ефективність використання радіоспектра характеризується питомою щільністю активних абонентів  $\gamma$ , рівній числу активних абонентів, що припадають на 1МГц смуги частот, тобто

$$\gamma = l/F \quad (1.11)$$

де  $l$  - число активних абонентів, що одночасно працюють в смузі частот шириною  $F$ . Замінюючи  $l$ , в (1.11) згідно (1.10), маємо

$$\gamma = T/h^2. \quad (1.12)$$

Часто питома щільність активних абонентів називається просто ефективністю системи зв'язку. З (1.12) випливає, що ефективність ААСС тим менше, чим більше необхідне відношення сигнал-завада на виході приймача. Таким чином, ААСС більш перспективні в тих випадках, коли не потрібна висока якість передачі інформації, що характерно для систем масового радіозв'язку. Для прикладу, в радіотелефонного системі рухомого зв'язку з частотним поділом каналів максимальна ефективність  $\gamma_{max} = 250$  аб/МГц, так як мінімальна ширина кожного каналу дорівнює 4 кГц і в 1 МГц можна розмістити 250 частотних каналів, тобто, активних абонентів.

В останні роки запропонований інший принцип побудови радіотелефонних систем рухомого зв'язку. Вся територія, що обслуговується розбивається на велике число зон у вигляді сот. У кожній зоні радіозв'язок ведеться на частотах, спеціально виділених цій зоні. За рахунок територіального рознесення зон з однаковими частотними каналами можливо багаторазове використання одних і тих же частотних каналів. Такі системи зв'язку отримали назву стільникових систем рухомого зв'язку (ССПС). Прийом сигналів в таких системах принципово супроводжується взаємними завадами так само, як і в ААСС. Тому застосування ШПС в ССПС перспективно, оскільки дозволяє успішно боротися з взаємними завадами. Ефективність ССПС

$$\gamma_{ССПС} \approx 3,63 \left(\frac{R_0}{D}\right)^2 / F_k \quad (1.13)$$

де  $R_0$  - радіус зони обслуговування,  $D$  - захисний інтервал,  $F_k$  - ширина частотного каналу. Якщо покласти  $R_0 = 30$  км,  $D \approx 4,4$  км, радіус зони  $R = 0,85$  км, а  $F_k = 50$  кГц, то  $\gamma_{\text{ССПС}} \approx 3333$  аб/МГц, тобто набагато вище ефективності звичайних систем рухомого зв'язку. Якщо ширину частотного каналу збільшити до 100...200 кГц, то ефективність ССПС стане рівною 1666 і 833 аб/МГц відповідно, що все одно буде набагато більш ефективним. Але при цьому можливе застосування ШПС з відносно невеликими базами (25...250), що в свою чергу дозволить використовувати просту апаратуру формування та обробки ШПС з невисокою стабільністю частоти. У свою чергу застосування ШПС дозволить успішно вирішити проблему адресації великого числа абонентів. Стільникові системи рухомого зв'язку з ШПС дозволять забезпечити зв'язком 60...240 тисяч рухомих абонентів у великих містах. Крім того, в таких системах можна поєднати передачу телефонних повідомлень з визначенням місця розташування рухомих об'єктів і їх охорону.

### 1.1.7 Основні структурні схеми широкосмугових систем зв'язку

Широкасмугові системи зв'язку з ШПС в залежності від призначення, тактико-технічних характеристик, бази ШПС, елементної бази можуть бути побудовані за різними схемами, перерахувати які в даний час неможливо через численні варіантів. Для якісного представлення про те, з яких основних пристроїв складаються ШСС, використаємо рис. 1.1. На рис. 1.1 представлено структурні схеми передавача і приймача цифрової системи зв'язку з фазоманіпульованим (ФМН) сигналом, призначені для передачі дискретних

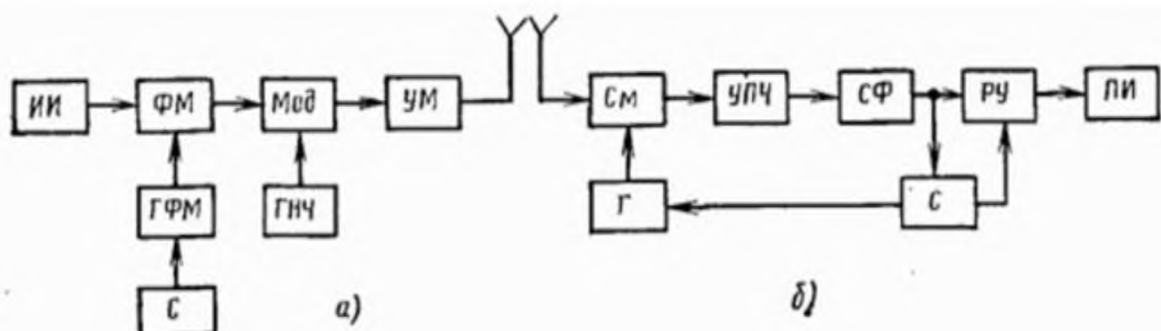


Рисунок 1.1 – Структурна схема передавача і приймача цифрової системи зв'язку із фазоманіпульованими ШПС

повідомлень.

У передавачі (рис. 1.1, а) від джерела інформації ІІІ послідовність двійкових одиниць 1 і 0 зі швидкістю  $R = 1/T$  (рис. 1.2, а) надходить на вхід фазового модулятора ФМ. На другий вхід ФМ надходить фазоманіпульований сигнал (рис. 1.2, б) від генератора ФМ сигналу ГФМ. Фазоманіпульований сигнал має тривалість  $T$  і являє собою послідовність відеоімпульсів 1 і 0 тривалістю  $\tau_0 = T/N$ , де  $N$  - число імпульсів. На рис. 1.2, б  $N = 13$ . Зазвичай вважають, що база ФМ сигналу приблизно дорівнює числу імпульсів ( $B \approx N$ ).

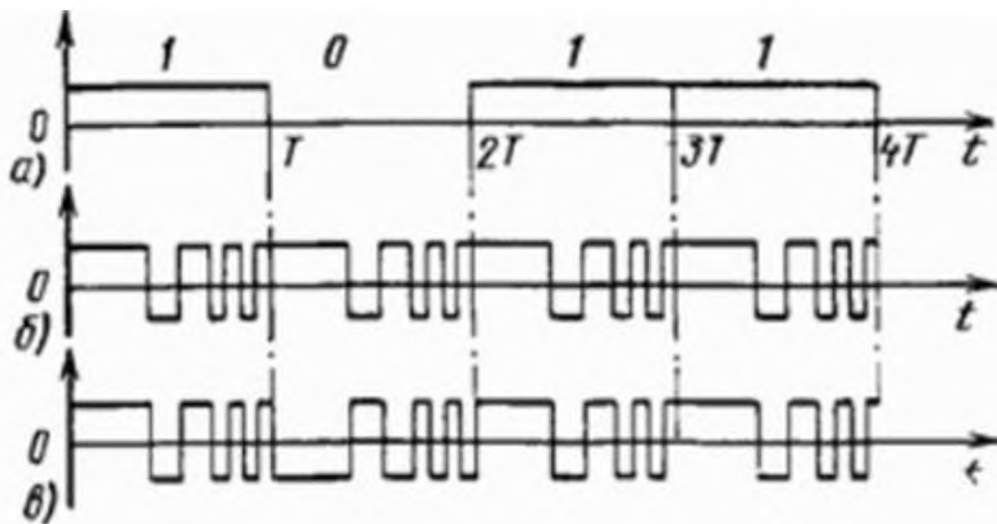


Рисунок 1.2 – Модуляція цифрової інформації ФМ ШПС

Ширина спектра ФМ сигналу  $F \approx 1/\tau_0$ . Роботою ГФМ управляє синхронізатор С, який формує необхідні сигнали управління і частоти. Послідовність ШПС у вигляді ФМ сигналів, що переносить інформаційні символи (рис. 1.2, в), надходить в модулятор Мод, в якому здійснюється балансна модуляція колювання з несучою частотою ФМ сигналом. Колювання з несучою частотою створюється генератором низької частоти ГНЧ. Підсилювач потужності УМ підсилює фазоманіпульований сигнал, а потім через антену сигнал випромінюється в простір. У приймальному (рис. 1.1, б) сигнал проходить через змішувач С<sub>м</sub>, переноситься за допомогою гетеродина Г на проміжну частоту, посилюється в підсилювачі проміжної частоти УПЧ і

обробляється узгодженим фільтром СФ. Сигнал з виходу СФ надходить на синхронізатор С і вирішальний пристрій РУ. Синхронізатор здійснює пошук ФМ сигналу по частоті за часом, накопичує сигнал для збільшення надійності синхронізації, управляє режимом роботи вирішального пристрою. Для пошуку ФМ сигналу по частоті синхронізатор перебудовує гетеродин. Після закінчення пошуку і входження в синхронізм на виході вирішального пристрою з'являється інформаційна послідовність у вигляді двійкових символів, яка передається одержувачу інформації ПИ. Приймач, зображений на рис. 1.1, б, є найбільш простим. Разом з тим необхідно відзначити, що узгоджений фільтр і синхронізатор, що містить блоки пошуку і синхронізації, є при великих базах ШПС складними пристроями. Крім того, для пошуку ШПС і підтримки синхронізму приймач охоплений петлею зворотного зв'язку. Реальний приймач ШПС може містити кілька блоків пошуку і спостереження, в тому числі блок пошуку ШПС за часом і тимчасової синхронізації, блок фазового автопідстроювання частоти ФАПЧ, які охоплені власними і взаємними зворотними зв'язками.

На рис. 1.3 представлені структурні схеми передавача і приймача радіотелефонного системи зв'язку з ФМ ШПС. В передавачі (рис. 1.3, а) телефонне повідомлення (рис. 1.4, а) від джерела інформації ИИ надходить на вхід широтно-імпульсного модулятора ШИМ, з виходу якого ШИМ сигнал подається на вхід фазового модулятора ФМ. На другий вхід ФМ подається ФМ ШПС (рис. 1.4, в), що формується ГФМ.

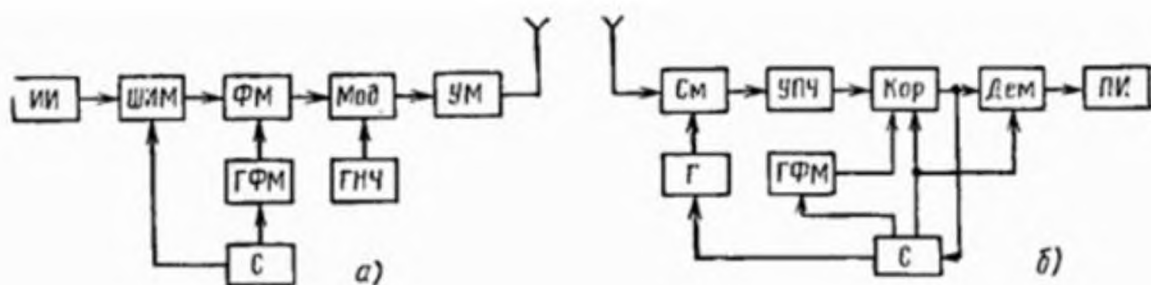


Рисунок 1.3 – Структурна схема передавача і приймача радіотелефонної системи зв'язку з фазоманіпульованими ШПС

Фазоманіпульований сигнал з виходу фазового модулятора (рис. 1.4, г), що містить інформацію, надходить на вхід модулятора М, в якому здійснюється балансна модуляція колювання з несучою частотою від ГНЧ. Потім посилений за потужністю в підсилювачі потужності УМ ФМ сигнал через антену випромінюється в простір.

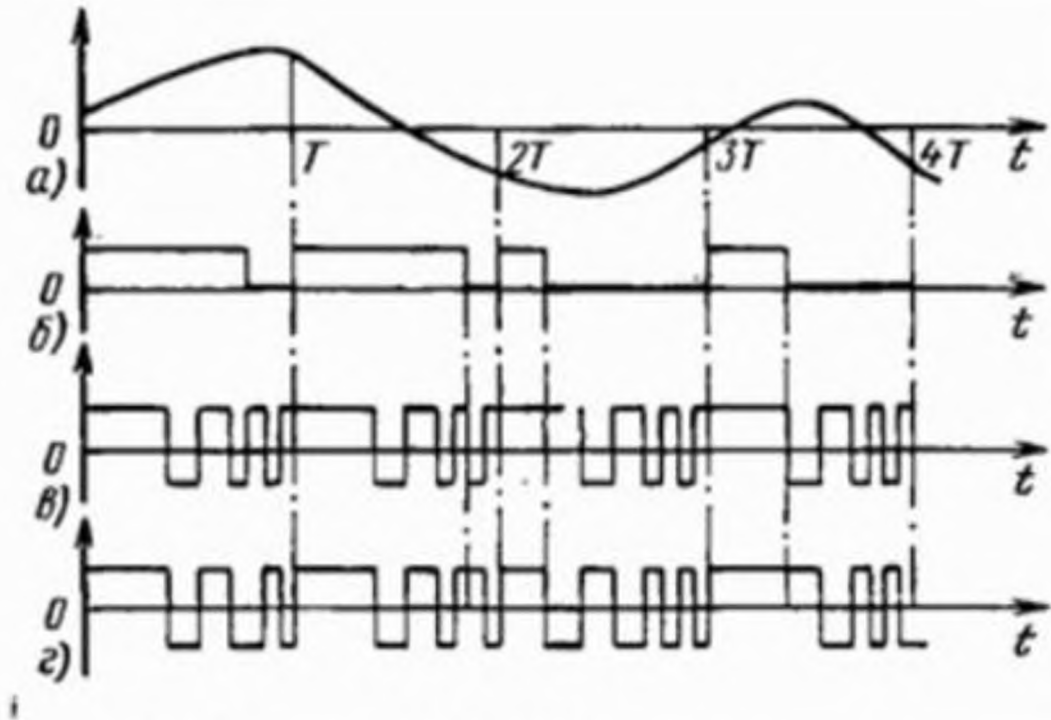


Рисунок 1.4 – Модуляція ФМ ШПС безперервним повідомленням за допомогою ШИМ

Роботою широтно-імпульсного модулятора і генератора ФМ сигналу керує синхронізатор С, який виробляє необхідні частоти і керуючі сигнали. У приймальному (рис. 1.3, б) прийнятий сигнал в змішувачі С за допомогою гетеродина Г переноситься на проміжну частоту і після УПЧ надходить на корелятор Кор. Корелятор, як і узгоджений фільтр, робить оптимальну обробку прийнятого сигналу. Хоча вони відрізняються за принципом роботи, але забезпечують однакову стійкість прийому. Корелятор складається з перемножувача і інтегратора. На другий вхід корелятора подається опорний сигнал у вигляді ФМ ШПС (рис. 1.4, в). Напряга на виході корелятора містить телефонне повідомлення у вигляді ШИМ сигналу, який подається на вхід демодулятора з виходу якого прийняте телефонне повідомлення передається

одержувачу інформації ПИ. Роботою приймача в цілому і його окремими блоками (Г, ГФМ, Кор, Дем) управляє синхронізатор С, який спочатку здійснює пошук ФМ ШПС за часом і частотою, а потім підтримує синхронізм.

На рис. 1.5 представлені структурні схеми передавача і приймача цифрової системи зв'язку з частотно-маніпульованим (ЧМ) ШПС (іноді такий ШПС називають сигналом з стрибаючою частотою).

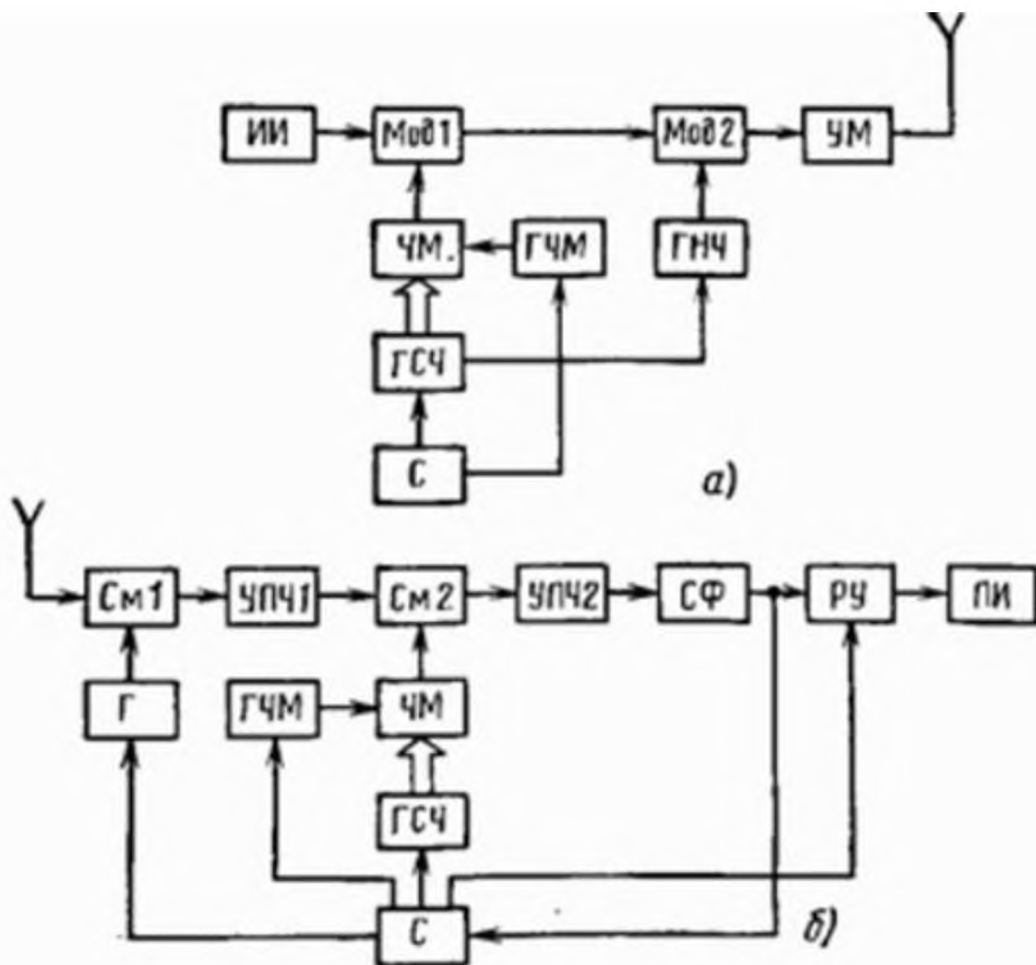


Рисунок 1.5 – Структурна схема передавача і приймача цифрової системи зв'язку з частотноманіпульованим ШПС

Відмінність передавача і приймача, зображених на рис. 1.5, від передавача і приймача на рис. 1.1 зводиться до наступного. У передавачі (рис. 1.5, а) в модуляторі Мод проводиться модуляція ЧМ ШПС дискретним повідомленням. ЧМ ШПС являє собою сигнал, що складається з  $M$  імпульсів, несучі частоти яких приймають одне з можливих значень від  $f_0$  до  $f_0 + \frac{M-1}{T}$  з



інтервалом між сусідніми значеннями  $\Delta f = \frac{1}{T}$ . Всього використовується  $M$  частот і жодна з них не застосовується двічі в одному ШПС. База такого сигналу  $B \approx M^2$ . ЧМ ШПС формується за допомогою частотного маніпулятора (ЧМ), у якого на один вхід через шину (широка стрілка) подаються  $M$  частот від генератора сітки частот ГСЧ. На інший вхід подається кодова послідовність від генератора кодової послідовності ЧМ ШПС (ГЧМ), яка визначає порядок зміни частот в ЧС ШПС. У модуляторі Мод2 проводиться перенесення ЧМ ШПС на несучу частоту. Роботою ГСЧ, ГЧМ, ГНЧ управляє синхронізатор С. В приймачі (рис. 1.5, б) ЧМ ШПС на проміжній частоті надходить на змішувач (См2) в якому проводиться перенесення всіх частот сигналу на другу проміжну частоту за допомогою опорного ЧМ ШПС, що надходить від частотного маніпулятора ЧМ. Призначення ГСЧ і ГЧМ таке ж, як і в передавачі (рис. 1.5, а). З виходу УПЧ2 сигнал тривалістю  $T$ , який не має частотної маніпуляції, надходить на СФ, а потім на РУ і С. Останній здійснює пошук ЧМ ШПС за часом і частотою, потім підтримує синхронізм і управляє роботою Г, ГСЧ, ГЧМ і РУ.

На рис. 1.6 представлені структурні схеми передавача і приймача цифрової системи зв'язку з фазо-частотноманіпульованим (ФМ-ЧМ) ШПС. Такий сигнал є складеним.

При зазначеній подвійній маніпуляції він складається з  $N$  імпульсів, групи яких передаються на  $M$  частотах. База такого ШПС дорівнює, приблизно  $B \approx N * M^2$ . Оскільки ФМ-ЧМ ШПС є об'єднанням ФМ і ЧМ сигналів, то і схема передавача (рис. 1.6, а), і схема приймача (рис. 1.6, б) є в свою чергу об'єднанням передавачів (рис. 1.1, а і 1.5, а) і приймачів (рис. 1.1, б і 1.5, б). Для додаткового підвищення завадостійкості використовуються коригувальні коди, які формуються в передавачі (рис. 1.6, а) за допомогою кодера (К) і декодуються в приймачі (рис. 1.6, б) за допомогою декодера (Д). У приймачі оптимальну фільтрацію здійснює коррелятор (Кор). Призначення інших блоків таке ж, як і в попередніх схемах.

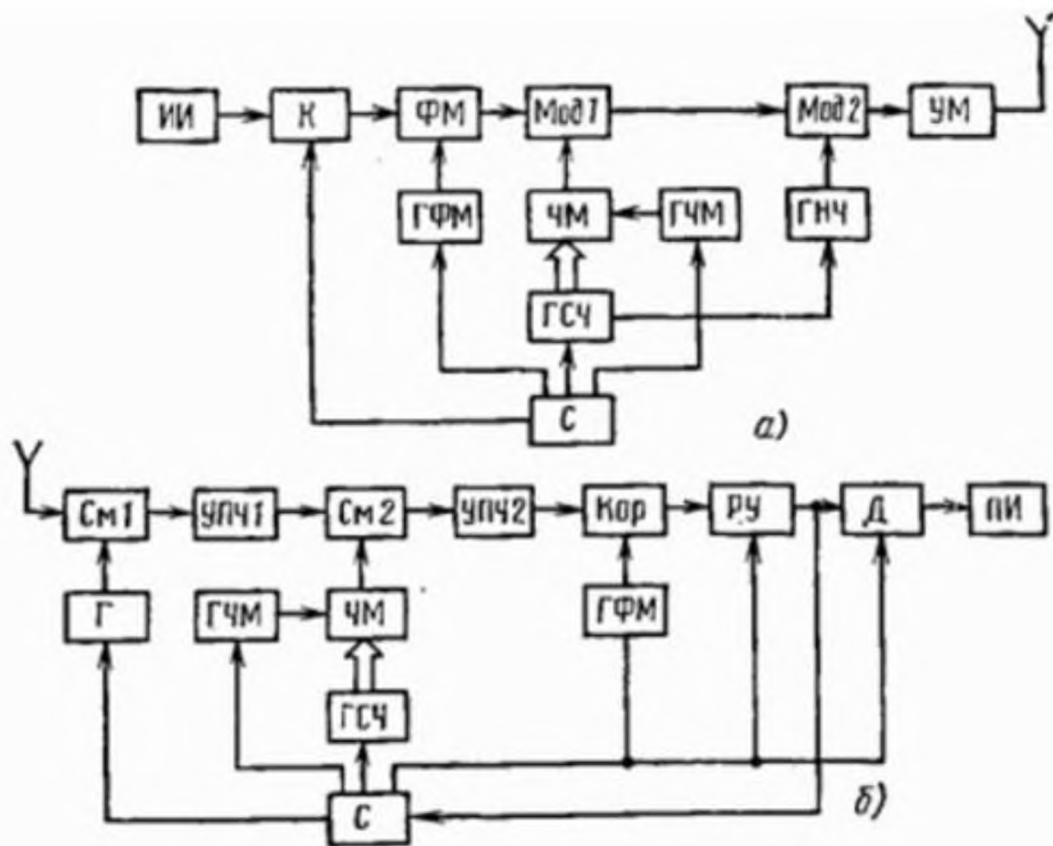


Рисунок 1.6 – Структурна схема передавача і приймача цифрової системи зв'язку із фазо-частотноманіпульованими ШПС і корекційними кодами

Представлені схеми не вичерпують усього різноманіття схем широкопasmових систем зв'язку з ШПС. Разом з тим вони дозволяють виділити основні вузли таких систем. До таких вузлів відносяться генератори формування ШПС (або автомати формування ШПС з їх зміною), генератори сітки частот, узгоджені фільтри, корелятори, блоки пошуку ШПС і синхронізації за часом і частотою. З представленого матеріалу випливає, що розробник широкопasmової системи зв'язку повинен вміти вибрати тип ШПС і його базу, метод обробки, визначити час пошуку і синхронізації, знайти стійкість приймача ШПС при дії різного роду завад, вибрати елементну базу і розробити на ній необхідні генератори ШПС, узгоджені фільтри і корелятори, блоки пошуку і синхронізації. Крім цього, розробник повинен вміти

проекувати інші вузли передавача і приймача, знати, як проходить ШПС через вузли передавача і приймача і які втрати при цьому мають місце. На всі питання, які виникають в процесі проектування широкосмугових систем зв'язку, не можна в більшості випадків дати однозначні відповіді. Тому проектування широкосмугових систем зв'язку в даний час є інженерним мистецтвом, яке ґрунтується на глибокому знанні теорії та техніки ШПС і на інтуїції розробника. Але тим не менш, з усіх питань проектування систем зв'язку з ШПС в даний час є основні (і в багатьох випадках фундаментальні) результати.

## 1.2 Шумоподібні сигнали

Сигналом називається фізична величина, що змінюється, і яка відображає повідомлення. Сигнал  $u$ , що є функцією часу  $t$  записується у вигляді  $u = u(t)$ .

### 1.2.1 Сигнали і спектри

Множина сигналів  $u_j(t)$  визначається єдиним правилом побудови, що називається системою сигналів. Таким чином, система сигналів визначена, якщо відомо правило побудови сигналів. Номер сигналу зазначений у вигляді індексу  $j$ . Якщо число сигналів в системі  $L$ , то, можна пронумерувати сигнали натуральними числами від 1 до  $L$  і позначити  $j = \overline{1, L}$ . Число  $L$  називається об'ємом системи сигналів.

Надалі розглядаються сигнали, які можна представити в наступному вигляді:

$$u(t) = A(t) \cos[\omega_0 t + \theta(t)] \quad (1.14)$$

де  $A(t)$  – огибаюча,  $\omega_0$  - несуча частота,  $\theta(t)$  - частина фази сигналу, що повільно змінюється. Поданню (1.14) відповідає радіочастотний сигнал. Так як розглядаються реальні сигнали (які можна сформувати і обробити), то всі функції часу і параметри правої частини (1.14) відомі.

Коли сигнал заданий в загальному вигляді  $u(t)$  і права частина (1.14) не відома, то необхідно скористатися перетворенням Гільберта і знайти пов'язаний сигнал  $\hat{u}(t)$ . В цьому випадку огибаюча  $A(t) = \sqrt{u^2(t) + \hat{u}^2(t)}$ , фаза  $\Theta(t) = \omega_0 t + \theta(t) = \arctg[\hat{u}(t)/u(t)]$ .

Якщо функція  $\theta(t)$  неперервна і має неперервну першу похідну, то миттєва частота сигналу  $\omega(t)$  по визначенню дорівнює першій похідній фази  $\theta(t)$ , тобто  $\omega(t) = \omega_0 + \theta'(t)$ .

$$\text{Перетворення Гільберта: } u(t) = \frac{1}{\pi} \int_{-\infty}^{\infty} \frac{\hat{u}(x)}{x-t} dx, \hat{u}(t) = -\frac{1}{\pi} \int_{-\infty}^{\infty} \frac{u(x)}{x-t} dx.$$

На рис. 1.7, а показаний фазоманіпульований сигнал (ФМН), що складається з чотирьох радіоімпульсів з однаковою частотою, але з різними початковими фазами. На рис. 1.7, б, в представлені його огибаюча  $A(t)$  і фаза  $\theta(t)$ . Огибаюча постійна на інтервалі тривалістю  $T$ , а фаза дорівнює двом значенням: 0 або  $\pi$ .

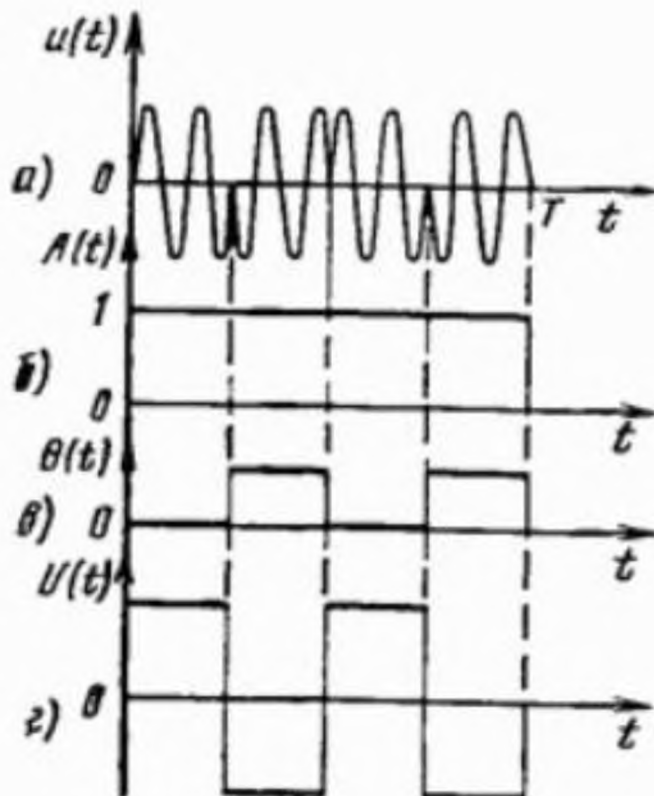


Рисунок 1.7 – Фазоманіпульований сигнал

Якщо несуча частота сигналу  $\omega_0 = 0$ , то такий сигнал є відеочастотним. На рис. 1.7, г зображений відеочастотний сигнал  $U(t)$  - послідовність позитивних і негативних прямокутних імпульсів, отриманих з ФМ сигналу рис. 1.7, а за умови, що  $\omega_0 = 0$ . Так як знаки імпульсів відеочастотного сигналу визначаються початковими фазами імпульсів радіочастотного сигналу, то за аналогією з радіочастотним сигналом відеочастотний також називається фазоманіпульованим сигналом.

Спектр сигналу визначається перетворенням Фур'є:

$$g(\omega) = \int_{-\infty}^{\infty} u(t)e^{-i\omega t} dt. \quad (1.15)$$

Спектр є функцією кутової частоти  $\omega = 2\pi f$ , де  $f$  - лінійна частота. (Надалі  $\omega$  і  $f$  називаються просто частотою.) Нескінченні межі інтегрування відповідають загальному випадку. При визначенні спектра фінітного сигналу (з кінцевою тривалістю) необхідно враховувати його розташування на осі часу  $t$ . Спектр може бути представлений у вигляді  $g(\omega) = |g(\omega)| \exp[i\varphi(\omega)]$ , де  $|g(\omega)|$  - амплітудний, а  $\varphi(\omega)$  - фазовий спектр сигналу  $u(t)$ .

Сигнал знаходиться по спектру за допомогою зворотного перетворення Фур'є:  $u(t) = \frac{1}{2\pi} \int_{-\infty}^{\infty} g(\omega) e^{-i\omega t} d\omega$ .

### 1.2.2. Основи оптимальної обробки сигналів

Якщо на вході приймача діє сигнал  $x(t)$ , рівний сумі корисного сигналу  $u(t)$  і завади  $n(t)$  або тільки заваді, то оптимальний приймач в разі сигналу з повністю відомими параметрами обчислює так званий кореляційний інтеграл, а потім порівнює його величину з порогом  $z_0$ . Якщо завада є гауссовим

випадковим процесом, спектральна щільність якого рівномірна (білий шум), то кореляційний інтеграл має вигляд

$$z = \int_0^T x(t)u(t)dt \quad (1.16)$$

Значення кореляційного інтеграла (1.16) знаходиться за допомогою коррелятора (рис. 1.8) або узгодженого фільтра (рис. 1.9). Основними елементами коррелятора, як випливає з виразу (1.16), є перемножувач, генератор сигналу і інтегратор. На перемножувач надходять вхідний сигнал  $x(t)$  і сигнал  $u(t)$  від генератора сигналу. Добуток  $x(t)$  і  $u(t)$  інтегрується з моменту приходу ( $t=0$ ) і до моменту закінчення виявленого сигналу ( $t=T$ ). Відзначимо, що коррелятор є пристроєм зі змінними параметрами, так як режим його залежить від зміни  $u(t)$  в часі.

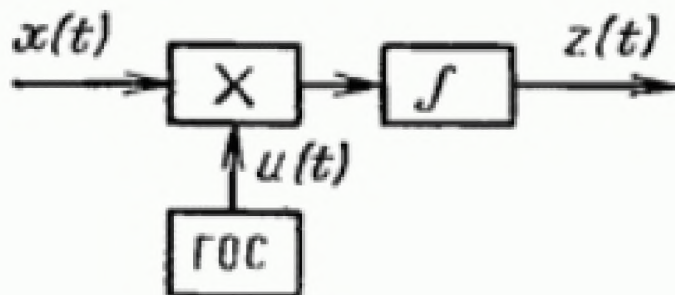


Рисунок 1.8 - Коррелятор

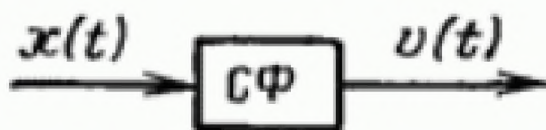


Рисунок 1.9 – Узгоджений фільтр

Оскільки операції множення і інтегрування лінійні, то коррелятор є лінійним пристроєм. Маючи на увазі, що він відфільтровує сигнал від завад і є лінійним пристроєм зі змінними параметрами, його іноді називають активним фільтром на відміну від пасивних фільтрів, параметри яких постійні в часі.

Узгоджений фільтр є пасивним фільтром. Напряга на виході узгодженого фільтра в момент закінчення сигналу ( $t=T$ ) з точністю до постійного множника  $a$  дорівнює напрузі на виході коррелятора

$$U(t) = az \quad (1.17)$$

Імпульсна характеристика узгодженого фільтра

$$h(t) = au(T - t) \quad (1.18)$$

яка за формою є дзеркально відображеним сигналом з запізненням  $T$ .

Спільним між коррелятором і узгодженим фільтром є рівність (з точністю до постійної) вихідних напруг в момент часу  $t=T$ . Це і визначає їх взаємну еквівалентність з точки зору виявлення сигналу. Різниця полягає в наступному. Коррелятор є пристроєм зі змінними в часі параметрами, а узгоджений Фільтр - пристроєм з постійними параметрами. Наслідком цього є те, що узгоджений фільтр інваріантний щодо затримки сигналу і його початкової фази (наскільки ці величини зміняться в сигналі на вході фільтра, настільки вони зміняться і в сигналі на виході), а коррелятор НЕ інваріантний.

Якщо сигнал має кілька не вимірюваних або вимірюваних випадкових параметрів, то структура оптимального приймача змінюється, але його основна частина залишається незмінною, так як завжди повинен бути узгоджений фільтр або коррелятор. Наприклад, при випадкової початковій фазі сигналу в

приймачі з узгодженим фільтром за фільтром повинен слідувати детектор для виділення огибаючої. У приймальнику кореляційного типу повинні бути другий (квадратурний) канал і схема виділення огибаючої. Тому в оптимальному приймачі завжди є узгоджений фільтр або корелятор.

### 1.2.3. Кореляційні функції сигналів

Оптимальний прийом сигналів здійснюється за допомогою узгоджених фільтрів або кореляторів. Нормований відгук узгодженого фільтра, що визначаються за допомогою інтеграла згортки,

$$r_{jk}(\tau) = \frac{1}{E} \int_{-\infty}^{\infty} u_j(t) u_k(t - \tau) dt \quad (1.19)$$

де  $u_j(t)$  - сигнал на вході фільтра, узгодженого з сигналом  $u_k(t)$ . Енергії сигналів з номерами  $j$  і  $k$  рівні  $E$ , а  $\tau$  - зрушення сигналу  $u_j(t)$  відносно відгуку  $u_k(t)$ . При  $j = k$  і  $\tau = 0$  з (1.19), відкидаючи індекси, маємо

$$r(0) = r_{max} = \frac{1}{E} \int_{-\infty}^{\infty} u^2(t) dt = 1 \quad (1.20)$$

що і визначає нормованість відгуку узгодженого фільтра.

Вираз у правій частині (1.19) визначає інтегральний взаємозв'язок між сигналами  $u_j(t)$  і  $u_k(t)$  при деякому зсуві  $\tau$ . Якщо  $\tau$  - змінна величина, то  $r_{jk}(\tau)$  - функціонал, що залежить як від функцій  $u_j(t)$  і  $u_k(t)$  так і від зсуву  $\tau$ . Саме тому  $r_{jk}(\tau)$  називається кореляційною функцією сигналів  $u_j(t)$  і  $u_k(t)$ . Залежно від того, узгоджений або не узгоджений сигнал з фільтром, чи є додаткове доплерівське зміщення несучої частоти сигналу, кореляційні функції по-різному трактують.



Взаємна функція невизначеності (ВФН) двох сигналів з номерами  $j$  і  $k$ , за визначенням, виражається через комплексні огинаючі сигналів і через їх спектри наступним чином:

$$R_{jk}(\tau, \Omega) = \frac{1}{2E} \int_{-\infty}^{\infty} U_j(t) U_k(t - \tau) e^{i\Omega t} dt = \frac{1}{4\pi E} \int_{-\infty}^{\infty} G_j(\omega - \Omega) G_k(\omega) e^{i\omega \tau} d\omega \quad (1.21)$$

де  $\tau$  - зсув по часу між сигналами,  $\Omega$  - доплерівське зрушення частоти. З точністю до малих вищого порядку нормований відгук узгодженого фільтра пов'язаний із ВФН (1.21) співвідношенням

$$r_{jk}(\tau, \Omega) = \operatorname{Re} R_{jk}(\tau, \Omega) \exp(i\omega_0 \tau) \quad (1.22)$$

Взаємнокореляційна функція (ВКФ) є перетином ВФН при  $\Omega = 0$ . Вважаючи  $\Omega = 0$ , з (1.21) отримуємо

$$R_{jk}(\tau) = \frac{1}{2E} \int_{-\infty}^{\infty} U_j(t) U_k(t - \tau) dt = \frac{1}{4\pi E} \int_{-\infty}^{\infty} G_j(\omega) G_k(\omega) e^{i\omega \tau} d\omega \quad (1.23)$$

Функція невизначеності (ФН). Якщо фільтр узгоджений з сигналом, тобто  $j=k$ , то із (1.21), опускаючи індекс  $j$  отримуємо визначення ФН

$$R(\tau, \Omega) = \frac{1}{2E} \int_{-\infty}^{\infty} U(t) U(t - \tau) e^{i\Omega t} dt = \frac{1}{4\pi E} \int_{-\infty}^{\infty} G(\omega - \Omega) G(\omega) e^{i\omega \tau} d\omega \quad (1.24)$$

Автокореляційна функція (АКФ) - перетин ФН при  $\Omega = 0$ . Вважаючи  $\Omega = 0$ , з (1.24) знаходимо

$$R(\tau) = \frac{1}{2E} \int_{-\infty}^{\infty} U(t) U(t - \tau) dt = \frac{1}{4\pi E} \int_{-\infty}^{\infty} |G(\omega)|^2 e^{i\omega \tau} d\omega \quad (1.25)$$

З рівності (1.25) видно, що АКФ є перетворенням Фур'є енергетичного спектра комплексної огинаючої сигналу. Згідно зворотньому перетворенню Фур'є енергетичний спектр

$$|G(\omega)|^2 = 2E \int_{-\infty}^{\infty} R(\tau) e^{-i\omega\tau} d\tau \quad (1.26)$$

#### 1.2.4. Фазоманіпульовані сигнали, як один з основних типів ШПС

Відома велика кількість різних ШПС. Загальноприйнятою термінології поки не існує. Проте, розглянемо деякий тип ШПС.

Фазоманіпульовані (ФМ) сигнали представляють послідовність радіоімпульсів, фази яких змінюються по заданому закону. Зазвичай фаза приймає два значення (0 або  $\pi$ ). При цьому радіочастотному ФМ сигналу відповідає відео- ФМ сигнал (рис. 1.10, а), що складається з позитивних і негативних імпульсів. Якщо число імпульсів  $N$  то тривалість одного імпульсу дорівнює  $\tau_0 = T/N$ , а ширина його спектру дорівнює приблизно ширині спектру сигналу  $F_0 = \frac{1}{\tau_0} = N/T$ . На частотно-часовій площині (рис. 1.10, б) штрихуванням виділено розподіл енергії одного елемента (імпульсу) ФМ сигналу. Всі елементи перекривають виділений квадрат зі сторонами  $F$  і  $T$ . База ФМ сигналу

$$B = FT = \frac{t}{\tau_0} = N \quad (1.27)$$

Тобто дорівнює кількості імпульсів у сигналі.

Можливість застосування ФМ сигналів в якості ШПС з базами  $B = 10^4 \dots 10^6$  обмежена в основному апаратурою обробки. При використанні узгоджених фільтрів у вигляді приладів з поверхневими акустичними хвилями (ПАВ) можливий оптимальний прийом ФМ сигналів з максимальними базами  $B_{max} = 1000 \dots 2000$ .

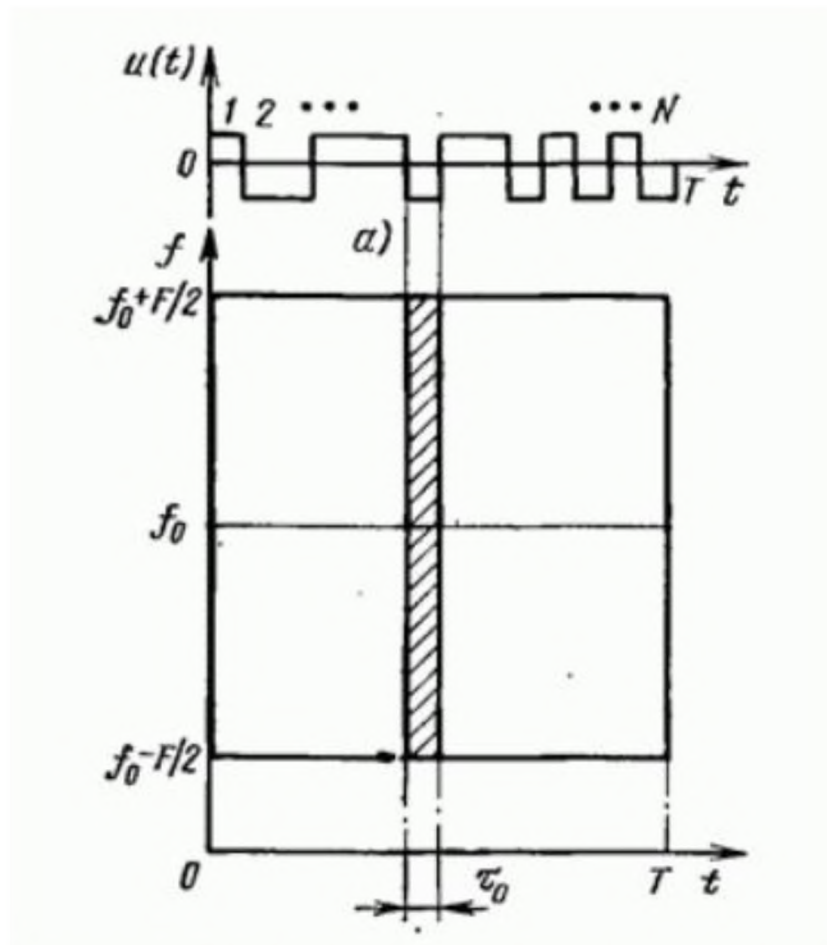


Рисунок 1.10 – фазоманіпульований сигнал (сигнал з кодовою фазовою модуляцією) і частотно-часова площа

ФМ сигнали, оброблювані такими фільтрами, мають широкі спектри (порядку 10...20 МГц) і відносно короткі тривалості (50...100 мкс). Обробка ФМ сигналів за допомогою відеочастотних ліній затримки при перенесенні спектру сигналів в область відеочастот дозволяє отримувати бази  $B = 100$  при  $F \approx 1$  МГц,  $T \approx 100$  мкс.

Вельми перспективними є узгоджені фільтри на приладах із зарядним зв'язком. Згідно з опублікованими даними за допомогою узгоджених фільтрів на приладах із зарядним зв'язком можна обробляти ФМ сигнали з базами  $10^2 \dots 10^3$  при тривалості сигналів  $10^{-4} \dots 10^{-1}$  с. Цифровий корелятор на приладах із зарядним зв'язком здатний обробляти сигнали до бази  $4 * 10^4$ .

Слід зазначити, що ФМ сигнали з великими базами доцільно обробляти за допомогою корреляторів. При цьому  $B = 4 * 10^4$  представляється граничною. Але при використанні корреляторів необхідно в першу чергу вирішити питання про прискорене входження в синхронізм.

Так як ФМ сигнали дозволяють широко використовувати цифрові методи і техніку формування і обробки і можна реалізувати такі сигнали з відносно великими базами, то тому ФМ сигнали є одним з перспективних видів ШПС.

### 1.3 Існуючі підходи до конфіденційної передачі інформації в системах зв'язку з фазоманіпульованими сигналами

Сьогодні відомі різні системи передачі конфіденційної інформації. Типова з них (аналог) є асинхронна адресна система зі складними фазоманіпульованими сигналами [1]. До недоліків відомої схеми слід віднести незадовільну скритність і стійкість в умовах структурних завад при обмеженій базі сигналу. З відомих систем передачі інформації найбільш близькою по технічній сутності і досягнутому результату до заявленого (підходу) є цифрова система зв'язку з ФМН сигналом [2]. Відома система випромінює в складі послідовно включених джерела інформації, першого фазового модулятора, першого модулятора, підсилювача потужності і передавальної антени, синхронізатора передавача, пов'язаного виходом з другим входом першого фазового модулятора через генератор фазоманіпульованого сигналу, генератора несучої частоти, пов'язаного виходом з другим входом першого модулятора, приймач в складі послідовно включених прийомної антени, змішувача, підсилювача проміжної частоти, узгодженого фільтра, вирішального пристрою і одержувача інформації, синхронізатора приймача, пов'язаного входом з виходом узгодженого фільтра, одним виходом з другим входом змішувача через гетеродин, а іншим виходом з першим входом вирішального пристрою. У передавачі відомої системи послідовність двійкових одиниць «1» і «0» від джерела інформації перетворюється в послідовність ФМН сигналів,

випромінюваних передавальною антеною в простір на несучій частоті. У приймачі прийнята приймальною антеною послідовність ФМН сигналів після перетворення, посилення, узгодженої фільтрації на виході вирішального пристрою перетворюється в інформаційну послідовність і надходить до одержувача інформації.

Недоліками відомої системи є відносно низькі скритність і завадостійкість, особливо, в умовах структурних завад при обмеженій базі сигналу. До структурних завад відносять завади, що мають ту ж структуру, що і корисний сигнал. Це внутрішньо-системні, ретрансляційні, імітаційні та інші завади. Перший недолік обумовлений тим, що недостатня, перш за все, така складова скритності, як структурна скритність. Дійсно, структура ФМН сигналу, що представляє біт інформації визначається використанням видом шумоподібного сигналу (ШПС). Класи ШПС і правила їх утворення відомі, наприклад, для широко використовуваних М-послідовностей. Для сучасних засобів радіорозвідки розпізнавання класу використовуваного ШПС можливо протягом прийому декількох біт інформації. Для боротьби з радіорозвідкою застосовують зміну ШПС, проте число використовуваних ШПС обмежена. Крім того, розпізнавання структури сигналу при відсутності маскуванню цієї структури не залежить від застосовуваного класу ШПС і реалізується сучасна форма радіорозвідки при перевищенні сигналу над шумом, що практично завжди має місце. Недостатня так само і друга складова скритності – інформаційна скритність.

Наприклад, для систем передачі інформації стійкість до розкриття змісту повідомлення визначається стійкістю шифру, яким кодують інформаційну послідовність. При цьому можливість створення стійкого шифру пов'язана з довжиною ключової послідовності. Спільною рисою прихованих сигналів і загальним показником скритності служить база сигналу  $B$ . З двох сигналів потенційно кращою скритністю володіє той, у якого більше  $B$  (для ФМН сигналів база дорівнює числу елементів сигналу  $M$  або його довжині). Однак, база сигналу завжди обмежена. Найчастіше це обмеження пов'язане зі

швидкістю передачі інформації. Крім того, при будь-якій базі процес дешифрування починається з виявлення засобом розвідки факту передачі «1» або «0» або переходу з «1» на «0» і навпаки. Саме цей факт певною системою легко виявляється, так як для передачі «1» використовується на передавальній стороні один і той же ФМН сигнал, а для передачі «0» протилежний (по фазі) йому.

Щодо другого недоліку слід зазначити, що стійкість прийому дискретної інформації в відомій системі визначається співвідношенням:

$$q_n^2 = 2 * \rho^2 * B, \quad (1.28)$$

де  $q_n^2$  – відношення сигнал/завада на вході вирішального пристрою;  $B$  - база сигналу;  $\rho^2$  – відношення потужностей сигналу  $P_c$  і завади  $P_n$  на вході приймача  $\rho^2 = \frac{P_c}{P_n}$ .

Співвідношення (1.28) є основним в техніці боротьби з потужними ( $\rho^2 \ll 1$ ) завадами. Якщо  $q_n^2 > 1$ , то надійна передача інформації можлива при  $\rho^2 \ll 1$ .

Оцінимо порогове значення відношення сигнал/завада на вході вирішального пристрою. Для цього скористаємося теоремою Шеннона про пропускну здатність  $C$  каналу передачі інформації, відповідно до якої

$$C = F \log_2(1 + \rho^2), \quad (1.29)$$

де  $F$  - ширина спектру сигналу, що дорівнює ширині смуги пропускання каналу. Перетворимо (1.29) до вигляду:

$$\frac{C \ln 2}{F} = \ln(1 + \rho^2). \quad (1.30)$$

Враховуючи, що  $\rho^2 \ll 1$ , розкладемо праву частину (1.30) в степеневий ряд, обмежившись першим членом ряду, одержимо:

$$C \approx \frac{\rho^2 * F}{\ln 2}. \quad (1.31)$$

Оскільки база сигналу  $V=F*T$ , де  $T$  – тривалість біта, а  $C = \frac{1}{T}$  – пропускна здатність каналу, вираз (1.28) набуває вигляду:

$$q_n^2 = \frac{2 * \rho^2 * F}{C} \quad (1.32)$$

Підставивши (1.31) в (1.32) отримаємо граничне значення відношення потужностей сигналу і завади на вході вирішального пристрою:

$$q_{n \text{ пор}}^2 \approx 2 \ln 2 \approx 1,4. \quad (1.33)$$

Якщо  $q_n^2 > q_{n \text{ пор}}^2$ , то помилка за рахунок дії завади буде невелика. Якщо ж  $q_n^2 \leq q_{n \text{ пор}}^2$ , то відповідно до теореми Шеннона помилка різко зростає.

Це особливо характерно для структурних завад, для яких найчастіше має місце їх повний збіг або навіть перекриття з корисним сигналом по ширині спектра, а також істотний збіг по структурі, оскільки структурна скритність, наприклад, ФМН сигналу відносно невелика і часто має місце виконання нерівності  $q_n^2 > q_{n \text{ пор}}^2$ .

Для боротьби зі структурними завадами широке застосування знайшла так звана схема ШОУ (широкосмуговий підсилювач - обмежувач - узгоджений фільтр), яка може використовуватися в приймальному відомої системи. В цьому випадку корисний сигнал і структурна завада виявляються однаковими за амплітудою на вході узгодженого фільтра, і вплив завади повністю визначається її взаємкореляційними властивостями з корисним сигналом.

Виходячи з фізичного змісту можна записати, що максимальна потужність корисного сигналу на виході узгодженого фільтра пропорційна

добутку потужності сигналу на вході приймача  $P_{c\text{ вх}}$  і коефіцієнта автокореляції сигналу  $K_{cc}$ , тобто  $P_{c\text{ вих}} \equiv P_{c\text{ вх}} * K_{cc}$ . Але аналогічна залежність справедлива і для структурної завади  $P_{n\text{ вих}} \equiv P_{n\text{ вх}} * K_{cn}$ , де  $K_{cn}$  - коефіцієнт взаємної кореляції сигналу та завади. Тоді для відношення потужностей можна записати:

$$\frac{P_{c\text{ вих}}}{P_{n\text{ вих}}} = \frac{P_{c\text{ вх}} * K_{cc}}{P_{n\text{ вх}} * K_{cn}} \quad \text{або} \quad q_n^2 = \rho^2 \frac{K_{cc}}{K_{cn}}.$$

Враховуючи, що  $K_{cc} \approx 1$ , вираз набуває вигляду:

$$q_n^2 = \frac{\rho^2}{K_{cn}}. \quad (1.34)$$

Отриманий вираз є важливим для оцінки завадостійкості системи з ШОУ в умовах структурних завад. У порівнянні з (1.27) він інваріантний до бази сигналу і з урахуванням (1.24) дозволяє для кожного фіксованого відношення сигнал/завада на вході  $\rho^2$  визначити граничне значення коефіцієнта взаємної кореляції структурної завади, починаючи з якого система виявляється повністю пригніченою.

Це ілюструється залежностями виду (1.32), наведеними на рис. 1.11, для різних значень вхідних відношень сигнал/завада  $\rho^2 \leq 1$ .

Для відомої системи, в разі побудови її приймача за схемою ШОУ, крива для  $\rho^2 = 1$  характеризує її завадостійкість в умовах дії структурних завад. Умова  $q_n^2 \leq q_n^2_{\text{пор}}$ , при якій відома система виявляється повністю пригніченою настає при  $K_{cn} = 0,7$  (рис. 1.11).

Разом із тим аналіз і моделювання відомої системи показує, що вже при  $K_{cn} \geq 0,5$  відбувається суттєва, часто неприйнятна, втрата працездатності системи в умовах структурних завад навіть для схеми ШОУ.



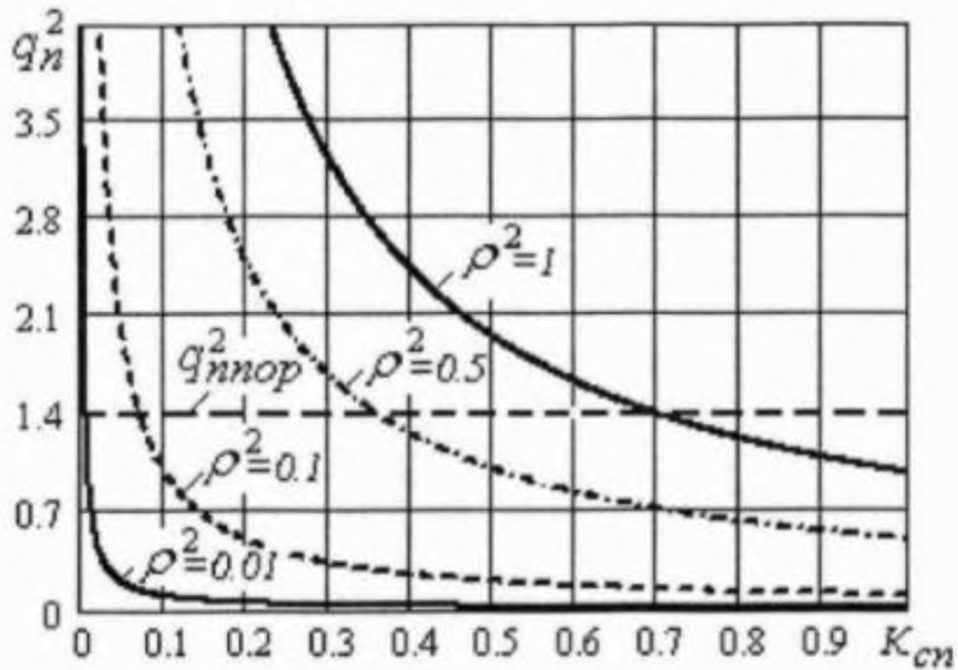


Рисунок 1.11 – Оцінка завадостійкості системи з ШОУ

#### 1.4 Висновок. Постановка задачі

Таким чином, завдання полягає в підвищенні структурної та інформаційної складових скритності, і так само як і для скритності, актуально підвищення завадостійкості відомої системи в умовах структурних завад при фіксованій базі ФМН сигналу.

Результат, на досягнення якого спрямований запропонований підхід, полягає в ускладненні і маскуванні структури сигналу, формованого на передавальній стороні, а так само в забезпеченні розпізнавання цієї структури і поліпшення компенсації структурних завад на приймальній стороні.

## РОЗДІЛ 2. СПЕЦІАЛЬНИЙ РОЗДІЛ

### 2.1 Підхід до конфіденційної передачі інформації в системах зв'язку з фазоманіпульованими сигналами

Результат досягається тим, що в відому систему передачі інформації, яка містить передавач в складі джерела інформації, послідовно включених першого фазового модулятора і першого модулятора, послідовно включених підсилювача потужності і передавальної антени, генератора фазоманіпульованого сигналу, синхронізатора передавача, пов'язаного першим виходом із входом генератора фазоманіпульованого сигналу, генератора несучої частоти, пов'язаного першим виходом з другим входом першого модулятора, і приймач в складі послідовно включених приймальної антени, змішувача, підсилювача проміжної частоти і узгодженого фільтра, послідовно включених вирішального пристрою і одержувача інформації, синхронізатора приймача, пов'язаного входом з виходом узгодженого фільтра, одним виходом з другим входом змішувача через гетеродин, а другим виходом з першим входом вирішального пристрою, в передавач введені блок управління фазою, що формує  $N$  імпульсів, де  $N = 2^n$ ,  $n \geq 1$ , діючих одночасно протягом інформаційного символу, кожен тривалістю рівний тривалості інформаційного символу і з комбінацією полярностей, добуток яких позитивний для одного з інформаційних символів і негативний для іншого з інформаційних символів, пов'язаний першим входом із виходом джерела інформації, другим входом із другим виходом синхронізатора передавача, першим виходом з першим входом першого фазового модулятора, а іншими виходами кожен через послідовно включені  $i$ -тий фазовий модулятор і  $i$ -тий модулятор з відповідним входом суматора, де  $2 \leq i \leq N$ , блок затримки з  $N$  виходами, пов'язаний входом з виходом генератора фазоманіпульованого сигналу, а  $N$  виходами кожен з другим входом відповідного фазового модулятора, генератор шуму, пов'язаний виходом з  $N + 1$  входом суматора, підключеного виходом до підсилювача

потужності, а першим входом до виходу першого модулятора,  $N-1$  виходів генератора несучої частоти, починаючи з другого, пов'язані з другими входами відповідних модуляторів, а вхід генератора несучої частоти пов'язаний з третім виходом синхронізатора передавача, в приймач введені  $n$  блоків перетину і  $n$  блоків затримки, при цьому перший блок перетину пов'язаний першим входом з виходом узгодженого фільтра безпосередньо, а другим входом через перший блок затримки, наступні  $n-1$  блоків перетину з'єднані кожен першим входом з виходом попереднього блоку перетину безпосередньо, а другим входом через відповідний по номеру блок затримки, вихід  $n$ -го блоку перетину пов'язаний з другим входом вирішального пристрою.

Завдання, на вирішення якої спрямована пропонована система передачі інформації, полягає в підвищенні скритності переданої інформації і завадостійкості в умовах дії структурних завад.

Сутність запропонованої системи передачі інформації полягає в тому, що на передавальній стороні формування біта інформації, що передається забезпечується шляхом підсумовування  $N$  ФМН сигналів певним чином зсунутих за часом відносно один одного і з певним поєднанням фаз. Сумарний сигнал, що представляє біт, стає схожим на «вирізку» шуму, крім того забезпечується його маскування в шумі шляхом адитивного накладення цього шуму. За рахунок управління фазами підсумованих ФМН сигналів можлива зміна форми результуючого сигналу навіть в тому випадку, коли в інформаційній посилці відсутнє чергування одиниць і нулів, а йдуть однакові символи.

На приймальній стороні проводиться тимчасове стиснення сигналу в фільтрі, узгодженому з вихідним «гладким» ФМН сигналом. Вихідний сигнал фільтра буде являти собою суму автокореляційних функцій (АКФ) підсумованих на передавальній стороні ФМН сигналів. Розташування  $N$  основних пелюсток АКФ на тимчасовій осі і відносні фази цих пелюсток представляють собою параметри селекції, за якими на основі використання процедури перетину проводиться розпізнавання і згортка  $N$  пелюсток в один,

визначення переданого символу і компенсація завад, перш за все структурних. Така організація формування та обробки сигналів при передачі двійковій послідовності символів призводить до суттєвого підвищення скритності і завадостійкості системи передачі інформації.

Запропонований підхід пояснюється кресленнями графічного матеріалу. На рис. 2.1 представлена структурна схема системи передачі інформації, де позначено: 1 - джерело інформації, 2 - блок управління фазою, 3 – синхронізатор передавача, 4 - генератор фазоманіпульованого сигналу, 5 - блок затримки з N виходами, 6.1 ... 6.i ... 6.N – фазові модулятори, 7.1 ... 7.i ... 7.N - модулятор, 8 – генератор несучої частоти, 9 - генератор шуму, 10 - суматор, 11 - підсилювач потужності, 12 - передавальна антена, 13 - приймальна антена, 14 - змішувач, 15 - гетеродин, 16 – підсилювач проміжної частоти, 17 - узгоджений фільтр, 18.1 ... 18.n - блоки затримки, 19.1 ... 19.n - блоки перетину, 20 - синхронізатор приймача, 21 – вирішальний пристрій, 22 - одержувач інформації.

Призначення елементів, що становлять структурну схему заявленої системи передачі інформації, впливає з назви цих елементів і пояснюється в описі принципу дії системи.

Перед поясненням принципу роботи запропонованої системи доцільно зробити деякі загальні зауваження щодо вибору сигналів і їх параметрів.

На передавальній стороні в якості вихідного сигналу, який бере участь у формуванні біта інформації, що передається, може бути використаний практично будь-який ФМН сигнал з маніпуляцією фаз «0», « $\pi$ ». Можлива комбінація різних сигналів, що складають вихідний. Моделювання показало, що принцип формування і обробки на основі процедури перетину, який використовується в заявленому пристрої забезпечує невисокий рівень бічних пелюсток АКФ на виході схеми обробки для будь-яких, навіть «поганих» з цієї точки зору сигналів. Найбільше застосування знайшли ФМН сигнали на основі псевдовипадкових M-послідовностей. Тому для імітаційної моделі обраний

саме такий сигнал, 15-елементна послідовність виду  $\{M_1^4\}$ , тривалістю  $\tau$  з тривалістю елементарного (парціального) імпульсу  $\Delta\tau$  рис. 2.2.

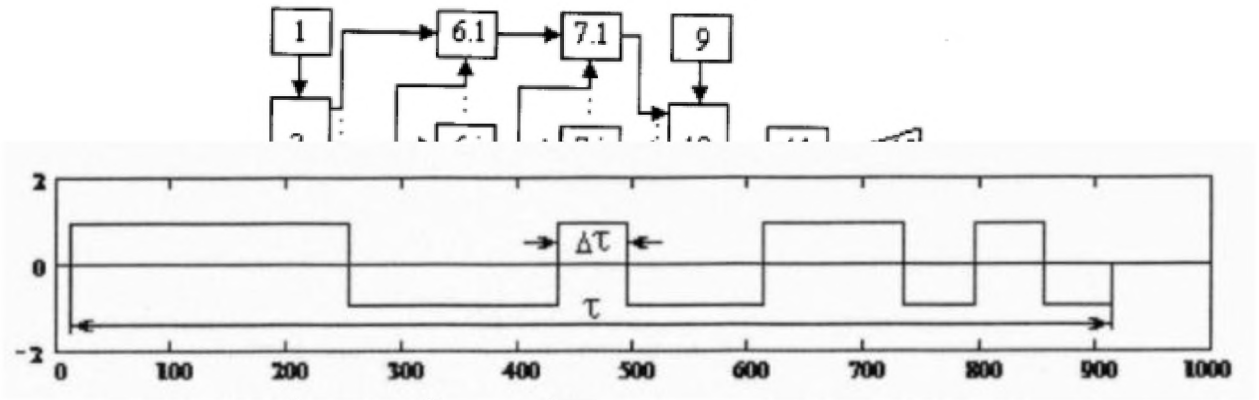
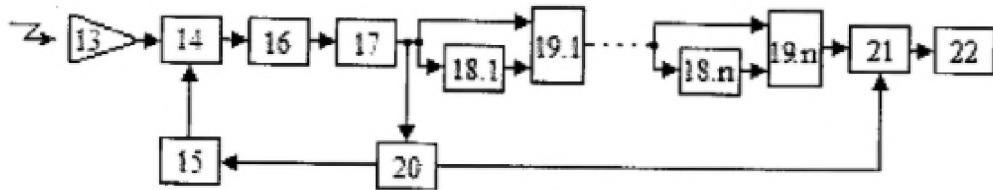


Рисунок 2.2 – Огинаюча сигналу 15-елементної M-послідовності з виходу генератора ФМН сигналу

а) - передавач



б) – приймач

Рисунок 2.1 – Структурна схема передачі інформації за запропонованим підходом

Високочастотний ФМН сигнал, на несучій частоті, представлений на рис. 2.3,

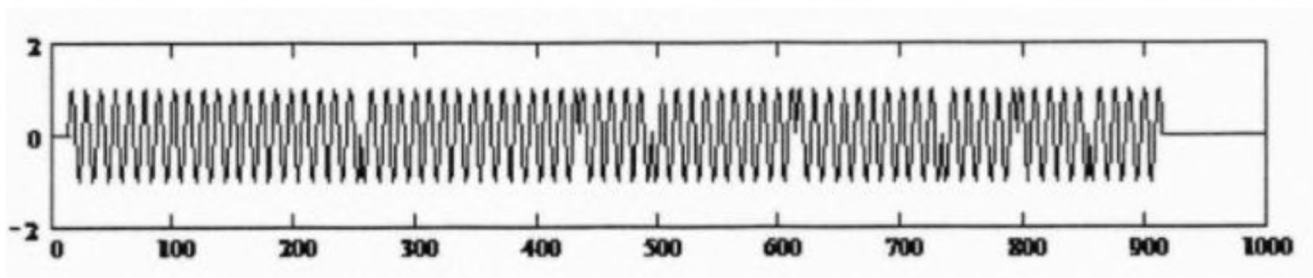


Рисунок 2.3 - Високочастотний ФМН сигнал, на несучій частоті

а на рис. 2.4 показана його АКФ, отримана на виході узгодженого фільтра приймача.

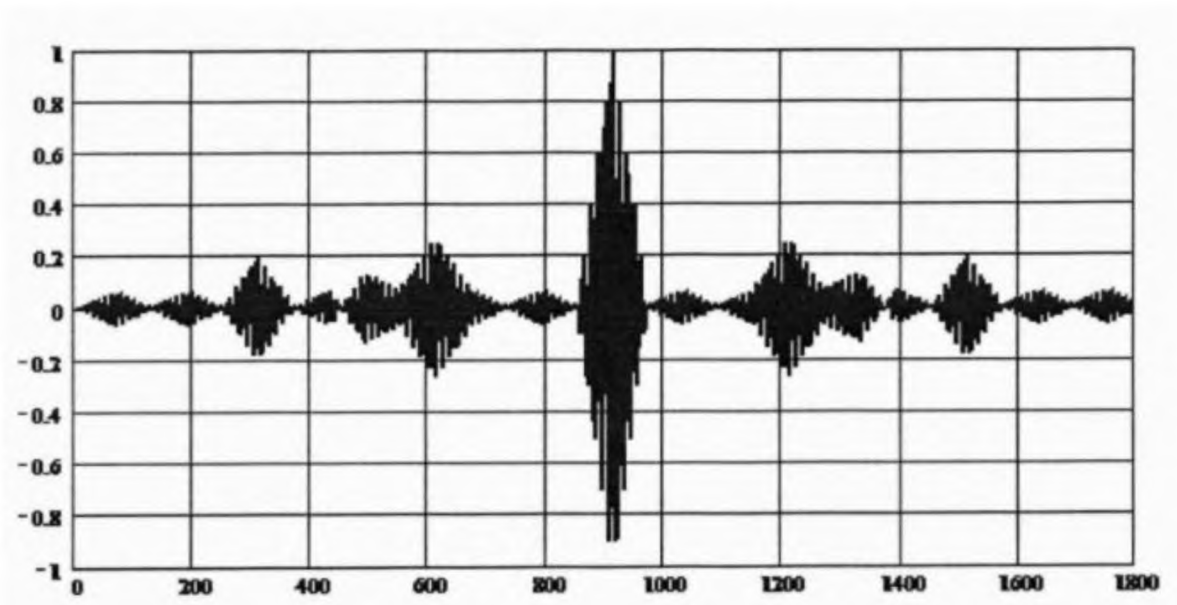


Рисунок 2.4 – Автокореляційна функція на виході узгодженого фільтра приймача

Вибір тимчасових затримок  $\Delta t_i$ , здійснюваний в блоці затримки 5, при формуванні сумарного сигналу повинен забезпечувати отримання на приймальній стороні результуючої АКФ на виході узгодженого фільтра у вигляді нерівномірного імпульсно-часового коду в складі  $2^n$  основних пелюсток (піків), де  $n \geq 1$ , а  $N = 2^n$ . Основу сигналу являє собою пара ФМН імпульсів, рознесених на інтервал  $\Delta t_1 \geq \Delta \tau$ . Якщо  $n=2$ , то наступна пара, в котрій  $\Delta t_1$  фіксовано, зсувається відносно першої на інтервал  $\Delta t_2 \geq \Delta t_1$ . При  $n=3$  друга група вже з 4-ох ФМН імпульсів з незмінними  $\Delta t_1$  і  $\Delta t_2$  зсувається відносно початку 1-ї групи на інтервал  $\Delta t_3 \geq \Delta t_2$ . Потім при  $n=4$  група з 8-ми імпульсів входить в незмінному вигляді в сумарний сигнал з 16-и ФМН імпульсів і т.д. Таким чином, з ростом  $n$  сигнали виявляються «вкладеними» попередній в наступний. Інакше кажучи, результуючий сигнал, який є сумою  $N = 2n$  ФМН імпульсів, можна представити у вигляді суми наступних самостійних груп  $2^1, 2^2, \dots, 2^i$  ( $i < n$ ) при довільному, але не однаковому виборі

інтервалів між групами  $\Delta t_i < \Delta t_j$ , при  $i < j$ . Можливо і інше співвідношення між інтервалами, важливо лише зберегти умову  $\Delta t_i \neq \Delta t_j$ , де  $i \neq j$ , тобто неповторюваність інтервалів і ефект вкладення. Однак найбільш просто реалізується сигнал із дедалі вищими значеннями тимчасових інтервалів. Такий принцип дозволяє, по-перше, спростити процедуру синтезу в поєднанні з забезпеченням досить складного його кодування в межах біта, по-друге, реалізувати попарно згортку піків АКФ на приймальній стороні при мінімальній кількості блоків затримки і блоків перетину, що реалізують цю згортку, яке визначається співвідношенням  $\log_2 N = n$ ; по-третє, використовувати властивості процедури перетину, які полягають в урахуванні знаків (фаз) при згортці та компенсації шумів і завад.

Вибір конкретних значень  $\tau$ ,  $\Delta\tau$ ,  $N$ ,  $n$ ,  $\Delta t_i$ ,  $B$  пов'язаний з розв'язуванням завданням передачі інформації, необхідною швидкістю  $C$ , широкополосністю  $F$ , показниками якості, включаючи скритність і стійкість перед завадами. При цьому значення  $\tau$ ,  $\Delta\tau$  і  $\Delta t_i$  повинні встановлюватися такими, щоб тривалість сумарного сигналу, що представляє біт інформації, не перевищувала тривалість цього біта  $T$ .

Разом з тим, як впливає з аналізу та результатів моделювання вже при  $n=2$  ( $N=4$ ) забезпечуються високі показники завадостійкості і скритності при інших рівних умовах для фіксованих значень швидкості передачі інформації і обраної для цього бази сигналу.

Принцип дії запропонованої системи передачі інформації розглянемо на прикладі формування в передавачі ФМН сигналу, що представляє двійкову одиницю «1» і обробки цього сигналу в приймачі (рис. 2.5).

У передавачі джерело інформації формує послідовність двійкових одиниць «1» і нулів «0» відповідно переданим повідомленням зі швидкістю  $C = \frac{1}{T}$ . Послідовність надходить на перший вхід блоку управління фазою 2. На рис. 2.5, а показаний цей сигнал у вигляді однієї двійкової одиниці «1» тривалістю  $T$ . Одночасно генератор ФМН сигналу 4 формує огинаючу цього

сигналу виду рис. 3 тривалістю  $\tau$ , яка надходить на вхід блоку затримки 5, а блок управління фазою 2 формує по кожному з виходів від 1-го до N-го позитивні або негативні імпульси управління фазою однакової тривалості  $T$ , діючі одночасно протягом інформаційного символу, і з комбінацією полярностей, добуток яких позитивний для одного з інформаційних символів і негативний для іншого. При цьому полярність кожного з імпульсів відповідає заданій комбінації знаків, обраній з набору певних заздалегідь для символів «1» і «0» дозволених комбінацій. Принцип формування цих комбінацій обмовляється далі по тексту. При моделюванні процесів формування та обробки сигналів в запропонованій системі прийняті  $n = 2, N = 2^n = 4$ .



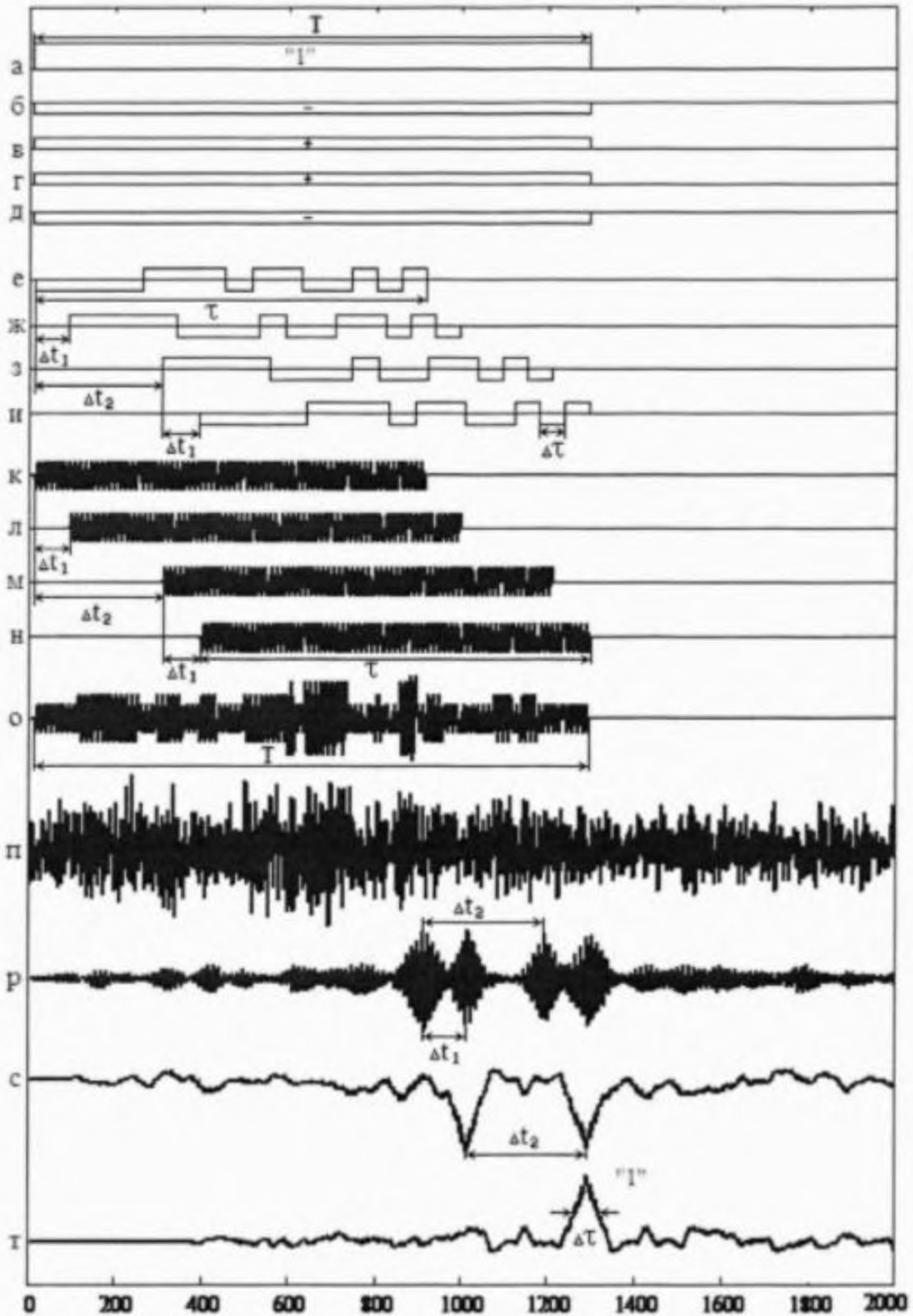


Рисунок 2.5 – Процеси в приймачі і передавачі при передачі «1»

На рис. 2.5 епюри б, в, г, д представляють собою вихідні сигнали блоку управління фазою 2 відповідно для 1 ... 4 виходів, які подаються на перші входи

відповідних фазових модуляторів 6.1 ... 6.N. На другі входи фазових модуляторів подаються однакові огинаючі ФМН сигналу виду рис. 2.3, що відрізняються по кожному з виходів від 1-го до N-го блоку затримки 5 тільки значенням тимчасового зсуву  $\Delta t_i$ , яке визначається блоком затримки. Полярність сигналу блоку 2 по кожному з виходів цього блоку буде визначати загальну фазу огинаючої модулюючого сигналу на виході відповідного модулятора 6.1-6.N.

Сигнали на виході вказаних модуляторів для розглянутого прикладу показані на рис. 2.5, е, ж, з, і. Тут загальні фази епюр рис. 2.5, е і рис. 2.5, і на виході модуляторів 6.1 і 6.4 визначаються негативною полярністю керуючих сигналів блоку 2 (рис. 2.5, б і рис. 2.5, д). Сигнали з виходів фазових модуляторів 6.1-6.N в якості керуючих надходять на перші входи відповідних модуляторів 7.1-7.N. На другі входи модуляторів подаються високочастотні сигнали несучої частоти з відповідних виходів генератора несучої частоти 8, що представляють собою безперервні гармонійні сигнали однакової амплітуди, частоти і початкової фази по кожному з виходів. Вихідні сигнали модуляторів 7.1-7.4 показані на рис. 2.5, к, л, м, н. кожен з них являє собою високочастотний ФМН сигнал тривалістю  $\tau$  з маніпуляцією фаз «0», « $\pi$ », яка визначається керуючим сигналом по першому входу. Відносні зсуви сигналів за часом з виходів модуляторів повторюють тимчасові зсуви, встановлені раніше в блоці затримки 5.

З виходів модуляторів ФМН сигнали надходять на відповідні 1-N входи суматора 10, де з урахуванням їх фаз підсумовуються. Вид сумарного сигналу показаний на рис. 2.5, о. Цей сигнал являє біт переданої інформації, в даному випадку двійкову одиницю «1», нагадує за формою вирізку шуму і має тривалість біта T.

Для підвищення скритності з генератора шуму 9 на N + 1 вхід суматора 10 подається шумовий сигнал, який накладається на сумарний інформаційний сигнал, маскуючи його. У розглянутому прикладі в якості шуму використовується нормально розподілений центрований випадковий процес зі

середнєквдратичним відхиленням рівним амплітуді ФМН сигналу з виходу модулятора. Зашумлений вихідний сигнал суматора показаний на рис. 2.5, п. Цей сигнал надходить на вхід підсилювача потужності 11, посилюється і випромінюється передавальною антеною 12. Синхронізація роботи блоків передавача забезпечується синхронізатором передавача 3, з першого, другого і третього виходів якого сигнали синхронізації надходять, відповідно, на вхід генератора ФМН сигналу 4, на другий вхід блоку управління фазою 2 і на вхід генератора несучої частоти 8. Сигнали синхронізатора реалізують узгодження формованих сигналів по параметрам часу та фази.

Обробка випромінюваного передавачем сигналу рис. 2.5, п проводиться в приймачі рис. 2.1, б. Сигнал, прийнятий приймальною антеною 13, перетворюється на проміжну частоту за допомогою змішувача 14 і гетеродина 15, посилюється в підсилювачі проміжної частоти 16 і надходить в узгоджений фільтр 17. Імпульсна характеристика фільтра 17 узгоджена з вихідним ФМН сигналом виду рис. 2.3 і реакція фільтра на такий сигнал являє собою АКФ виду рис. 2.4. Тому кожен зі складових аддитивної суми вхідних сигналів піддається незалежному стиску по часу.

Результуюча АКФ сумарного сигналу на виході узгодженого фільтра буде являти собою  $N$  основних пелюсток (піків) з відносними за часом зсувами, що відповідають зсувам, встановленим в передавачі в блоці 5 при формуванні сигналу. Відносні фази пелюсток «0» або « $\pi$ » будуть визначатися полярністю керуючих імпульсів з виходу блоку 2. Форма сигналу на виході узгодженого фільтра 17 при  $N = 4$  показана на рис. 2.5, р, де позначені їх зсуви за часом.

Далі завдання обробки полягає в розпізнаванні форми АКФ, як імпульсночасового коду з урахуванням фаз, шляхом попарної згортки її пелюсток, компенсації шумів і завад і визначенні виду прийнятого двійкового символу. Реалізація попарної згортки забезпечується за допомогою блоків перетину 19.1 ... 19.n і блоків затримки 18.1 ... 18.n. Для цього сигнал  $x_{17}(t)$  з виходу узгодженого фільтра 17 подається на перший вхід першого блоку перетину 19.1 безпосередньо, а на другий його вхід через блок затримки 18.1,

де затримується на інтервал  $\Delta t_1$ . Блок 19.1 виробляє над вхідними сигналами процедуру перетину виду:

$$u_{19.1}(t) = |x_{17}(t) + x_{17}(t - \Delta t_1)| - |x_{17}(t) - x_{17}(t - \Delta t_1)| \quad (2.1)$$

Тут  $u_{19.1}(t)$  миттєве значення сигналу на виході блоку 19.1 як функція часу  $t$ .

Вираз (2.1) може бути представлено в іншому вигляді:

$$u_{19.1}(t) = 2 * \text{sign}\{x_{17}(t)\} * \text{sign}\{x_{17}(t - \Delta t_1)\} * \min\{|x_{17}(t)|, |x_{17}(t - \Delta t_1)|\} \quad (2.2)$$

Записи (2.1) і (2.2) еквівалентні, але фізичний зміст процедури з'ясовується із співвідношення (2.2). З нього випливає, що процедура перетину забезпечує вибір подвоєного меншого за модулем з двох зіставлених значень (сигналів) з знаком, рівним добутку знаків цих значень.

Оскільки тривалість затримки в блоці 18.1 відповідає зрушенню між пелюстками пари АКФ  $\Delta t_1$ , На входах блоку 19.1 одночасно діють перший і другий пелюстки кожної поточної пари. Взаємодія сигналів проводиться відповідно до (2.2) на проміжній частоті. Фази взаємодіючих пелюсток АКФ будуть визначатися тим, які були полярності імпульсів з виходів блоку управління фазою 2 для відповідного ФМН сигналу в передавачі. У моделі керуючі імпульси для першого і четвертого сигналів негативні (рис. 2.5, б, д), а для другого і третього сигналів позитивні (рис. 2.5, в, г). Отже, перший і другий, а також третій і четвертий пелюстки АКФ, відповідні цим сигналам на виході узгодженого фільтра, будуть протилежні по фазі. Відповідно до загальних властивостей процедури перетину для огинаючої сигналу (після фільтра нижніх частот на виході блоку 19.1, усуває несучу частоту) справедливо співвідношення:

$$U_{19.1}(t) = U_m \cos \Delta\varphi(t), \quad (2.3)$$

де  $U_m$  – амплітуда,  $\Delta\varphi(t)$  - поточна різниця фаз взаємодіючих сигналів. Оскільки для розглянутих пар пелюсток АКФ  $\Delta\varphi = \pi$ , на виході першого перетину 19.1 кожна пара буде згорнута в одну пелюстку негативної полярності. Вихідний сигнал блоку 19.1 показаний на рис. 2.5, с. Часовий інтервал між імпульсами відповідає встановленим зсувам другої пари в передавачі, тобто  $\Delta t_2$ .

Слід підкреслити, що при цьому відбувається і часткова компенсація шумів і завад в силу властивості (2.2) вибирати менше, оскільки часове зрушення призводить до декореляції завад.

З виходу першого блоку перетину 19.1 сигнал надходить на перший вхід другого блоку перетину безпосередньо, а на другий його вхід через другий блок затримки 18.2. Затримка в блоці 18.2 відповідає тимчасовому зрушенню між парами  $\Delta t_2$ , тому вихідний сигнал другого блоку перетину 19.2 буде:

$$U_{19.2}(t) = |U_{19.1}(t) + U_{19.1}(t - \Delta t_2)| - |U_{19.1}(t) - U_{19.1}(t - \Delta t_2)|. \quad (2.4)$$

Оскільки обидва імпульсу на входах другого блоку перетину діють одночасно і обидва негативні, вони будуть згорнуті в силу (2.2) в один позитивний. Сигнал на виході другого блоку перетину 19.2 показаний на рис. 2.5, т. Тривалість цього імпульсу відповідає тривалості дискрети ФМН сигналу на передавальній стороні, тобто  $\Delta t$ .

Крім згортки в другому блоці перетину відбувається подальша компенсація шумів і завад, що буде показано далі. Якщо  $n > 2$  і  $N = 2^n > 4$ , то розглянуті процедури відбуваються з кожною парою «вкладених» один в одного сигналів. При цьому значення затримки в кожному наступному блоці затримки повинно відповідати встановленому тимчасовому зрушенню  $\Delta t_i$  для відповідного «вкладеного» сигналу.

Результатом згортки АКФ є сигнал виду рис. 2.5,т на виході 19.n-го блоку перетину.

Вельми важливим моментом з точки зору підвищення інформаційної складової скритності є можливість представлення одного і того ж двійкового символу за допомогою різноманітних фаз, які сумуються на передавальній стороні сигналів, що приводить до різних форм огинаючої сумарного сигналу і внутрішньосигнальної фазовій структурі.

Дійсно, в силу знакового характеру реалізації перетину (властивості (2.2) і (2.3)) для кожного  $N$  можна так підібрати комбінації полярностей керуючих імпульсів в формувачі 2, що кожен із символів «1» і «0» може бути представлений певною кінцевою множиною неповторюваних знаків для згортаємих пелюсток АКФ в приймальнику. При цьому результуючий добуток знаків відповідно до (2.2) буде, наприклад, для «1» позитивним, а для «0» негативний. В даному випадку при  $n=2$ ,  $N=4$  існує вісім різних комбінацій для представлення «1» і стільки ж для представлення «0».

Наведемо їх для представлення «1»:  $\{+,+,+,+\}$ ;  $\{-,-,-,-\}$ ;  $\{+,-,+,-\}$ ;  $\{-,+,-,+\}$ ;  $\{+,-,-,-\}$ ;  $\{-,-,+,+\}$ ;  $\{+,-,-,+\}$ ;  $\{-,+,+,-\}$ ; для представлення «0»:  $\{+,-,+,+\}$ ;  $\{-,+,+,+\}$ ;  $\{+,+,+,-\}$ ;  $\{+,+,-,+\}$ ;  $\{-,-,-,+\}$ ;  $\{-,-,+,+\}$ ;  $\{+,-,-,-\}$ ;  $\{-,+,-,-\}$ .

Аналіз показує, що в загальному випадку для заданого  $N$  кількість неповторюваних комбінацій знаків  $K_y$  кожного з двійкових символів підпорядковується правилу  $K_y = 2^{2^n-1}$ . Ці комбінації заздалегідь встановлюються, як в наведеному вище прикладі для  $N=4$  і використовуються при формуванні імпульсів в блоці 2. Дозволені комбінації встановлюються заздалегідь шляхом попарного перемноження знаків, що становлять ту чи іншу комбінацію, і відбору неповторюваних комбінацій. У наведеному прикладі для  $N=4$  попарний добуток знаків у кожній з відібраних комбінацій для можливого представлення «1» позитивний, а для подання «0» негативний. Полярність цих імпульсів на кожному з виходів повинна відповідати знаку встановленої комбінації для передачі «1» і «0». Кількість використовуваних комбінацій з дозволених може бути різна. Воно встановлюється організацією схеми блоку 2, яка пояснюється далі.

Процеси формування та обробки сигналів при передачі двійкового «0» відбуваються аналогічно і показані на рис. 2.7 епюри від а до т.

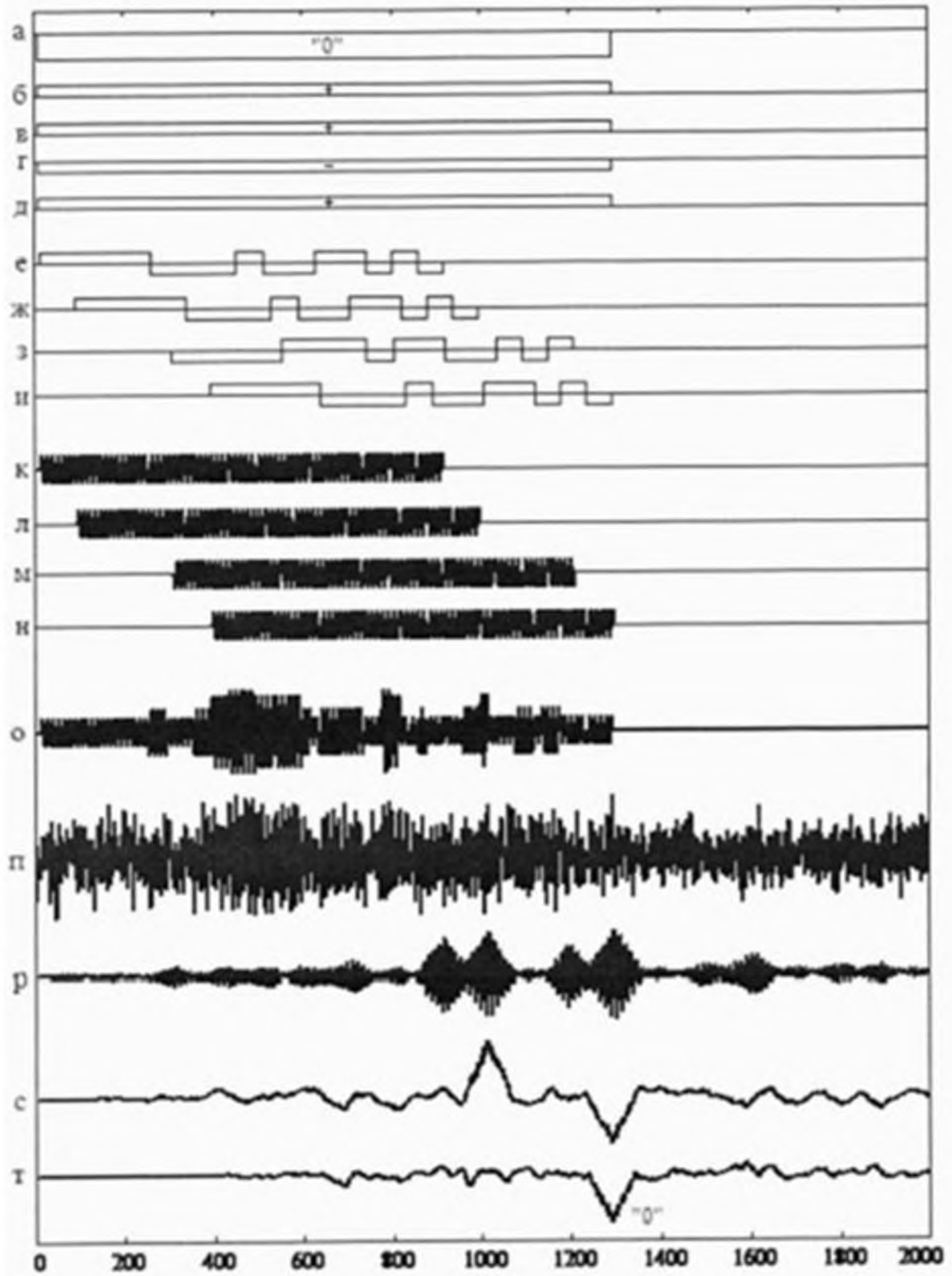


Рисунок 2.6 - Процеси в приймачі і передавачі при передачі «0»

Тут символ «0» з джерела інформації показаний у вигляді негативного сигналу (рис. 2.6, а), а в якості дозволеної комбінації для представлення «0» обрана наступна: {+, +, -, +}. Епюри сигналів з виходів блоку 2, відповідні цій комбінації показані на рис. 2.6, б, в, г, д.

Далі процес обробки полягає в ухваленні рішення про наявність чи відсутність того чи іншого двійкового символу в прийнятому повідомленні. Для цього з виходу блоку перетину 19.п сигнал надходить на другий вхід вирішального пристрою 21, де відбувається порівняння сигналу з встановленим порогом, що забезпечує необхідні показники якості. В цьому ж блоці формується інформаційна послідовність символів, що відповідає прийнятим рішенням.

Синхронізатор приймача 20 здійснює пошук ФМН сигналу по частоті і по часу, перебудовуючи гетеродин 15, накопичує сигнал для збільшення надійності синхронізації, управляє режимом роботи вирішального пристрою. Для цього на вхід синхронізатора надходить сигнал з виходу узгодженого фільтра 17, а першим і другим виходами синхронізатор пов'язаний з входом гетеродина і першим входом вирішального пристрою відповідно.

Після закінчення пошуку і входження в синхронізм на виході вирішального пристрою 21 з'являється інформаційна послідовність у вигляді двійкових символів, яка надходить одержувачу інформації 22.

## 2.1 Оцінка ефективності запропонованого підходу до конфіденційної передачі інформації в системах зв'язку з фазоманіпульованими сигналами

Для оцінки завадостійкості запропонованої системи передачі інформації в умовах різних завад змодельовано процес їх обробки в приймачі. Результати у вигляді епюр напружень, що характеризують різні етапи обробки, представлені на рис. 2.7. Позначення епюр відповідають прийнятим на рис. 2.5, 2.6.



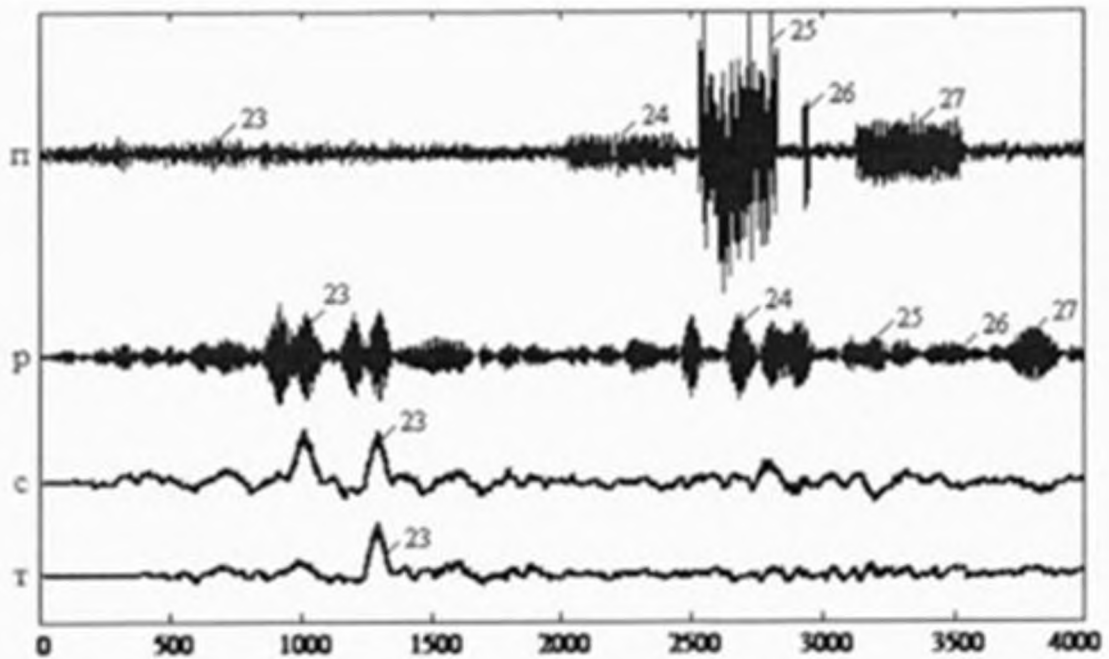


Рисунок 2.7 – Процес обробки сигналу в приймачі в умовах дії різних завад

На рис. 2.7, П показана діюча на вході приймача суміш у вигляді замаскованого в шумі сумарного ФМН сигналу 23 при  $N = 4$ , сформованого для подання «1» на основі дозволеної комбінації керуючих сигналів у вигляді  $\{+, +, +, +\}$ , і завад.

В якості завад використані: сигналоподібна завада 24 у вигляді ФМН сигналу на основі 7-елементного коду Баркера, що збігається з корисним сигналом по спектру (Тривалості дискрет однакові) і з коефіцієнтом взаємної кореляції  $K_{сп} \sim 0.6$ ; завада типу «шумовий спалах» 25, сформована шляхом підсумовування декількох нормально розподілених шумових «вирізок» з різними значеннями дисперсій і з тривалістю приблизно рівній тривалості корисного сигналу; короткий радіоімпульс 26 з тривалістю значно меншою тривалості дискрети корисного сигналу; довгий радіоімпульс 27, перевищує тривалість корисного сигналу. Всі завади істотно перевищують корисний сигнал по амплітуді і діють на несучій (проміжній) частоті сигналу (в моделі прийнята частота  $f = 8$  МГц). Для спрощення і наочності розглянутий випадок роздільної дії сигналу і завад.

На рис. 2.7, р показана суміш корисного сигналу і завад на виході узгодженого фільтра 17. Цифрові позначення сигналу і завад тут відповідають прийнятим на рис. 2.7, п. Як впливає з епюри при прийнятих умовах і сумарних базах корисного сигналу і структурних завад, накопичення цих завад в узгодженому фільтрі таке, що на виході вони сумірні за амплітудою з корисним сигналом. Умова  $q_n^2 > q_{n\text{пор}}^2$  не виконується як для сигналоподібної завади у вигляді коду Баркера 27, так і для «Шумового спалаху», який можна вважати з певними припущеннями еквівалентним дії одночасно декількох (більше 5) ФМН сигналів в силу випадкового характеру їх накладення, і імпульсної завади у вигляді потужного «довгого» імпульсу.

Моделювання та аналіз показують, що досить близька картина на виході узгодженого фільтра має місце і в тому випадку, якщо прийнятий спосіб захисту від завад у вигляді ШОУ. Таким чином, на якісному рівні (рис. 2.7, р) очевидна недостатня стійкість в умовах структурних завад.

Процес обробки суміші у введених елементах пропонованої системи передачі інформації ілюструється епюрами рис. 2.7, с, т.

На рис. 2.7, з показані сигнали на виході першого блоку перетину (19.1). Практично вже на цьому етапі обробки діє корисний сигнал 23 у вигляді пари пелюсток і залишки істотно скомпенсованих завад і шумів.

Другий блок перетину 19.2 виробляє згортку попередньої пари корисного сигналу і забезпечує подальшу компенсацію завад і шумів. Сигнал на виході блоку 19.2 показаний на рис. 2.7, т. Як видно з малюнка, кінцевий результат обробки вхідної суміші корисного сигналу, шумів і завад (рис. 2.7, п) на вході вирішального пристрою являє собою корисний сигнал 23. Шуми і завади майже повністю компенсовані, є їх окремі незначні сплески в порівнянні з результатом обробки в змодельованому прототипі (рис. 2.7, р).

Таким чином, якісний аналіз свідчить про істотний вигравш пропонованої системи в завадостійкості в умовах структурних завад.

Кількісна оцінка ефективності пропонованої системи проведена шляхом визначення статистичних показників якості на основі імітаційного

моделювання. Для цього змодельовані виявителі відповідно до схеми рис. 2.1, б для пропонованої системи і змодельованого прототипу.

За показники якості прийняті: ймовірність помилкової тривоги  $P_{пт}$ , ймовірність правильного виявлення  $P_{вияв}$ , ймовірність помилки при впливі завад  $P_{пом}$ .

При цьому під  $P_{пт}$ , розуміється ймовірність перевищення шумом заданого порогу виявлення; під  $P_{вияв}$  - ймовірність перевищення сумішшю сигналу і шуму фіксованого порога виявлення; під  $P_{пом}$  - ймовірність перевищення сумішшю завади і шуму цього порогу.

Оцінка зазначених ймовірностей визначалася як відношення числа позитивних результатів  $n$  до загальної кількості дослідів  $M$ :  $P = \frac{n}{M}$ .

Залежності ймовірності помилкової тривоги від відносного порога виявлення наведені на рис. 2.8 у вигляді  $P_{пт} = f(\frac{U_{пор}}{\sigma_{ш}})$ . Тут  $U_{пор}$  - значення порогу прийняття рішення у вирішальному пристрої,  $\sigma_{ш}$  - середньоквадратичне значення шуму на вході досліджуваної схеми. На рис. 2.8 цифрою 28 позначена  $P_{пт}$  для пропонованої системи; цифрою 29 - для змодельованого прототипу, цифрою 30 - для змодельованого прототипу при побудові обробки за принципом ШОУ.

З рис. 2.8 видно, що при однакових значеннях відносного порога рівень помилкових тривог для пропонованої системи істотно нижче, ніж для змодельованого прототипу.

Залежності ймовірності правильного виявлення від відносного рівня сигналу  $U_c$  на вході показані на рис. 2.9 у вигляді  $P_{вияв} = f(\frac{U_c}{\sigma_{ш}})$  при фіксованому порозі, що забезпечує  $P_{пт} = 0,005$ . Тут крива 31 відповідає пропонованій системі, крива 32 – змодельованому прототипу, крива 33 – змодельованому прототипу за схемою ШОУ. Поведінка кривих  $P_{вияв}$  свідчить про приблизно однакові енергетичні можливості заявленої системи і змодельованого прототипу за схемою ШОУ в забезпеченні необхідної якості виявлення.

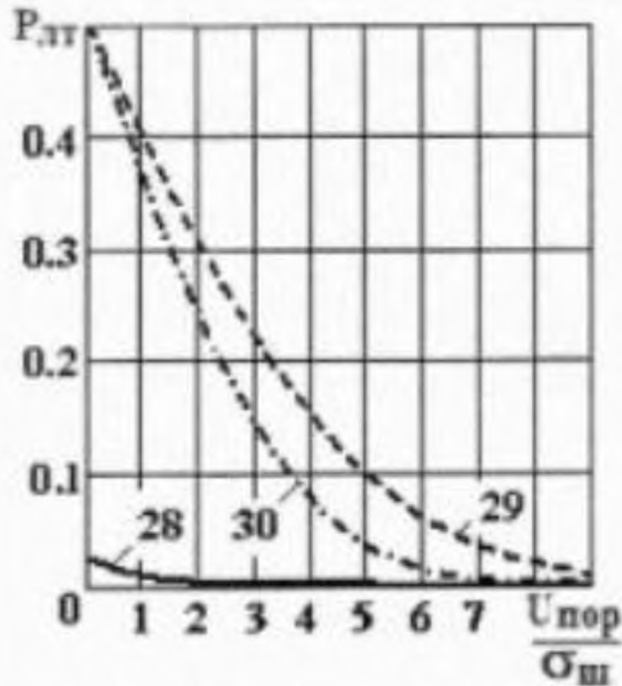


Рисунок 2.8 – Показник якості пропонованої системи передачі інформації

У той же час має місце певний порівняно невеликий програш змодельованому прототипу в  $P_{\text{вияв}}$  (криві 31, 32), що пояснюється наявністю некогерентної обробки в заявленій системі, починаючи з другого блоку перетину (19.2).

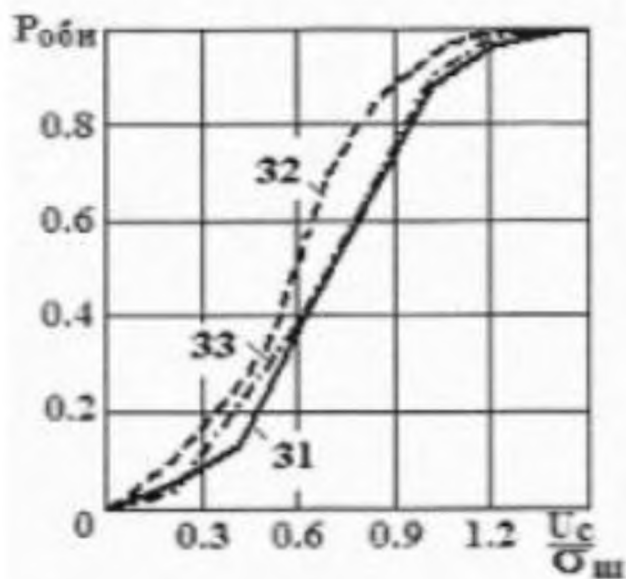


Рисунок 2.9 – Показник якості пропонованої системи передачі інформації

Загальний висновок свідчить про приблизно однакових енергетичних можливостях заявленої системи і змодельованого прототипу.

Залежності ймовірностей помилки від відносного рівня структурної завади на вході показані на рис. 2.10, 2.11 у вигляді  $P_{\text{пом}} = f\left(\frac{U_{\text{пом}}}{\sigma_{\text{ш}}}\right)$  при фіксованому порозі.

В якості структурної завади в одному випадку (для рис. 2.11) використовувався ФМН сигнал, що повністю співпадає з вихідним корисним по часовим параметрам і частково відрізняється фазовою структурою, з коефіцієнтом кореляції  $K_{\text{сп}} \approx 0,6 \sim 0,7$ . В даному випадку використовувалася М-послідовність того ж класу, що і корисний сигнал. На рис. 2.10 крива 34 відповідає пропонованій системі, крива 35 – змодельованому прототипу, крива 36 - прототипу за схемою ШОУ. Суттєву перевагу в завадостійкості в умовах подібних завад для пропонованої системи очевидна.

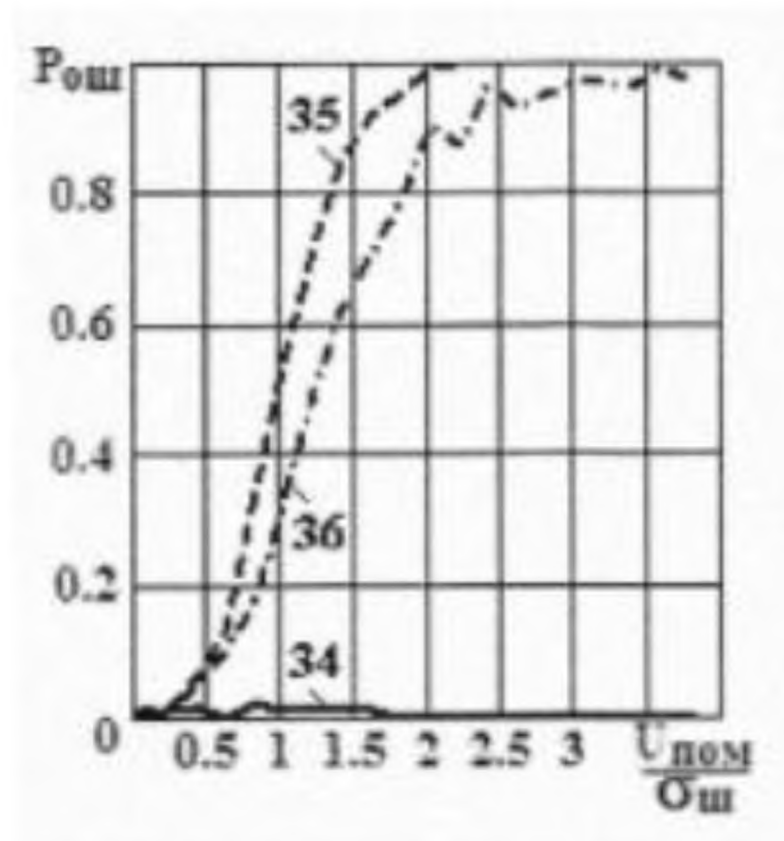


Рисунок 2.10 – Показник якості пропонованої системи передачі інформації

Аналогічні результати отримані для структурних завад у вигляді Д-кодів, М-послідовностей, 13-елементного коду Баркера (при сумірності баз корисного сигналу і завад).

У другому випадку (рис. 2.11) в якості структурної завади використовувався «довгий» ФМН сигнал ( $\tau_{\text{пер}} \gg \tau$ ). При цьому дотримувалась умова рівності тривалості дискрет ( $\Delta\tau_{\text{пер}} \gg \Delta\tau$ ). Завада формувалася у вигляді довільної комбінації ФМН сигналів різних класів, в яку в якості фрагментів вбудовувалися випадковим чином 1-3 корисних сигналів (тобто в цьому випадку  $K_{\text{сс}} = K_{\text{сп}} \approx 0,9 - 1$ ). На рис. 12 крива 37 відповідає пропонованій системі, крива 38 – змодельованому прототипу, крива 39 – змодельованому прототипу за схемою ШОУ.

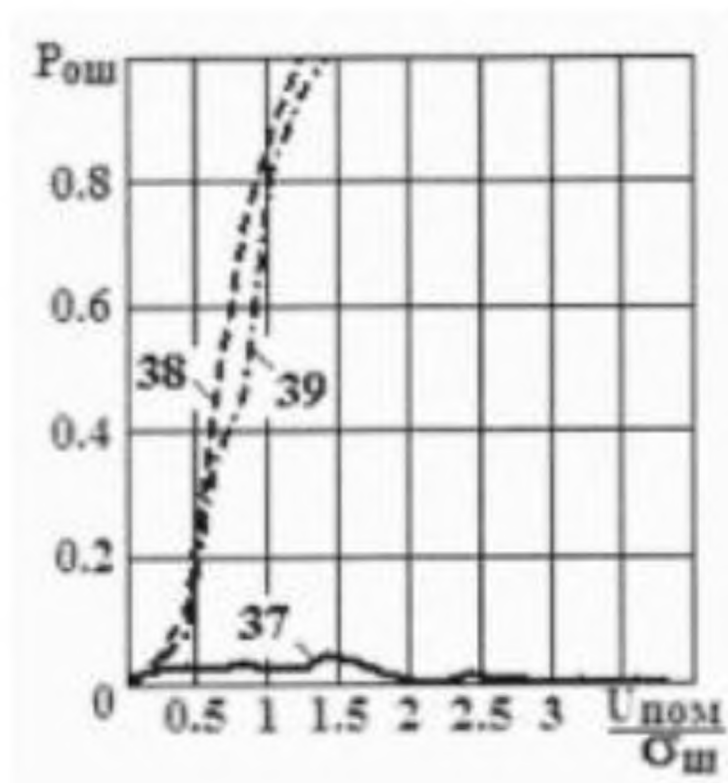


Рисунок 2.11 – показник якості пропонованої системи передачі інформації

З аналізу кривих випливає, що в умовах подібних завад змодельований прототип завадостійкістю не володіє. У той час як в заявленій системі ймовірність помилки не перевищує 0,05.

Слід також зауважити, що компенсація завад в обох випадках (рис. 2.11, 2.12) в запропонованій системі тим вище, чим більша амплітуда завади.

Нарешті, практичну значущість має оцінка завадостійкості в умовах структурних завад, коли одночасно число таких завад на вході приймача більше 5. Подібна ситуація має місце при роботі, наприклад, асинхронних адресних систем з ШПС. В силу множинності ФМН сигналів і випадкового характеру їх накладення сумарний сигнал завади на вході приймача буде являти собою випадковий процес з нормальним розподілом. Але така ситуація еквівалентна «шумовому спалаху», яка якісно вже розглянута (рис. 2.7).

Що стосується кількісної оцінки, то така можлива на основі аналізу залежностей ймовірності помилкової тривоги від відносного порога (рис. 2.8), які досліджувалися в нормально розподіленому шумі. Дійсно, зафіксуємо, наприклад, нульовий поріг ( $U_{\text{пор}} = 0$ ,  $\sigma_{\text{ш}} = \text{const}$ ) і оцінимо ймовірності помилкової тривоги. Якісно це епюра рис. 2.7, р для змодельованого прототипу і епюра рис. 2.7, т для пропонованої системи. Введемо коефіцієнт виграшу  $K_{\text{в}}$  у вигляді відносини ймовірностей помилкових тривог для змодельованого прототипу і заявленої системи, вираженого в дБ  $K_{\text{в}} = 20 \log_{10} \left( \frac{P_{\text{пт прот}}}{P_{\text{пт сист}}} \right)$  при фіксованому порозі. Ці залежності представлені на рис. 2.12, де цифрою 40 позначений коефіцієнт виграшу в порівнянні з змодельованим прототипом, а цифрою 41 - з змодельованим прототипом за схемою ШОУ. При нульовому порозі виграш становить 26 дБ.

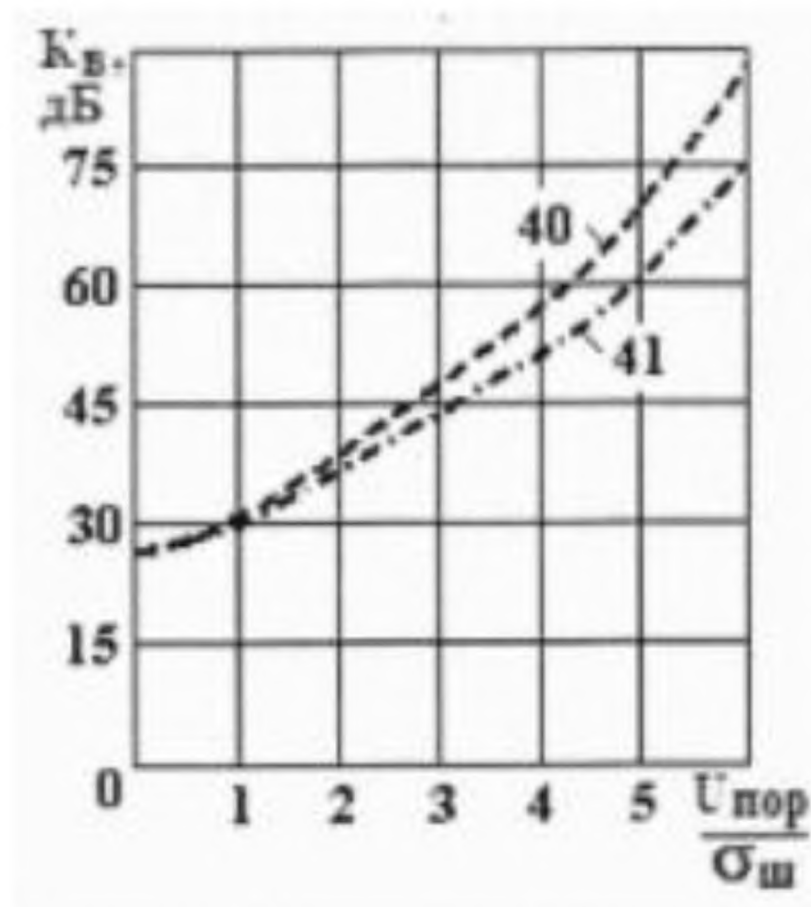


Рисунок 2.12 – Показник якості пропонованої системи передачі інформації

Слід зауважити, що це обумовлено властивостями послідовно здійснюваної процедури перетину в заявленій системі і дозволяє, крім того, забезпечувати маскування корисного сигналу в шумі на передавальній стороні з подальшою його компенсацією на приймальній стороні без істотного погіршення якості обробки з точки зору втрат у відношенні сигнал/шум. Що не розповсюджується на змодельований прототип. Оцінку скритності пропонованої системи проведемо, використовуючи результати роботи [3].

Під структурної скритністю будемо розуміти кількість двійкових вимірювань, які необхідно провести оператору для повного визначення структури сигналу. Оскільки в якості вихідної послідовності при формуванні сигналу використовується  $M$ -послідовність з кількістю елементів  $B$ , то скритність  $S$  такого сигналу для змодельованого прототипу буде:



$$S_{\text{пр}} = \log_2 B. \quad (2.5)$$

У запропонованій системі представляючий біт сигнал є сумою зсунутих  $N$  сигналів, схожий на вирізку шуму і замаскований шумом, тобто є випадковим сигналом. Скритність такого сигналу повністю визначається його базою, але, оскільки, крім фазової маніпуляції з'явилася випадкова амплітудна маніпуляція, на кожній позиції оператору потрібно оцінювати амплітуду, що еквівалентно подвоєнню бази  $2B$ . Для отримання нижньої межі оцінки будемо припускати, що маскування шумом відсутнє. Тоді структурна скритність такого сигналу буде:

$$S_{\text{стр}} = \log_2 2^{2B} = 2B. \quad (2.6)$$

Для передачі двійкових символів у пропонованій системі може бути використано  $2^N$  комбінацій, які необхідно розпізнати для подальшого інформаційного аналізу. Але це еквівалентно збільшенню вихідної бази в  $2^N$  разів. Тоді скритність заявленої системи може бути виражена у вигляді:

$$S_c = \log_2 2^{2^{n+1} * B} = 2^{n+1} * B. \quad (2.7)$$

Виграш в скритності представимо у вигляді відношення скритності заявленої системи до скритності змодельованого прототипу в залежності від бази

$$\frac{S_c}{S_{\text{пр}}} = \frac{2^{n+1} * B}{\log_2 B}. \quad (2.8)$$

Залежності виду (2.8) представлені на рис. 2.13 для випадків  $n = 2$  ( $N = 4$ ) і  $n = 3$  ( $N = 8$ ). В розглянутому прикладі для  $B = 15$  і  $n = 2$  значення виграшу в

скритності порівняно з прототипом складає приблизно 30 разів. При збільшенні бази і кількості сигналів, що сумуються, що представляють біт, зростання ще більше. Маскування сигналу шумом ще більш збільшує скритність і дозволяє обмежитися мінімальною кількістю підсумованих ФМН імпульсів для подання біта при фіксованій базі.

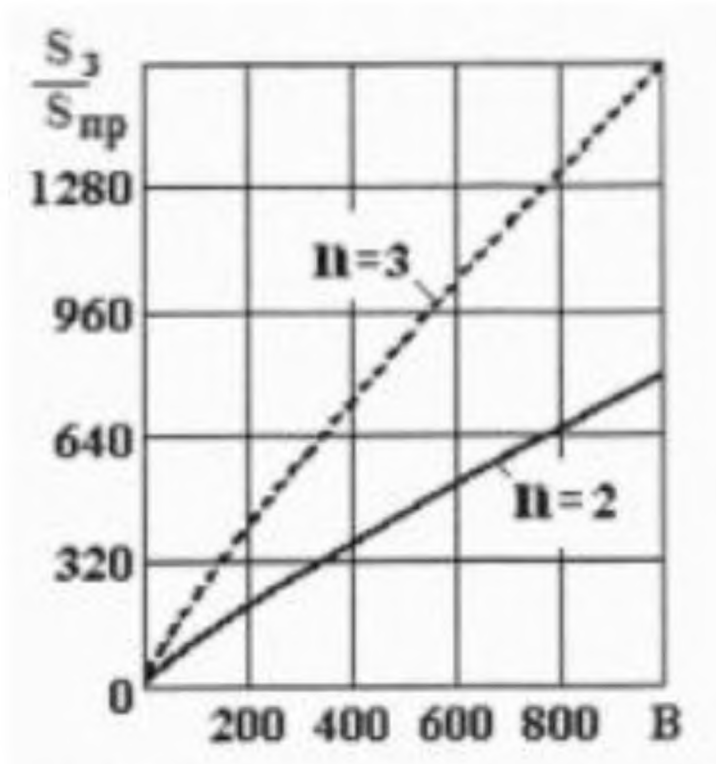


Рисунок 2.13 – Показник якості пропонованої системи передачі інформації

Також, слід відзначити можливість побудови всієї апаратури за універсальною аналого-цифровою схемою. В цьому випадку широкопasmовою частина передавача і приймача будується в аналоговому вигляді, а частина елементів пов'язана з формуванням і управлінням сигналами на передавальній стороні і оптимальним виявленням і обробкою на приймальній стороні - в цифровому на основі високошвидкісних багаторозрядних АЦП, цифрових перетворювачів частоти на основі цифрових синтезаторів DDS і логічних інтегральних схем із можливістю програмування (ПЛІС), що дозволяють шляхом реконструкції своєї «прошивки» всю трудомісткість по організації

процедур обробки зосередити в області програмного забезпечення при незмінній апаратурній частині.

Подібна побудова апаратури на сучасній елементній базі наведена в статті [4].

Зазначимо, також на наступні можливі варіанти побудови нововведених і деяких пов'язаних з ними елементів, заявленої системи передачі інформації. Джерело інформації 1 в залежності від призначення системи може представляти собою різного роду датчики. Наприклад, для телеметричних систем це може бути оптикоелектричний перетворювач [5].

Блок управління фазою 2 являє собою формувач  $N$  імпульсів з  $N$  виходами і двома входами. По одному входу подається інформаційний символ «1» або «0», який визначає вид дозволеної комбінації полярностей вихідних імпульсів блоку. По іншому входу надходить синхронізуючий сигнал. На виходах блоку повинні бути отримані імпульси, що збігаються за часом, однакові по амплітуді і тривалості із заданою (відомою) комбінацією полярностей. Побудова схеми такого формувача є порівняно простою стандартною задачею схемотехнічного проектування. Він може бути побудований на керованих мікросхемах, що виконують функції комутаторів з необхідною кількістю комутованих каналів [6]. Або на основі комбінаційних схем, що реалізують задану систему перемикаючих функцій [7].

Наприклад, на рис. 2.14 представлена структурна схема можливої реалізації блоку управління фазою при  $N = 4$ , якщо символ «1» представляється дозволеною комбінацією виду «-, +, +, -», а символ «0» - комбінацією виду «+, +, -, +». Схема включає в себе перший і другий розділові діоди; 23.1 ... 23.3 - перший, другий і третій інвертори; 24.1, 24.2 - першу і другу схеми «І» на два входи; 25.1, 25.2 - перший і другий формувачі імпульсів; 26.1 ... 26.2 - першу, другу, третю і четверту схему «АБО» на два входи.

Робота схеми полягає в наступному. Позитивний імпульс зі входу 1, відповідний «1», що пройшов через розділовий діод, дозволяє проходження зі

входу 2 через другий вхід першої схеми «І» 24.1 синхроімпульса, що надходить на перший формувач імпульсу 25.1.

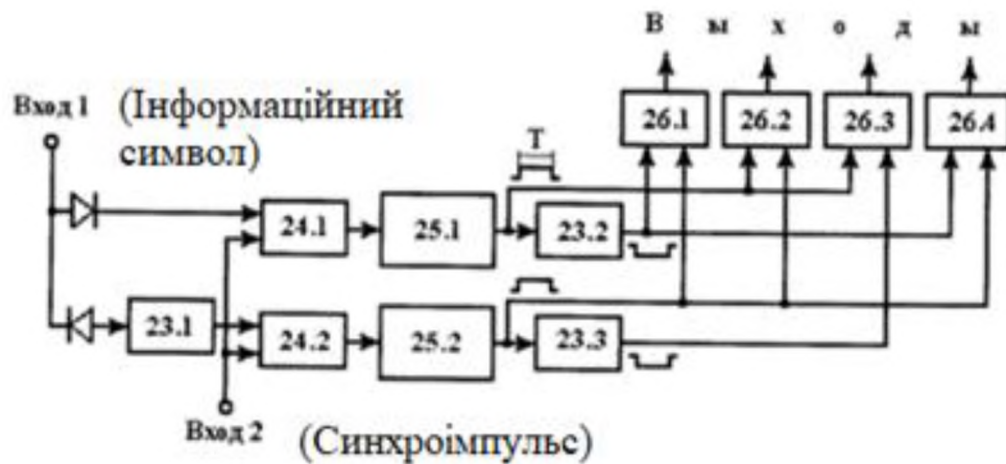


Рисунок 2.14 - Структурна схема можливої реалізації блоку управління фазою

Пристрій для формування (формував) забезпечує отримання на виході імпульсу позитивної полярності заданої тривалості  $T$ . Одночасно другий інвертор 23.2 (схема «НЕ») формує такий же імпульс негативної полярності. Позитивний імпульс надходить на перші входи другої 26.2 і третьої 26.3 схем «АБО», а негативний імпульс надходять на перші входи першої 26.1 і четвертої 26.4 схем «АБО». Підключення перших входів схем «АБО» відповідає заданій дозволений комбінації для символу «1», одержуваної на виходах схем «АБО» у вигляді керуючих фазою імпульсів.

Аналогічним чином відбувається формування керуючих імпульсів при надходженні інформаційного символу, відповідного «0». В цьому випадку негативний імпульс зі входу 1, відповідний «0», що пройшов через розділовий діод, включений зустрічно і через перший інвертор 23.1, дозволяє проходження зі входу 2 через другий вхід другої схеми «І» 24.2 синхроімпульса, що надходить на другий формувач імпульсу 25.2. Пристрій для формування 25.2 забезпечує отримання на виході імпульсу позитивної полярності заданої тривалості  $T$ . Одночасно третій інвертор 23.3 (схема «НЕ») формує такий ж імпульс негативної полярності. Позитивний імпульс надходить на другі входи

першої 26.1, другої 26.2 і четвертої 26.4 схем «АБО», а негативний імпульс надходять на другий вхід третьої 26.3 схеми «АБО». Підключення других входів схем «АБО» відповідає заданій дозволеній комбінації для символу «0», одержуваній на виходах схем «АБО» у вигляді керуючих фазою імпульсів.

Як видно з прикладу, вибір для представлення «1» і «0» інших дозволених комбінацій призводить до зміни конфігурації підключення схем «АБО». Змінюється схема і при зміні значення  $N$  (кількості імпульсів, що представляють біт). В даному прикладі  $N = 4$ . Якщо прийняти  $N = 8$ , то кількість схем «АБО» має бути теж 8, змінюється так само конфігурація їх підключення. В даному прикладі використовується всього дві комбінації, однак, і в цьому випадку реалізуються всі переваги заявленої системи передачі інформації.

Реалізація елементів, що входять в схему рис. 2.14, сумнівів не викликає, оскільки давно відпрацьована. Зокрема, практична реалізація схем «АБО», «І», інвертора («НЕ») приведена, наприклад, в книзі [8]. Пристрій для формування імпульсу може бути виконаний у вигляді чекаючого мультівібратора за схемою [9].

Синхронізатор передавача 3 може бути реалізований на основі задаючого автогенератора з кварцовою стабілізацією частоти і резонатором на поверхневих акустичних хвилях (ПАХ) [10].

Блок затримки з  $N$  виходами 5 може бути реалізований у вигляді багатовідвідної лінії затримки з ПАХ [11].

Генератор шуму 9 може бути зібраний за типовою схемою формування прямошумової завади [12].

Суматор 10 може бути виконаний за пасивною схемою на резисторах на частотах до 150 МГц, або на гібридних з'єднаннях в діапазоні СВЧ [13].

Блоки перетину 19.1 ... 19.n можуть бути реалізовані на базі сумматорів, вираховуючих пристроїв і пристроїв обчислення модуля [14].

Блоки вирахування і суматори, що входять в блоки перетину 19, можуть бути виконані за звичайною схемою підсилювачів з прямим і інверсним виходами або на двох прямих входах [15].

Пристрої обчислення модуля входять в блоки перетину 19, можуть бути зібрані на операційних підсилювачах [16].

Вирішуючий пристрій 21 включає в себе пороговий пристрій і пристрій формування вторинних імпульсів, заданої тривалості, амплітуди і полярності, відображаючих прийняття гіпотези про прийом двійкового символу «1» або «0». Він може бути реалізований за схемою вирішуючого пристрою, передбаченого для подібних випадків [17].

## 2.2 Висновок

Таким чином, отримані оцінки і результати моделювання підтверджують працездатність, достовірність, і досягнення технічного результату заявленої системи передачі інформації, яка в порівнянні із змодельованим прототипом, полягає в істотному (в десятки і сотні разів) поліпшенні скритності і завадостійкості в умовах структурних завад при фіксованій базі сигналу.

Можливість практичної реалізації заявленої системи передачі інформації впливає з того, що система будується на типових, відомих і технологічно відпрацьованих елементах і алгоритмах.

Це стосується як загальних з прототипом елементів і зв'язків, побудова та функціонування яких детально описані в різних джерелах, [17, 18, 19], так і нововведених елементів.

## РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

### 3.1 Обґрунтування витрат на організацію запропонованої системи зв'язку з фазоманіпульованими сигналами

Метою обґрунтування витрат на організацію запропонованої системи зв'язку з фазоманіпульованими сигналами є розрахунок капітальних витрат, оцінка величини можливого збитку від атаки, визначення та аналіз показників економічної ефективності.

### 3.2 Визначення трудомісткості організації запропонованої системи зв'язку з фазоманіпульованими сигналами

Трудомісткість продукції – показник, який характеризує витрати робочого часу на виробництво будь-якої споживчої вартості або на виконання конкретної технологічної операції. Трудомісткість проектування запропонованої системи передачі інформації розраховується за формулою (3.1):

$$t = t_0 + t_d + t_a + t_o + t_{па} + t_{од} \quad (3.1)$$

де  $t_0$  – витрати праці на підготовку і опис поставленого завдання;

$t_d$  – витрати праці на дослідження інформації про застосування ФМН сигналів в системах зв'язку;

$t_a$  – витрати праці на аналіз існуючих систем зв'язку з ФМН сигналами;

$t_o$  – витрати праці на організацію запропонованої системи зв'язку з ФМН сигналами;

$t_{па}$  – витрати праці на порівняльний аналіз скритності та завадостійкості запропонованої системи із існуючими підходами;

$t_{од}$  – витрати праці на оформлення документації.

У таблиці 3.1 зведені дані тривалості процесів, що мали місце при організації системи зв'язку для конфіденційної передачі даних з використанням ФМН сигналів.

Отже, загальна трудомісткість за формулою 3.1:

$$t = 7 + 25 + 30 + 36 + 27 + 21 = 146 \text{ годин}$$

Таблиця 3.1 – Дані тривалості процесів, що мали місце при організації системи зв'язку для конфіденційної передачі даних з використанням ФМН сигналів

Назва робочого процесу	Тривалість, год.
Витрати праці на підготовку і опис поставленого завдання	7
Витрати праці на дослідження інформації про застосування ФМН сигналів в системах зв'язку	25
Витрати праці на аналіз існуючих систем зв'язку з ФМН	30
Витрати праці на організацію запропонованої системи зв'язку з ФМН сигналами	36
Витрати праці на порівняльний аналіз скритності та завадостійкості запропонованої системи із існуючими підходами	27
Витрати праці на оформлення документації	21



3.3 Розрахунок капітальних витрат на організацію системи зв'язку для конфіденційної передачі інформації з використанням фазоманіпульованих сигналів

Капітальні витрати на організацію системи зв'язку з використанням ФМН сигналів включають витрати на заробітну плату інженера телекомунікацій і вартість машинного часу. Заробітна плата – винагорода, обчислена, зазвичай, у грошовому виразі, яку за трудовим договором власник або уповноважений ним орган виплачує працівникові за виконану ним роботу. Розмір заробітної плати залежить від складності та умов виконуваної роботи, професійно-ділових якостей працівника, результатів його праці та господарської діяльності підприємства. Витрати на заробітну плату розраховуються за формулою 3.2:

$$\text{ЗП} = t * C \quad (3.2)$$

де  $t$  – загальна тривалість організації системи зв'язку;

$C$  – середня годинна заробітна плата інженера телекомунікацій з урахуванням єдиного соціального внеску, грн/год.

Середня заробітна плата інженера телекомунікацій у місті Дніпро на кінець 2020 р. складає 9000 грн. Отже, річний фонд заробітної плати складає:

$$\text{Фр} = \text{ЗП} * 12 \quad (3.3)$$

$$\text{Фр} = 9000 * 12 = 108000 \text{ грн}$$

Єдиний соціальний внесок складає 22%, тобто:

$$\text{ЄСВ} = 22\% * \text{Фр} \quad (3.4)$$

$$\text{ЄСВ} = 22\% * 108000 = 23760 \text{ грн}$$

Визначимо номінальний річний фонд робочого часу, при цьому прийнявши середню тривалість робочого дня рівну 8 годинам:

$$F_{рч} = (T_k - T_{св} - T_{вих} - T_{від}) * t_p \quad (3.5)$$

де  $T_k$  – кількість календарних днів у році, днів;

$T_{св}$  – кількість святкових днів у році, днів;

$T_{вих}$  – кількість вихідних днів у році, днів;

$T_{від}$  – календарна тривалість відпустки, днів;

$t_p$  – середня тривалість робочого дня, год.

Отже, річний фонд часу за формулою 3.3 складає:

$$F_{рч} = (365 - 11 - 104 - 25) * 8 = 1800 \text{ годин}$$

Середня годинна заробітна плата інженера телекомунікацій визначається співвідношенням 3.6:

$$C_{гзп} = \frac{\Phi_{ЗПесв}}{F_{рч}}, \text{ грн/год} \quad (3.6)$$

де  $\Phi_{ЗПесв}$  – річний фонд заробітної плати з урахуванням єдиного соціального внеску ( $\Phi_p + \text{ЄСВ}$ );

$F_{рч}$  – річний фонд робочого часу.

Середня заробітна плата інженера телекомунікацій за годину за формулою 3.4 дорівнює:

$$C_{гзп} = \frac{\Phi_p + \text{ЄСВ}}{F_{рч}} = \frac{131760}{1800} = 73,2 \text{ грн/год}$$

Отже, витрати на оплату праці розробника складають:

$$ЗП = 146 * 73,2 = 10687,2 \text{ грн}$$

Розрахунок вартості машинного часу, необхідного для розробки на ЕОМ включає витрати на програмне та апаратне забезпечення і витрати за електроенергію, здійснюється по формулі 3.7:

$$Змч = Собл + Сел \quad (3.7)$$

де Собл – витрати на обладнання, грн;

Сел – витрати на електроенергію, грн.

Для розрахунку вартості машино-часу необхідно знати вартість ЕОМ та ПЗ на момент їх придбання і введення в експлуатацію, потужність ЕОМ і вартість споживаної електроенергії. Вартість персонального комп'ютеру Asus X556U ( $K_{аз}$ ) складає 13700 грн, програмного забезпечення Matlab 6.5 ( $K_{зпз}$ ) – 5000 грн, разом – 18700 грн.

Витрати на електроенергію залежать від часу роботи на ЕОМ та собівартості машино-години роботи ЕОМ і розраховується за формулою:

$$Сел = Смч * t, \quad (3.8)$$

$$Смч = W * Цел \quad (3.9)$$

Де  $W$  – потужність ЕОМ,  $W = 0,5$  кВт/год.

$Цел$  – вартість 1 кВт год електроенергії. Станом на кінець 2020 року за обсяг, спожитий понад 100 кВт · год електроенергії на місяць (включно) складає 1,68 грн. [20]

$$Сел = 0,5 * 1,68 * 146 = 122,64 \text{ грн}$$

Отже, витрати на проектування та моделювання запропонованої системи передачі конфіденційної інформації складають:

$$K = 18700 + 122,64 + 10687,2 = 29509,84 \text{ грн}$$

3.4 Розрахунок річних експлуатаційних витрат на утримання і обслуговування запропонованої системи передачі конфіденційної інформації

Річні поточні витрати складаються з:

$$C = C_{\text{в}} + C_{\text{к}} + C_{\text{ак}} \quad (3.10)$$

де  $C_{\text{в}}$  – вартість відновлення і модернізації системи. Візьмемо значення рівне нулю, адже підхід через свою новизну в модернізації не потребує;

$C_{\text{к}}$  – витрати на керування системою в цілому;

$C_{\text{ак}}$  – витрати викликані активністю користувачів запропонованої системи передачі конфіденційної інформації.

$$C_{\text{к}} = C_{\text{н}} + C_{\text{а}} + C_{\text{з}} + C_{\text{ев}} + C_{\text{ел}} + C_{\text{о}} + C_{\text{тос}} \quad (3.11)$$

де  $C_{\text{н}}$  – витрати на навчання адміністративного персоналу й кінцевих користувачів;

$C_{\text{а}}$  – річний фонд амортизаційних відрахувань;

$C_{\text{зев}}$  – річний фонд заробітної плати інженерно-технічного персоналу з урахуванням єдиного соціального внеску;

$C_{\text{ел}}$  – вартість електроенергії, що споживається, визначається за формулою:

$$C_{\text{ел}} = P * F_{\text{р}} * C_{\text{е}} \quad (3.13)$$

де  $P$  – встановлена потужність апаратури запропонованої системи передачі конфіденційної інформації, кВт;

$F_p$  – річний фонд робочого часу запропонованої системи передачі конфіденційної інформації;

$C_e$  – тариф на електроенергію, грн/кВт·годин;

$C_o$  – витрати на залучення сторонніх організацій для виконання деяких видів обслуговування, навчання та сертифікацію обслуговуючого персоналу;

$C_{\text{тос}}$  – витрати на технічне й організаційне адміністрування та сервіс системи.

Річний фонд амортизаційних відрахувань ( $C_a$ ) складає 25% від капітальних витрат:

$$C_a = 29509,84 * 0,25 = 7377,46 \text{ грн}$$

Потужність ( $P$ ) апаратури становить 0,04 кВт.

За 40-годинного робочого тижня річний фонд робочого часу системи інформаційної безпеки ( $F_p$ ) становить 1920 год.

Тариф на електроенергію ( $C_e$ ) складає 1,68 грн/кВт·годин.

Вартість електроенергії, що споживається апаратурою запропонованої системи передачі конфіденційної інформації протягом року ( $C_{\text{ел}}$ ) становить:

$$C_{\text{ел}} = 0,04 * 1920 * 1,68 = 129,02 \text{ грн}$$

Витрати на залучення сторонніх організацій для виконання деяких видів обслуговування, навчання та сертифікацію обслуговуючого персоналу запропонованої системи передачі конфіденційної інформації ( $C_o$ ) складають 2% від вартості капітальних витрат.

$$C_o = 29509,84 * 0,02 = 590,2 \text{ грн}$$

Витрати на технічне й організаційне адміністрування та сервіс запропонованої системи передачі конфіденційної інформації ( $C_{\text{тоc}}$ ) складають 2% від вартості капітальних витрат.

$$C_{\text{тоc}} = 29509,84 * 0,02 = 590,2 \text{ грн}$$

Визначимо річні поточні витрати:

$$\begin{aligned} C &= 7377,46 + 590,2 + 590,2 + 590,2 + 129,02 + 144936 + 885,3 \\ &= 155098,38 \text{ грн} \end{aligned}$$

### 3.5 Оцінка величини можливого збитку від атаки

Упущена вигода від простою атакованого вузла або сегмента лінії виробництва становить:

$$U = \Pi_{\text{п}} + \Pi_{\text{в}} + V \quad (3.10)$$

де  $\Pi_{\text{п}}$  – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента лінії виробництва, грн;

$\Pi_{\text{в}}$  – вартість відновлення працездатності вузла або сегмента, визначимо рівним нулю, адже не застосовна для запропонованої системи;

$V$  – втрати від зниження обсягу виробництва за час простою атакованого вузла або сегмента лінії виробництва, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента лінії виробництва являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$\Pi_{\Pi} = \frac{\sum Z_c \times \text{Ч}_c}{F} \times t_{\Pi} \quad (3.11)$$

де  $F$  – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 год)

$Z_c$  – місячна заробітна плата співробітника атакованого вузла або сегмента лінії виробництва з нарахуванням єдиного соціального внеску, грн на місяць;

$\text{Ч}_c$  – чисельність співробітників атакованого вузла або сегмента лінії виробництва, осіб.;

$t_{\Pi}$  – час простою вузла або сегмента лінії виробництва внаслідок атаки, годин.

Середня місячна заробітна плата у місті Дніпро на кінець 2020 р. співробітника лінії виробництва становить 11000 грн. Кількість співробітників – 25.

Визначимо оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента лінії виробництва:

$$\Pi_{\Pi} = (11000 * 25 / 176) \times 6 = 9375 \text{ грн}$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із середньогодинного обсягу продажів і часу простою атакованого вузла або сегмента корпоративної мережі (час повторного введення втраченої інформації і час відновлення після атаки не застосовні для запропонованої системи):

$$V = \frac{O}{F_r} \times t_{\Pi} \quad (3.12)$$

де  $O$  – обсяг виробництва атакованого вузла або сегмента лінії виробництва, грн у рік;

$F_r$  – річний фонд часу роботи організації (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 год.

$$V = 5000000 / 2080 \times 6 = 14423,08 \text{ грн}$$

Визначимо упущену вигоду від простою атакованого вузла або сегмента лінії виробництва:

$$U = 9375 + 14423,08 + 0 = 23798,08 \text{ грн}$$

Таким чином, загальний збиток від атаки на вузол або сегмент лінії виробництва організації складе:

$$B = \sum_I \sum_N U \quad (3.13)$$

де  $N$  – середнє число можливих атак на рік;

$I$  – число атакованих вузлів або сегментів корпоративної мережі.

$$B = 23798,08 \times 3 \times 8 = 571153,85 \text{ грн}$$

3.6 Загальний ефект від впровадження запропонованої системи зв'язку з фазоманіпульованими сигналами

Загальний ефект від впровадження запропонованої системи зв'язку з фазоманіпульованими сигналами з урахуванням ризиків порушення доступності інформації становить:

$$E = B * R - C \quad (3.14)$$



де  $B$  – загальний збиток від атаки на вузол або сегмент лінії виробництва організації;

$R$  – очікувана ймовірність атаки на вузол або сегмент лінії виробництва, частки одиниці;

$C$  - річні експлуатаційні витрати;

$$E = 571153,85 * 0,35 - 155098,38 = 44805,47 \text{ грн}$$

3.7 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Оцінка економічної ефективності системи захисту інформації, розглянутої у спеціальній частині дипломної роботи, здійснюється на основі визначення та аналізу наступних показників:

а) коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає показник ROSI (Return on Investment for Security);

б) термін окупності капітальних інвестицій  $T_o$ .

Коефіцієнт повернення інвестицій показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки. Щодо до інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол, а отже:

$$ROSI = \frac{E}{K}$$

(3.15)

де ROSI – коефіцієнт повернення інвестицій;

$E$  – загальний ефект від впровадження системи інформаційної безпеки, грн;

$K$  – витрати на проектування та моделювання запропонованої системи передачі конфіденційної інформації, грн.

$$ROSI = 44805,47 / 29509,84 = 1,52$$

Термін окупності капітальних інвестицій показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_o = \frac{K}{E} = \frac{1}{ROSI} \quad (3.16)$$

де  $T_o$  – термін окупності капітальних інвестицій.

$$T_o = \frac{1}{1,52} = 0,66 \text{ років.}$$

### 3.8 Висновок

У третьому розділі кваліфікаційної роботи була визначена економічна ефективність запропонованої системи зв'язку з фазоманіпульованими сигналами.

Було розраховано капітальні та експлуатаційні витрати, які склали 29509,84 грн і 155098,38 грн відповідно.

Оцінено величину можливого збитку від реалізованої атаки через упущену вигоду – 571153,85 грн.

Визначено термін окупності капітальних інвестицій. Він склав 7 місяців 28 днів.

Таким чином можна вважати, що впровадження запропонованої системи зв'язку з фазоманіпульованими сигналами на підприємство є економічно доцільним рішенням.

## ВИСНОВКИ

1. В результаті аналізу типових підходів до застосування ФМН сигналів в системах зв'язку для конфіденційної передачі інформації встановлено, що застосування ФМН сигналів дозволяє забезпечувати завадостійкість щодо структурних завад, а також структурну та інформаційну складові скритності, але на недостатньому рівні. В результаті аналізу основних структурних схем систем зв'язку встановлено, що проектування завадостійких і скритних систем з ФМН сигналами наразі є актуальною задачею, яка ґрунтується на глибокому знанні теорії і схемотехніки.

2. Перевага запропонованого підходу полягає в підвищенні структурної та інформаційної складових скритності, а також підвищенні завадостійкості відомої системи в умовах структурних завад при фіксованій базі ФМН сигналу.

3. Результат досягається тим, що в передавач введені блок управління фазою, пов'язаний першим входом з виходом джерела інформації, другим входом - з другим виходом синхронізатора передавача, першим виходом з першим входом першого фазового модулятора, а іншими виходами кожен через послідовно включені  $i$ -й фазовий модулятор і  $i$ -й модулятор - з відповідним входом суматора, де  $2 \leq i \leq N$ ,  $N = 2^n$ ,  $n \geq 1$ , блок затримки з  $N$  виходами,

пов'язаний входом з виходом генератора фазоманіпульованого сигналу, а  $N$  виходами кожен - зі другим входом відповідного фазового модулятора, генератор шуму, пов'язаний виходом з  $N + 1$ -м входом суматора, підключеного виходом до підсилювача потужності, а першим входом - до виходу першого модулятора,  $N-1$  виходів генератора несучої частоти, починаючи з другого, пов'язані з другими входами відповідних модуляторів, а вхід генератора несучої частоти пов'язаний з третім виходом синхронізатора передавача, в приймач введені  $n$  блоків перетину і  $n$  блоків затримки, при цьому перший блок перетину пов'язаний першим входом з виходом узгодженого фільтра безпосередньо, а другим входом через перший блок затримки, наступні  $n-1$  блоків перетину з'єднані кожен першим входом - з виходом попереднього блоку перетину безпосередньо, а другим входом через відповідний за номером блок затримки, вихід  $n$ -го блоку перетину пов'язаний зі другим входом вирішуючого пристрою.

## ПЕРЕЛІК ПОСИЛАНЬ

1. «Радиотехнические системы передачи информации»: Учебное пособие для ВУЗов / В.А. Борисов, В.В. Калмыков, Я.М. Ковальчук и др.; Под редакцией В.В. Калмыкова - М.: «Радио и связь», 1990. - 304 с.: ил., с. 237-238, рис. 11.9.
2. Л.Е. Варакин «Системы связи с шумоподобными сигналами». - М.: «Радио и связь», 1985. - 384 с., ил., рис. 1.7, с. 16.
3. З.М. Каневский, В.П. Литвиненко. Теория скрытности. Воронеж, ВГУ., 1991. - 76 с.
4. Н.Г. Пархоменко, Б.М. Баташов. Решение задачи оптимальной обработки сигналов со сложными видами модуляции при помощи универсальных устройств на ПЛИС. Радиоконтроль. Вып. №5, 2002 г., с. 81-88; рис. 1, с. 82; рис. 2, рис. 3, с. 83; рис. 4, с. 85.
5. Е.С. Левшина, П.В. Новицкий. Электрические измерения физических величин: (Измерительные преобразователи). Уч. пособ. для вузов. - Л.: Энергоатомиздат. Ленингр. отд-ние, 1983. - 320 с., ил., с. 308, рис. 12-22.

6. Цифровые и аналоговые микросхемы. М.: Радио и связь, 1989, с. 47-139.
7. В.И. Корнейчук, В.П. Тарасенко, Ю.Н. Мишинский. Вычислительные устройства на микросхемах: Справочник - К.: Техника, 1986. - 264 с. ил., с. 217, рис 2.7.
8. Б.С. Гершунский. Основы электроники и микросхемотехники: Учебник. - 4-е изд., перераб. и доп. - К.: Выща шк., 1989. - 423 с. на стр. 212.
9. Шило В.Л. Популярные цифровые микросхемы: Справочник. - М.; Радио и связь, 1987. - 352 с.: ил. - (Массовая радиобиблиотека). Вып. 1111.
10. А.А. Дворников, В.И. Огурцов, Г.М. Уткин. Стабильные генераторы с фильтрами на поверхностных акустических волнах. - М.: Радио и связь. 1983 - 136 с., ил., с. 113, рис. 4.9.
11. А.И. Куприянов, А.В. Сахаров. Радиоэлектронные системы в информационном конфликте. - 2-е изд. - М.: Вузовская книга, 2007. - 528 с.: ил., с. 154, рис. 8.1.
12. А.П. Голубков, А.Д. Долматов, А.П. Лукошкин и др. Проектирование радиолокационных приемных устройств. Уч. пособ. для радиотех. спец. вузов: Под. ред. М.А. Соколова. - М.: Высш. шк., 1984 - 325 с., ил., с. 33, рис. 1.23, с. 127-129.
13. В.И. Гордиенко, С.Е. Дубровский, Р.И. Рюмшин, Д.В. Фенев. Универсальный многофункциональный структурный элемент систем обработки информации. / Радиоэлектроника / Изв. ВУЗов, №3, 1998, - с. 13-17, рис. 1, с. 14.
14. А.Г. Алексеенко. Применение прецизионных аналоговых интегральных микросхем. - М.: Радио и связь, 1981, рис. 2, 3, с. 77, рис. 2, 3.
15. В.П. Боровский, В.И. Костенко, В.М. Михайленко и др. Справочник по схемотехнике для радиолюбителя. Под. ред. Бобровского А.П., - К.: Техника, 1989, с. 211, рис. 12.4.

16. В.Б. Пестряков, В.П. Афанасьев, В.Л. Гурвиц и др. Шумоподобные сигналы в системах передачи информации. Под ред. проф. В.Б. Пестрякова. М.: - Сов. радио, 1973 - 424 с. с. 232, рис. 6.8.3.
17. Р.К. Диксон. Широкополосные системы. Перевод с англ. Л.Ф. Жигулина. Под ред. В.И. Журавлева.
18. Радио и связь, 1985. - 384 с., ил; В.Б. Пестряков, В.П. Афанасьев, В.Л. Гурвиц и др
19. Шумоподобные сигналы в системах передачи информации. Под ред. проф. В.Б. Пестрякова. М.: Сов. радио. 1973. - 424 с., ил. и др.
20. Минфин. Тарифы на электроэнергию в 2020 году: <https://index.minfin.com.ua/tariff/electric/>  
(дата звернення 05.12.2020)
21. В. В. Колесов, А. И. Полубехин, Е. П. Чигин, А. Д. Юрин. Применение дискретных хаотических алгоритмов в широкополосных телекоммуникационных системах. Вестник СибГУТИ. 2016. № 3
22. Методичні вказівки до виконання економічної частини дипломного проекту зі спеціальності 125 Кібербезпека / Упоряд.: І.В. Шереметьєва, Д.П. Пілова, Н.М. Романюк. – Дніпро: Національний технічний університет «Дніпровська політехніка», 2017. – 17 с.
23. Методичні рекомендації до виконання дипломних робіт (проектів) бакалаврів та магістрів спеціальностей 125 Кібербезпека, 172 Телекомунікації та радіотехніка / Упоряд.: О.Ю. Гусєв, О.В. Герасіна, О.М. Алексєєв, О.В. Кручінін. – Дніпро: НГУ, 2020. – 50 с.

## ДОДАТОК А. ВІДОМІСТЬ МАТЕРІАЛІВ КВАЛІФІКАЦІЙНОЇ РОБОТИ

№	Формат	Найменування	Кількість листів	Примітки
<i>Документація</i>				
1	A4	Реферат	3	
2	A4	Список умовних скорочень	1	
3	A4	Зміст	2	
4	A4	Вступ	1	
5	A4	Стан питання. Постановка задачі	30	
6	A4	Спеціальна частина	30	
7	A4	Економічна частина	11	



8	A4	Висновки	2	
9	A4	Перелік посилань	3	
10	A4	Додаток А	1	
11	A4	Додаток Б	1	
12	A4	Додаток В	1	
13	A4	Додаток Г	1	

#### ДОДАТОК Б. ПЕРЕЛІК ДОКУМЕНТІВ НА ОПТИЧНОМУ НОСІЇ

1 Презентація Ковтун К.А.pptx

2 Диплом Ковтун К.А.docx

ДОДАТОК В. ВІДГУК КЕРІВНИКА ЕКОНОМІЧНОГО РОЗДІЛУ

Відгук керівника економічного розділу:

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

Керівник розділу

\_\_\_\_\_

(підпис)

\_\_\_\_\_

(ініціали, прізвище)

ДОДАТОК Г. ВІДГУК КЕРІВНИКА КВАЛІФІКАЦІЙНОЇ РОБОТИ  
**ВІДГУК**  
**на кваліфікаційну роботу студента групи 125м-19-1 Ковтуна К.А.**  
**на тему: «Забезпечення конфіденційності при передачі інформації в**  
**системах зв'язку з фазоманіпульованими сигналами»**

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на \_\_\_\_ сторінках.

Мета роботи є актуальною, оскільки вона спрямована на підвищення завадостійкості систем зв'язку в умовах структурних завад при фіксованій базі фазоманіпульованого сигналу.

При виконанні роботи автор продемонстрував добрий рівень теоретичних знань і практичних навичок. На основі аналізу положень про застосування шумоподібних сигналів в системах зв'язку, а також існуючих підходів до

конфіденційної передачі інформації в системах зв'язку з фазоманіпульованими сигналами в ній сформульовані задачі, вирішенню яких присвячений спеціальний розділ. У ньому було запропоновано підхід до конфіденційної передачі інформації в системах зв'язку з підвищеною скритністю та завадостійкістю при фіксованій базі фазоманіпульованого сигналу та оцінено його ефективність.

Практична цінність роботи полягає в тому, що запропонований підхід може використовуватися в засобах радіозв'язку та радіотелеметрії для забезпечення конфіденційності при передачі інформації.

Рівень запозичень у кваліфікаційній роботі відповідає вимогам «Положення про систему виявлення та запобігання плагіату».

В цілому робота задовольняє усім вимогам, а її автор Ковтун К.А. заслуговує на оцінку «  
» та присвоєння кваліфікації «Магістр з кібербезпеки» за спеціальністю 125 Кібербезпека.

**Керівник роботи,  
к.т.н., доцент**

**О.В. Герасіна**