Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет інформаційних радіотехнологій та технічного захисту інформації
(повна назва)

Кафедра медіаінженерії та інформаційних радіоелектронних систем
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти *другий (магістерський)*
(позначення документа)

Аналіз методів обробки телевізійних сигналів

(тема)

Виконав:
студент 2 курсу, групи *МІм-22-2*
Роман СКОРИК
(прізвище, ініціали)

Спеціальність *172 Телекомунікації та радіотехніка*
(код і повна назва спеціальності)

Тип програми *освітньо-професійна*
(освітньо-професійна або освітньо-наукова)

Освітня програма *Медіаінженерія*
(повна назва освітньої програми)

Керівник *проф. Володимир КАРТАШОВ*
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Володимир КАРТАШОВ
(підпис) (прізвище, ініціали)

2023 р.

Харківський національний університет радіоелектроніки

Факультет Інформаційних радіотехнологій та технічного захисту інформації
Кафедра Медіаінженерії та інформаційних радіоелектронних систем

Рівень вищої освіти другий (магістерський)
Спеціальність 172 Телекомунікації та радіотехніка.
(код і повна назва)
Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма "Медіаінженерія"

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«____»_____ 20 ___ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Студентові *Скорику Роману Михайловичу*
(прізвище, ім'я, по батькові)

1. Тема роботи *Аналіз методів обробки телевізійних сигналів*
затверджена наказом по університету від " *20* " *10* *2023 р. №* *1224 Ст*
2. Термін подання студентом роботи *08.01.2023 р.*
3. Вихідні дані до проекту (роботи)
В дослідженнях використовувати адаптивний скремблер з паралельним аналізом. Дослідження виконати з використанням середовища Matlab. В якості джерела цифрового сигналу використовувати послідовність відеокадрів.
4. Перелік питань, що потрібно опрацювати в роботі
ВСТУП
1 Аналітичний огляд методів канального кодування сигналів
2 Методи скремблювання
3 Моделювання адаптивного скремблера
4. Результати моделювання адаптивного скремблера
ВИСНОВКИ
ПЕРЕЛІК ПОСИЛАНЬ
ДОДАТКИ
5. Перелік графічного матеріалу із зазначенням обов'язкових креслеників, схем, плакатів, комп'ютерних ілюстрацій:
Узагальнена структурна схема СПІ; Структурна схема формувача ПВП; Структурні схеми систем передачі інформації з ізольованим і неізольованим генераторами ПВП; Структурна схема адаптивного скремблера; Алгоритм моделювання; Результати моделювання

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Аналітичний огляд методів канального кодування сигналів	20.10.23–10.11.23	
2.	Аналіз методів скремблювання	11.1.23–20.11.23	
3.	Моделювання адаптивного скремблеру з використанням програм середовища *Matlab.*	21.11.23–30.11.23	
4.	Опис і аналіз результатів моделювання адаптивного скремблера	01.12.23–15.12.23	
5.	Графічна частина роботи	16.12.23–01.11.23	
6.	Перевірка керівником	02.12.23–04.01.23	
7.	Перевірка на академічний плагіат	05.01.23–05.03.23	
8.	Перевірка завідувачем кафедри, рецензування	06.01.23–07.01.23	

Дата видачі завдання *20.10.2023 р.*

Студент  *Роман СКОРИК*
(підпис)

Керівник роботи _____ *проф. Володимир КАРТАШОВ*
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка магістерської роботи має: 76 сторінок, 28 рисунків, 2 таблиці, 31 джерел.

КАНАЛЬНЕ КОДУВАННЯ, ПАРЦІАЛЬНЕ КОДУВАННЯ, СКРЕМБЛЮВАННЯ, ПСЕВДОВИПАДКОВІ ПОСЛІДОВНОСТІ, ВЛАСТИВОСТІ ПВП, ГЕНЕРАТОРИ ПВП, АДАПТИВНИЙ СКРЕМБЛЕР, MATLAB

Об’єкт дослідження – адаптивний скремблер з ізольованим генератором псевдовипадкових бітових послідовностей.

Предмет дослідження –методи адаптивного скремблювання з ізольованим генератором псевдовипадкових бітових послідовностей.

Мета роботи – дослідження ефективності роботи адаптивного скремблера з паралельним аналізом для системи цифрового телебачення в порівнянні з простим скремблером.

Метод дослідження – аналітичне і математичне імітаційне моделювання адаптивного скремблера, оптимізація його структури і параметрів.

В магістерській роботі в середовищі MATLAB методом математичного моделювання досліджена ефективність роботи адаптивного скремблера з паралельним аналізом. Усі результати моделювання зведені в таблицю, з ціллю зручності аналізу ефективності адаптивного скремблювання результати зображені на гістограмах й по ним зроблені висновки. Сформульовані практичні рекомендації з використання досліджених методів і пристроїв скремблювання прі передачі цифрового телевізійного сигналу.

ABSTRACT

The explanatory note of the master's thesis has: 76 pages, 28 figures, 2 tables, 31 sources.

CHANNEL CODING, PARTIAL CODING, Scrambling, PSEUDO-RANDOM SEQUENCES, INTERLEAVING, PVP PROPERTIES, PVP GENERATORS, ADAPTIVE SCRAMBLER, MATLAB

The object of research is an adaptive scrambler with an isolated generator of pseudorandom bit sequences.

The subject of research is adaptive scrambling methods with an isolated generator of pseudorandom bit sequences.

The purpose of the work is to study the efficiency of the adaptive scrambler with parallel analysis for the digital television system in comparison with a simple scrambler.

The research method is analytical and mathematical simulation modeling of an adaptive scrambler, optimization of its structure and parameters.

In the master's thesis, the effectiveness of the adaptive scrambler with parallel analysis was investigated using mathematical modeling in the MATLAB environment. All simulation results are summarized in a table, for the convenience of analyzing the effectiveness of adaptive scrambling, they are shown on histograms and conclusions are drawn based on them. Formulated practical recommendations for the use of researched scrambling methods and devices in the transmission of a digital television signal.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

АС- адаптивний скремблер;

БВН- код без повернення до нуля;

ЕВК - енергетичний виграш кодування;

ВЧ – висока частота;

ЗК- завадостійке кодування;

НЧ -низька частота;

ОЛФ - оптимальний лінійний фільтр;

ОНФ - оптимальний нелінійний фільтр;

ПВП – псевдовипадкова послідовність;

ПЕОМ - персональний комп'ютер;

РС – код Ріда -Соломона;

РЛС - радіолокаційна система;

СПІ -система передачі інформації.

ВСТУП

Розвиток інформаційно-телекомунікаційних систем пов’язують із підвищенням швидкості й достовірності обробки та передачі інформації. Вирішення цієї проблеми за рахунок підвищення енергетичних ресурсів системи себе вичерпало. Один з напрямків, який отримав широкий розвиток, пов’язують із розробкою теорії та практики побудови методів кодування із заданими характеристиками.

Системи передачі інформації в даний час є переважно є цифровими. Цифрове телебачення, зокрема, являє собою спосіб і технічні засоби передачі та прийому стисненого цифрового відеосигналу, які є сучасною альтернативою традиційному аналоговому телебаченню та забезпечують істотно більш високу якість передачі та відтворення зображень за рівних або менших матеріальних витрат [1-3]. Телевізійний сигнал, який призначений для передачі каналом зв'язку, являє собою в цьому випадку послідовність кодових (цифрових) комбінацій імпульсів [5-8].

Сучасні цифрові технології отримання, передачі та запису (зберігання) інформації відкривають сучасному суспільству якісно нові можливості та горизонти розвитку інформаційної галузі, а також усього людства загалом. У порівнянні з поширеною раніше аналоговою системою сучасне цифрове телевізійне мовлення забезпечує наступні істотні переваги:

- дуже висока якість зображення;
- значне число програм мовлення;
- менші вимоги до потужності телевізійного сигналу, що передається;
- знижуються вимоги щодо рівня сигнал-шум в каналі передачі повідомлень;
- відсутнє повторення зображень.

Істотне зниження вимог до потужності телевізійного сигналу, що передається, призводить до значного послаблення взаємного впливу сусідніх каналів один на одного.

У той же час під час передачі або запису сигналів цифрового телебачення часто виникають пакетні помилки, що спотворюють відразу кількох сусідніх символів цифрової послідовності. З використанням лише простих кодів, що дозволяють виправляти поодинокі помилки, немає можливості виправити такі пакети помилок [6]. У цьому випадку необхідно користуватися завадостійкими кодами з більш складною структурою і більшими можливостями, а також використовувати скремблювання цифрової послідовності. Стосовно аналізованої задачі застосування скремблювання дозволяє виключити з цифрового потоку даних довгі послідовності нулів і одиниць - групи бітів, що періодично повторюються. Вирішується також завдання «розрівнювання» спектра сигналу та підвищення надійності синхронізації приймального пристрою з джерелом даних, що передаються по лінії зв’язку.

Стосовно телекомунікаційних систем процес скремблювання також дозволяє підвищити надійність синхронізації пристроїв, забезпечує виділення тактової частоти сигналу безпосередньо з сигналу, що приймається, а також зменшує рівень перешкод. Істотна область завдань застосування скремблеру полягає в захисті інформації, що передається по каналу, від несанкціонованого доступу.

Для алгоритмів скремблювання дуже важливі швидкість функціонування і істотно випадковий характер допоміжної цифрової послідовності, який не можна відновити у разі перехоплення повідомлення противником. Процедура скремблювання може включати додавання певних компонент в сигнал, що передається, або зміна деяких його частин сигналу, щоб ускладнити процес відновлення вихідного виду сигналу або щоб надати сигналу заданих статистичних властивостей.

Скремблери в даний час застосовуються в телефонних мережах загального користування, супутниковому та радіорелейному радіозв'язку, цифровому телевізійному мовленні, а також з метою захисту інформації від копіювання.

Зазвичай процес скремблювання виконується на останньому етапі цифрової обробки цифрової послідовності безпосередньо перед модуляцією.

Завдання даної магістерської роботи полягає у дослідженні методом математичного моделювання адаптивного скремблера з паралельним аналізом, порівняння його з простим скремблером та отримання якісних показників ефективності їхньої роботи.

1. КАНАЛЬНЕ КОДУВАННЯ СИГНАЛІВ

1.1. Загальні відомості

В даний час у світі спостерігається інтенсивне розвиток цифрових систем передачі даних, таких як космічні, супутникові, мобільні системи та ін. Усі подібні цифрові системи використовують для зв'язку бездротові канали, в яких на переданий радіосигнал значну дію здійснюють заваді різної фізичної природи. Внаслідок дії завад прийняті цифрові дані з великою ймовірністю завжди будуть містити помилки. Але для багатьох практичних завдань допустима лише невелика частка помилок в оброблюваних цифрових даних. Таким чином, на практиці виникає актуальне завдання забезпечення надійної передачі цифрової інформації каналами зв'язку з шумами(рис.1.1) [1-3].

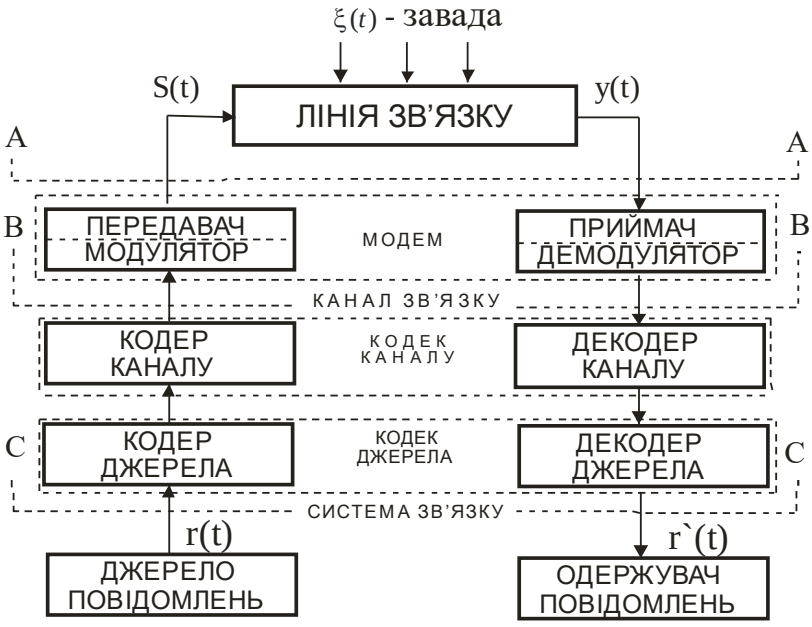


Рис. 1.1. Узагальнена структурна схема СПІ

Значний важливий внесок при вирішенні даної задачі відіграє теорія завадостійкого кодування. З її використанням розробляються методи та моделі захисту цифрових інформаційних систем від помилок, що базуються на застосуванні ефективних завадостійких кодів. Використання відомих на даний час кодів дозволяє отримати на практиці так званий енергетичний виграш кодування (ЕВК), що характеризує рівень можливого зниження енергетики каналу передачі інформації при кодуванні в порівнянні з відсутністю засобів кодування, якщо достовірність передачі інформації в обох випадках буде однакова. Цей енергетичний виграш можна використовувати з метою покращення якісних параметрів і характеристик багатьох важливих для практики властивостей систем передачі даних та іншої інформації, наприклад, для зменшення розмірів великих і дуже дорогих антен, підвищення дальності та якості зв'язку, збільшення швидкості передачі даних, зниження потужності передавача і т.п.

Зараз у рамках теорії кодування розроблено багато завадостійких кодів та методів декодування, які розрізняються рівнем енергетичного виграшу, надмірністю, складністю реалізації та рядом інших параметрів. Канальний завадостійкий код для реалізації цифрового запису та передачі повинен відповідати наступним основним істотним вимогам [4,5]:

1) спектр кодової послідовності не повинен мати постійну складову, а рівень низькочастотних компонентів у сигналі повинен бути мінімальним;

2) код, що використовується, повинен забезпечувати високу ефективність;

3) код повинен мати прийнятні властивості самосинхронізації (тривалість безперервних послідовностей одиниць або нулів повинна бути мінімальною);

4) перешкодостійкий код повинен володіти малою чутливістю до міжсимвольних спотворень, перешкод та помилок тактової синхронізації (розкриви очей-діаграми по вертикалі та ширина по горизонталі повинні бути максимальними) (див. рис.1.2, а);

5) технічний пристрій кодування має бути досить простим за своєю технічної реалізації [1].

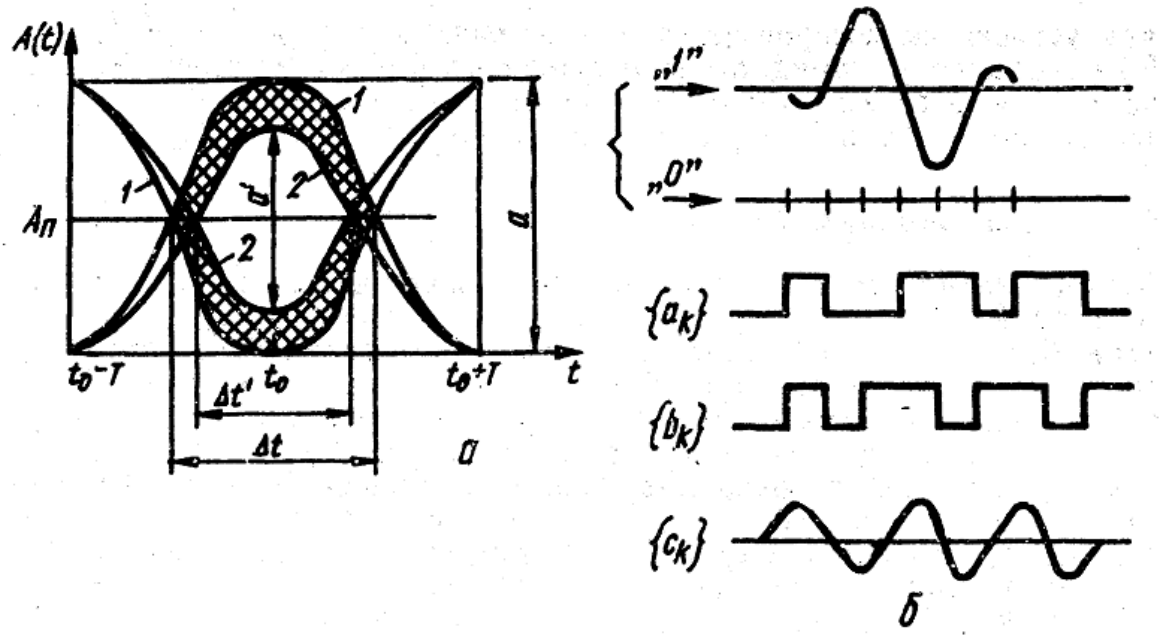


Рисунок 1.2 – Око-діаграма дворівневого (0,1) цифрового сигналу за відсутності (1) та наявності (2) міжсимвольних перешкод:
а – розкрив діаграми ; Δt – ширина діаграми; t_0 – момент стробування послідовності; Т – тимчасовий тактовий інтервал; А – амплітудний рівень, $A_п$ – граничне значення амплітудного рівня сигналу (а) та принцип формування парціально-кодованого цифрового сигналу: «1», «0» - елементи (рівні) сигналу; $\{a_k\}$, $\{b_k\}$, $\{c_k\}$ – вхідна, закодована та вихідна цифрові послідовності відповідно (б).

1.2 Перешкодостійкий код Міллера

Перешкодостійкий код Міллера має досить високу ефективність, має прийнятну якість самосинхронізації, має невелику постійну спектральну складову, а його модифікації (наприклад, код Міллера в квадраті) зовсім не містять постійної спектральної складової. Основний суттєвий недолік коду Міллера полягає в тому, що за період передачі одного символу вихідної інформаційної послідовності необхідно здійснити два рішення про наявність 1 або 0, що знижує його показник стійкості до перешкод [1].

1.3 Блокове кодування

Блокове завадостійке кодування полягає в поділі вихідного інформаційного цифрового потоку на окремі блоки завдовжки k біт і в перетворенні їх у блоки дещо більшої протяжності довжиною у n біт, але які мають кращі завадостійкі властивості. Так, у першому використовуваному телевізійному блоковому коді 8/10 блоки з 8 біт перетворюються на більш довгі блоки по 10 біт і далі відбираються ті 252 збалансованих кодових слова, які містять у своєму складі по п'ять нулів і одиниць. Це дозволяє повністю виключити постійну складову спектрі сигналу.

Недоліки блочного завадостійкого коду 8/10 за його низької ефективності викликають необхідність розширення смуги пропускання каналу приблизно 25 %. Крім того, на кордоні між сусідніми словами можливі цифрові комбінації, що містять десять позицій одиниць і нулів. Внаслідок цього підвищуються вимоги до системи виділення тактової частоти в системі.

Відомою фірмою «Sony» розроблено перешкодостійкий блоковий код 8/8 з ефективністю, що дорівнює 1, який заснований на методі впорядкування кодових цифрових слів та інверсії кожного другого слова. Однак в інформаційній доповіді цієї фірми зазначається, що ступінь

придушення постійної та низькочастотних складових спектру залежить від наявних конкретних статистичних властивостей телевізійного сигналу, що передається, і не завжди виявляється прийнятним. Крім того, якщо у вихідному телевізійному сигналі містяться біти допоміжної інформації або звукових сигналів, то правило кодування, що використовується, повинно бути змінено, тобто запропонований метод не є універсальним. Тому замість завадостійкого коду 8/8 був запропонований новий блоковий код 8/9, який за своїми властивостями є компромісом між кодом 8/10 і високоефективним кодом 8/8 [6].

1.4 Парціальне завадостійке кодування

Парціальне завадостійке кодування застосовується в системах зв'язку порівняно недавно. При такому вигляді кодування спеціально вводиться в послідовність міжсимвольна інтерференція, в результаті чого імпульси, що передаються займають не один, а два або більше тактових часових інтервалів, тобто рівні у різних часових тактах будуть корельованими. Іноді таке кодування у літературі називають корелятивним. Крім того, після кодування зростає число рівнів сигналу, що передається в порівнянні з вихідним інформаційним двійковим сигналом, що призводить до підвищення відношення сигнал-шум для отримання необхідної ймовірності помилки. У той же час, при цьому вдається отримати бажаний «смушковий» спектр кодової послідовності з малим рівнем НЧ і спектральних ВЧ складових, а також істотно підвищити ефективність використання смуги частот, що визначається ставленням швидкості передачі інформації до смуги частот пропускання системи.

Методи парціального завадостійкого кодування передбачають такі операції: скремблювання, попереднє кодування (передкодування) та парціальне кодування.

Призначення попереднього кодування ось у чому. Внаслідок того, що рівні в сигналі, що передається, корельовані в різних тактових часових інтервалах, то одна помилка при передачі може призвести до помилкового декодування інших елементів кодової послідовності. Щоб уникнути подібного поширення помилок, вихідний інформаційний цифровий сигнал перекодується. Передаточна функція передкодеру така:

$$H(D)=1/K(D) \bmod 2, \tag{1.1}$$

де *K (D)* — передатна функція парціального кодеру, яка описується в загальному випадку виразом:

$$K(D)=\sum_{k=0}^{N} h_k D^k , \tag{1.2}$$

де h_k – цілі числа (зазвичай використовуються два ненульові числа h_k;

D – оператор затримки кодової цифрової послідовності на один такт або один інформаційний біт.

Системи парціального завадостійкого кодування поділяються на кілька класів, кожен із класів характеризується сукупністю коефіцієнтів h_k. У пристроях запису інформації поширене парціальне кодування, для якого h_k = 1,0 – 1 ($k = \overline{0,2}$). У цьому випадку передавальні функції передкодеру та кодеру рівні відповідно:

$$H(D)=1/(1 - D^2) \bmod 2, \tag{1.3}$$

$$K(D)=(1 - D^2). \tag{1.4}$$

Попереднє кодування реалізується шляхом підсумовування за модулем 2 коду БВН та вихідного коду, затриманого на два тимчасові такти:

$$b_n = a_n \oplus b_{n-2}, \tag{1.5}$$

де a_n, b_n — відповідно біти вхідної інформаційної та передкодованої послідовності; $\oplus$ — знак підсумовування за модулем 2. Парціальне завадостійке кодування здійснюється відніманням з передкодованого сигналу його копії, яка затримана на два такти. Передатна функція парціального кодеру записується як:

$$K(j\omega) = 1 - \exp(j2\omega T), \tag{1.6}$$

де T — тривалість часово такту.

Модуль коефіцієнту передачі

$$\left|K(j\omega)\right| = \left|2\sin \omega T\right|, \tag{1.7}$$

тобто спектр сигналу на виході кодеру буде мати нулі на нульовій частоті та на частотах, які кратні 1/2T. Після парціального кодеру включається низькочастотний фільтр зі смужкою пропускання 1/2T. Таким чином, спектр цифрової послідовності імпульсів, що передається, обмежений частотою Найквіста, що дозволяє реалізувати передачу інформації зі швидкістю 2 біт/Гц.

Процес формування сигналів у системі парціального кодування пояснюється рис. 1.2, на якому представлені вхідна $\{a_k\}$, перекодована $\{b_k\}$ і вихідна $\{c_k\}$ цифрові послідовності. З наведених на рис. 1.3 спектрів перешкодостійкого парціального коду, а також коду 8/10 і коду Міллера в квадраті (M^2) можна зробити висновок, що спектр парціального коду є більш компактним (він має менший рівень НЧ та ВЧ компонент) і краще узгоджується з амплітудно-частотним каналом.

На рис. 1.3 наведено нормовані енергетичні спектри, що усереднені по всьому ансамблю кодованих цифрових послідовностей. У реальному телевізійному зображенні у вигляді цифрових послідовностей можуть

зустрітися однорідні поля, при яких спектри кодів 8/10 і M^2 мають більш інтенсивні компоненти НЧ або ВЧ, ніж представлені на рис. 1.3 [7]. У той же час отримані спектри парціального коду за будь-яких телевізійних сюжетів не виходять за межі «синусної» характеристики.

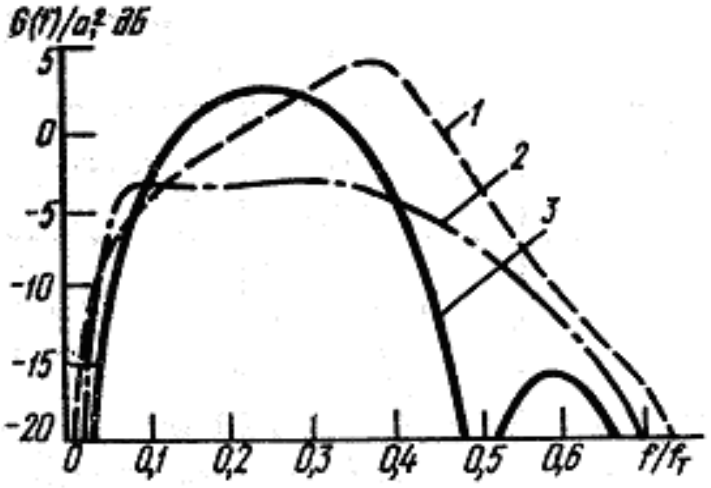


Рисунок 1.3 – Енергетичні спектри кодів:
M^2 -(1), 8/10 -(2) і парціального (3);
$G(f)/a^2$ – спектральна щільність сигналів, нормована до розкриття очей-діаграми

Особливість використання парціального завадостійкого кодування в технічних пристроях полягає в тому, що передкодування здійснюється під час запису, а парціальне кодування - при відтворенні. При цьому на запис надходить дворівневий сигнал, а багаторівневий (у даному випадку трирівневий 1, 0 - 1) формується при відтворенні після парціального кодеру. Це в загальному випадку не знижує завадозахищеності, але вимагає усунення постійної складової записуваного сигналу, що досягається зазвичай за рахунок використання скремблювання.

Таким чином, парціально-кодований сигнал формується не при записі, а при відтворенні, тому такий спосіб обробки сигналу часто в літературі називають не кодуванням, а своєрідним методом детектування [2].

1.5 Криптографія та шифрування

1.5.1 Загальні відомості

Вивчення шляхів та методів передачі інформаційних повідомлень, які б не допускали стороннього втручання, називається криптографією. Терміни «шифрування та кодування» позначають перетворення інформаційних повідомлень, які виконуються на стороні, що передає, а терміни дешифрування і декодування — зворотні перетворення, що проводяться на приймальній стороні. Основними причинами використання криптографічних систем під час передачі повідомлень є:

- забезпечення конфіденційності, тобто, запобігання вилучення інформації, що передається з каналу сторонньою особою (підслуховування);

- автентифікація, запобігання впровадженню каналу передачі інформації сторонніми людьми (обманний доступ).

На практиці часто, як у разі виконання електронного пересилання чи договірних переговорів, важливо забезпечити електронний еквівалент письмового підпису. Це необхідно для того, щоб усунути будь-які непорозуміння між відправником та одержувачем інформації щодо того, яке повідомлення було надіслано абонентом і чи було воно взагалі надіслано.

На рис. 1.3 зображено модель криптографічного інформаційного каналу. Повідомлення, або відкритий текст M, шифрується за допомогою певного конвертованого перетворення $E_к$, формуючого шифрований текст $C = E_к(M)$. Отриманий шифрований текст пропускається через незахищений або загальнодоступний інформаційний канал. Після отримання шифрованого повідомлення, його вихідне або початкове значення відновлюється за допомогою операції дешифрування, яке описується зворотним перетворенням $D_к = E_к^{-1}$, представленим так [8]:

$$D_k(C) = E_k^{-1}[E_k(M)] = M \ . \qquad (1.8)$$

Параметром К позначається безліч символів або характеристик, званих ключем, який визначає конкретне перетворення, що шифрує перетворення $E_к$ із заданого сімейства криптографічних перетворень. Спочатку захищеність криптосистем залежала від секретності всього виробленого процесу шифрування, але зрештою було розроблено такі інформаційні системи, котрим загальна природа процесу шифрування чи алгоритму могла бути загальновідома, а секретність інформаційної системи залежала від спеціального ключа. Ключ використовувався для шифрування вихідного нешифрованого повідомлення, так і для дешифрування шифрованого повідомлення. У більшості криптосистем кожен абонент, який має доступ до ключа, може виконувати як шифрування, так і дешифрування повідомлення. Ключ передається абонентам та авторизованим користувачам через деякий секретний канал; ключ, як правило, залишається незмінним протягом певного часу та значної кількості передач. Метою криптоаналітика (супротивника) є оцінка відкритого вихідного тексту М за допомогою аналізу наявного шифрованого тексту, отриманого із загальнодоступного каналу, без використання ключа [9].

Схеми виконання шифрування можна розділити на дві основні категорії: блокова процедура та шифрування потоку даних, або просто потокове шифрування. При блоковому вигляді шифрування нешифрований текст ділиться деякі блоки фіксованого розміру, після чого кожен отриманий блок шифрується незалежно. Отже, однакові блоки відкритого тексту за допомогою наявного даного ключа будуть перетворюватися на однакові блоки шифрованого тексту (подібно до блокового завадостійкого кодування).

При поточному методі шифрування (подібного згорткового кодування) блоків фіксованого розміру не існує. Кожен біт відкритого тексту m_i, шифрується за допомогою деякого i-го елементу k_i послідовності символів (так званого ключового потоку), що генерується ключем. Процес шифрування в цьому випадку є періодичним, якщо ключовий потік починає

повторюватися після *p* символів (причому *p* фіксовано); в іншому випадку процес шифрування є неперіодичним.

Процедура шифрування істотно відрізняється від схеми канального кодування. Наприклад, при шифруванні дані відкритого інформаційного тексту не повинні явно фігурувати в шифрованому тексті, а при канальному завадостійкому кодуванні в систематичній формі коди часто містять незмінені біти вихідного інформаційного повідомлення плюс біти парності.

Існують і інші відмінності шифрування та канального завадостійкого кодування. При блочному методі шифрування єдиний біт помилки на вході дешифратора може змінити значення багатьох вихідних бітів у блоці. Цей ефект, відомий як накопичення помилки (error propagation), часто є на практиці бажаною криптографічною властивістю, оскільки для несанкціонованих користувачів створює додаткові серйозні складності при розшифровці отриманих повідомлень. У той же час при канальному завадостійкому кодуванні така властивість є небажаною, оскільки бажано, щоб система виправила якнайбільшу кількість помилок і на вихідну інформацію вхідні помилки впливали якнайменше [10].

1.5.2 Завдання системи шифрування

Основні вимоги до систем шифрування інформаційних повідомлень можна сформулювати так:

- необхідно забезпечити *прості та недорогі* засоби шифрування та дешифрування для авторизованих користувачів, які мають відповідний ключ;

- бажано завдання криптоаналітика з виробництва оцінки нешифрованого тексту у разі відсутності ключа зробити *якомога складнішим і найдорожчим.*

Послідовно хронологічно криптосистеми, що створюються, поділяються на *безумовно захищені* або схеми, *захищені за обчисленнями*. При цьому мають на увазі, що *система безумовно захищена*, якщо інформації, яка є у криптоаналітика, недостатньо для визначення властивостей перетворень шифрування та дешифрування, незалежно від того,

яку обчислювальну потужність він (криптоаналітик) має. Одна з таких інформаційних систем, яка називається системою *разового заповнення*, включає шифрування повідомлення за допомогою випадкового ключа, який може застосовуватися тільки один раз. Такий ключ ніколи не використовується повторно; отже, криптоаналітик не отримує необхідної інформації, яка може використовуватися для розшифрування наступних повідомлень, отриманих при використанні того ж ключа. Незважаючи на те, що така система є безумовно захищеною, у системах зв'язку вона застосовується порівняно рідко, оскільки для кожного нового повідомлення необхідно розповсюдити новий ключ, а це зазвичай дуже важко [10].

Взагалі, розподіл ключів авторизованим користувачам системи є основною проблемою при використанні будь-якої криптосистеми, навіть якщо отриманий ключ застосовується протягом досить тривалого періоду часу. Хоча й можна показати, що деякі інформаційні системи є безумовно захищеними, загальної процедури доказу захищеності довільної криптосистеми наразі не існує. Таким чином, при описі більшості криптосистем вказується, що вони захищені за обчисленням на *x* років; це означає, що за деяких обставин, сприятливих для криптоаналітика (тобто при використанні найсучасніших та продуктивних комп'ютерів), захист системи може бути зламаний за *x* років, але не раніше.

1.5.3 Класичні погрози

Найменша нині криптоаналітична загроза - це *атака шифрованого тексту* (ciphertext-only attack). При використанні цього методу криптоаналізу криптоаналітик може мати деяку вихідну інформацію про загальну інформаційну систему та мову, що використовується в повідомленні, але єдиними суттєвими даними, що є у нього, є шифроване повідомлення, яке було перехоплено із загальнодоступного каналу.

Більш серйозною загрозою криптосистеми є *атака відомого відкритого тексту* (known plaintext attack). Ця атака включає знання відкритого тексту, а також і його шифрованого еквівалента. Жорстка

структура більшості бізнес-форм та мов програмування часто дає опоненту певну кількість апріорних відомостей про елементи відкритого повідомлення. Збройний цими даними та шифрованим повідомленням, криптоаналітик може проводити криптоаналіз з використанням відомого відкритого тексту. Незважаючи на те, що атака відомого заздалегідь відкритого тексту не завжди можлива, вона використовується практично досить часто, щоб система не вважалася захищеною, якщо вона не призначена для протистояння такому типу атак.

Якщо криптоаналітик повинен вибирати вихідний відкритий текст для цього шифрованого повідомлення, то загроза називається *атакою вибраного відкритого тексту* (chosen plaintext attack).

2 МЕТОДИ СКРЕМБЛЮВАННЯ ПОВІДОМЛЕНЬ

2.1 Загальні відомості

Скремблювання інформаційних повідомлень може виконуватись з різними цілями. Найбільш поширена мета скремблювання - захист інформаційних даних, що передаються від несанкціонованого доступу. Для її досягнення розроблено безліч відомих методів кодування та відповідних схемних рішень. Але найбільш цікавою для практики є інше завдання, пов'язане з «розрівнюванням» спектра сигналу, що передається, і підвищенням синхронізації приймального пристрою з джерелом даних, що передаються по лінії зв'язку.

Стосовно даної актуальної задачі мета скремблювання полягає у виключенні з потоку інформаційних даних досить довгих послідовностей логічних нулів, логічних одиниць і груп бітів, що періодично повторюються [2,6]. Щоб це забезпечити необхідно перетворити вихідні дані так, щоб вони були як випадкові, тобто. позбавлені будь-якої певної закономірності. При цьому код, що використовується, набуває властивостей, необхідних для цифрового запису: з'являється можливість самосинхронізації пристроїв без введення надлишкових бітів, зменшується рівень постійної складової спектру сигналу і т.п. Скремблювання інформаційних послідовностей може також використовуватися у поєднанні з певним видом канального кодування, наприклад, парціальним кодуванням.

У цифрових системах передачі повідомлень, зокрема, в цифровому телевізійному мовленні, для скремблювання до цифрового сигналу, що передається, іноді додають додатковий сигнал, в якості якого прийнято використовувати псевдовипадкові послідовності (ПВП).

Ці псевдовипадкові послідовності складаються з чисел, зокрема - бітів, багато властивостей яких збігаються з властивостями випадкових

сигналів. Нулі та одиниці в ПВП розташовані на перший погляд хаотично, але насправді кожна ПСП формується відповідно до певного алгоритму, що залежить від деякої кількості параметрів.

Здійснюється скремблювання інформаційних послідовностей за допомогою операції підсумовування за модулем 2 використовуваного коду з псевдовипадковою послідовністю, що накладається, в якості якої на практиці прийнято використовувати досить вивчені М-послідовності, які мають максимально можливий період довжини рівний

$$L = 2^m - 1,$$

де m — ступінь полінома, що утворює послідовність ПВП.

В Таблиці 2.1 наведено деякі результати розрахунків математичного очікування та кореляційної функції з деяких типових послідовностей.

Таблиця 2.1 Значення математичного очікування та кореляційної функції деяких типових послідовностей

Вид послідовності	M{y}	M{z}	$K_y(\tau)$	$K_z(\tau)$
000…	0	0.5+1/2L	0	-1/L
111…	1	0.5-1/2L	1	-1/L
Випадкова	0.5	0.5	0	0
Довільна	$0 \le M\{y\} \le 1$	$(0.5-1/2L) \le M\{z\} \le (0.5+1/2L)$	$0 \le K_y(\tau) \le 1$	$0 \le K_z(\tau) \le \lvert -1/L \rvert$

В результаті виконання операції скремблювання код БВН наближається за своїми властивостями до випадкового сигналу (він рандомізується), тобто. володіючи невипадковою природою генерування та формування, він відповідає за низькими властивостями псевдовипадкових сигналів.

Справді, ймовірність появи нуля в скрембльованій інформаційній послідовності визначається виразом

$$P_0 = p_0 q_1 + p_1 q_0 , \qquad (2.1)$$

де p_0, p_1 - ймовірності появи нуля та одиниці у вихідній послідовності;

q_0, q_1 — ті ж ймовірності в ПСП, використовуваної для скремблювання.

Оскільки значення ймовірностей рівні $q_0 = q_1 \approx 0{,}5$, то P_0=0,5(p_0+p_1)=0,5, і незалежно від виду вихідної послідовності ймовірності появи символів 0 і 1 в скрембльованому сигналі зводяться до значення ймовірності 0,5.

Для ілюстрації процесу рандомізації послідовностей у табл. 2.1 наведено отримані при розрахунках значення математичного очікування $M\{y\}$ та кореляційної функції $K_y(x)$ для деяких типових послідовностей. Зрозуміло, що дані статистичні характеристики ПСП залежатимуть від довжини періоду використовуваної послідовності і не залежатимуть від виду поліному, що утворює:

$$M\{x\}=0{,}5 + L/2, \qquad (2.2)$$

$$K_x(\tau)= - 1/L, \qquad (2.3)$$

при $T \le \tau \le (L - 1)T$, де T — тривалість тимчасового такту.

З табл. 2.1 слідує, що зазначені параметри $M\{z\}$ і $K_z(\tau)$ скрембльованої послідовності $z = y + x$ (y — вхідна послідовність, x — скремблююча ПВП) наближаються до відповідних параметрів шуканої псевдовипадкової сигнальної послідовності [11].

Для процедури дескремблювання в приймальному пристрої необхідно виконувати формування такої ж ПВП, як і тієї, яка використовувалася для скремблювання на стороні, що передає. З цією метою приймач тим чи іншим способом передають сукупність параметрів алгоритму формування ПВП. Не

маючи сукупності цих структурних параметрів, неможливо здійснити дескремблювання прийнятого сигналу.

Скремблювання сигналу шляхом складання послідовності за модулем 2 з ПВП застосовується в стандарті DVB (Digital Video Broadcasting) і деяких випадках, коли обмеження доступу не потрібно, тобто під час використання безкоштовних ТБ-програм. Це пов’язано з тим, що таке скремблювання наближає властивості переданого інформаційного сигналу властивостям шуму. При цьому енергія сигналу більш рівномірно розподіляється по смузі частот каналу, що забезпечує ефективніше використання інформаційного каналу зв'язку та підвищення стійкості до перешкод. Відповідно, у приймальному пристрої необхідно виконувати процес дескремблювання [11].

2.2 Перемежування

Одним із найбільш ефективних методів зменшення впливу пакетних помилок, що часто зустрічаються на практиці, є перемежування або перемішування (англ. interleaving) інформаційної послідовності. Дані послідовності, перед передачею каналом зв'язку, переставляються в заданому порядку, але в приймальній частині тим чи іншим шляхом вони відновлюються у вихідний порядок, тобто, виконується операція деперемежування. Внаслідок цього пакетні помилки, що виникають у каналі зв'язку, перетворюються на набір розосереджених на часової осі одиночних помилок, які значно простіше виявляються і виправляються з використанням відомих кодів, що виправляють такі помилки [11].

Приклад операцій перемежування та деперемежування показаний на рис. 2.1. Вихідний інформаційний цифровий сигнал є послідовністю 4-розрядних двійкових слів, які передаються біт за бітом (рис. 2.1, а). Перемежування здійснюється у межах кожного з чотирьох слів, тобто, у межах відрізків цифрового інформаційного сигналу, що включає 16 біт.

Числа показують номери бітів у цьому часовому відрізку. У результаті операції перемежування біти переставляються в такий спосіб (рис. 2.1,б). Біти, спотворені внаслідок дії пакетної помилки, відмічені зірочками. В результаті виконання деперемежування (рис. 2.1, в) відбувається відновлення вихідного порядку бітів та спотворені біти розосереджуються за послідовністю.

Переставлятися можуть як окремі біти послідовності, а й групи бітів, наприклад, байти. У стандартах цифрового телебачення DVB операція перемежування здійснюється в межах пакетів транспортного цифрового потоку після кодування методом Ріда-Соломона, в результаті якого обсяг інформаційних пакетів збільшується з 188 до 204 байтів. Кожен цифровий пакет розбивається на 12 окремих груп по 17 байтів. Спочатку виконується передача перших байт всіх груп, тобто байти з номерами 1, 18, ..., 171, 188, потім передаються другі байти груп: 2, 19, ..., 172, 189 і т.д. Наприкінці передаються останні байти груп, з номерами 17, 34, ..., 187, 204. Таким чином, у процесі виконання перемежування різні байти послідовності зміщуються на відстані від 0 до 176 позицій у межах пакета цифрового транспортного потоку. У приймальній частині відновлюється вихідний порядок проходження байтів послідовності.

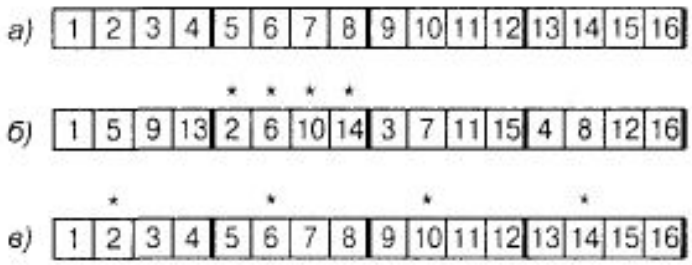


Рисунок 2.1 – Операції перемежування та деперемежування

Операцію перемежування можна використовувати також для виконання шифрування сигналу, що передається, так як відновлення правильного порядку символів можливе тільки при знанні закону і порядку перестановки [12].

2.3 Розширення спектру

Методи розширення спектру сигналу отримали назву внаслідок того, що смуга частот, яка використовується для передачі сигналу, набагато ширша за мінімальну смугу, необхідну для передачі даних. Відповідна система зв'язку називається системою з розширеним спектром сигналу у таких випадках:

- використовувана смуга частот значно ширше мінімально необхідної смуги передачі даних;

- розширення спектру сигналу здійснюється за допомогою розширюючого (або кодового) спеціального сигналу, який не залежить від інформації, що передається;

- відновлення вихідної послідовності даних приймальним пристроєм ("звуження спектру") здійснюється шляхом зіставлення отриманого інформаційного сигналу і синхронізованої копії розширюючого спектр сигналу.

Розширення спектру також відбувається при використанні деяких схем модуляції сигналу, таких як частотна та імпульсно-кодова види модуляції. Однак ці схеми взагалі не відносяться до методів розширеного спектру, оскільки не задовольняють усім наведеним вище умовам [10].

Розглянемо переваги систем зв'язку розширеного спектра стосовно придушення перешкод. Як відомо, білий гаусів шум — це математична модель шуму з нескінченно великою потужністю, яка рівномірно розподілена по всьому спектру частот. Наявність такого шуму в каналі не обов'язково означає відсутність ефективного зв'язку, оскільки інтерферувати з сигналом можуть лише складові шумові обмеженої потужності. Інші складові шуму ефективно відсіваються частотними пристроями. Для типового цифрового

відеосигналу це означає, що характеристики зв'язку погіршуються тільки шумами, що знаходяться в діапазоні частот сигналу [10].

2.4 Псевдовипадкові послідовності

Системи зв'язку з розширеним спектром при передачі опорного сигналу (transmitted reference - TR) можуть використовувати випадковий кодовий сигнал для операцій розширення та звуження спектру, оскільки кодовий сигнал і модульований даними кодовий сигнал одночасно передаються в різних областях спектру. Метод збереження опорного сигналу (stored reference - SR) не дає можливості використовувати суто випадкові кодові сигнали, оскільки код зберігається або генерується приймачем. У системах SR повинен обов'язково застосовуватися псевдошумовий (pseudonoise) або псевдовипадковий (pseudorandom) кодовий допоміжний сигнал.

У чому полягає відмінність псевдовипадкового від істинно випадкового кода? Випадкова цифрова послідовність непередбачувана і описується у статистичному сенсі. Псевдовипадковий код насправді не випадковий — це по суті детермінований періодичний сигнал. Псевдовипадковим він називається лише тому, що його статистичні властивості збігаються з дискретним білим шумом. Для звичайного користувача такий сигнал здаватиметься суто випадковим.

При випробуваннях цифрових лінійних трактів та вимірі в них коефіцієнтів помилок як випробувальні цифрові сигнали в них використовуються псевдовипадкові послідовності (ПВП). Рекомендаціями МККТТ визначено, що як випробувальний сигнал для первинних та вторинних цифрових трактів може бути ПСП з періодом повторення 215 – 1, а для третинних та чотирирічних – з періодом 223 – 1.

ПВП в цифрових інформаційних системах передачі використовуються також як спеціальні сигнали дисперсії для рандомізації

(надання випадкового характеру) переданого цифрового сигналу, виключення дискретних складових у спектрі та поліпшення умов виділення тактової частоти.

ПВП можуть використовуватися для шифрування повідомлень, можуть також застосовуватися як адресні та синхронізуючі сигнали, застосовуються також як квазішумоподібні сигнали в системі закритого зв'язку і в системах, що мають режим багатостанційного доступу і поділу сигналів за формою, в радіолокаційних системах далекометрії і т.п. [10].

2.5 Властивості псевдовипадкових послідовностей

Які властивості повинен мати псевдовипадковий код, щоб бути справді випадковим? Існує три основні властивості періодичної бінарної цифрової послідовності, які можна використовувати для перевірки на випадковість.

1. ***Збалансованість.*** Для кожного часового інтервалу послідовності кількість двійкових одиниць у ньому повинна відрізнятись від числа двійкових нулів не більше ніж на один символ.

2. ***Циклічність. Циклом*** називається безперервна послідовність однакових двійкових чисел. Поява іншої двійкової цифри у послідовності починає новий цикл. Довжина циклу дорівнює кількості цифр у послідовності. Бажано, щоб у кожному фрагменті цифрової послідовності приблизно половину її становили цикли обох типів довжиною 1, приблизно одну чверть протяжністю або довжиною 2, приблизно одну восьму протяжністю 3 і т. п.

3. ***Кореляція***. Якщо деяку частину цифрової послідовності та її циклічно зрушена копія поелементно порівнювати, то бажано, щоб кількість збігів відрізнялася від числа розбіжностей не більше ніж на одиницю.

Широке застосування практично ПВП зумовлено і простотою їх генерації.

Формувач ПВП являє собою послідовний регістр (регістр зсуву), який охоплений логічним зворотним цифровим зв'язком. Хоча ПВП за своїми властивостями наближається до випадкового цифрового сигналу, вона все ж таки є детермінованою, періодичною цифровою послідовністю. Період її повторення та структура ПВП визначаються довжиною регістра зсуву, що використовується в генераторі та видом функції зворотного зв'язку. Найбільший період послідовності ПВП, що генерується n-розрядним регістром зсуву, становить $M = 2^n - 1$ символів. У такій псевдовипадковій послідовності зустрічаються всі можливі поєднання n символів (включаючи серію символів n одиниць поспіль) [10].

2.6 Автокореляційна функція ПВП

Автокореляційна функція $R_x(\tau)$ періодичного сигналу $x(t)$ з періодом повторення T_0 записана нижче у нормованій математичній формі:

$$\mathrm{R}_{\mathrm{x}}(\tau) = \frac{1}{K}\left(\frac{1}{T_0}\right)\int_{-T_0/2}^{T_0/2} x(t)x(t+\tau)dt\,, \qquad (2.4)$$

де

$$\mathrm{K} = \frac{1}{T_0}\int_{-T_0/2}^{T_0/2} x^2(t)dt\,. \qquad (2.5)$$

Якщо сигнал $x(t)$ є періодичний імпульсний сигнал, що є псевдовипадковим кодом, то кожен з елементарних імпульсів такого сигналу називають ***кодовим символом*** (code symbol) або ***елементарним сигналом*** (chip). Нормована автокореляційна функція псевдовипадкового цифрового сигналу при одиничній тривалості елементарного сигналу і періодом повторення елементарних сигналів може бути записана в наступному вигляді:

.

$$R_x(\tau) = \frac{1}{p} \quad . \tag{2.6}$$

Графік нормованої автокореляційної математичної функції послідовності максимальної довжини $R_x(\tau)$ представлен на рис. 2.2. Зрозуміло, що для значення τ = 0, коли сигнал *x(t)* та його копія ідеально збігаються, функція автокореляції R(τ) = 1. За будь-якого циклічного зсуву між послідовностями *x(t)* і x(t + τ) при (1 ≤ τ < p) автокореляційна функція дорівнюватиме -1/p (для великих значень параметру p дві послідовності практично декорельовані між собою при зрушенні на один елементарний сигнал).

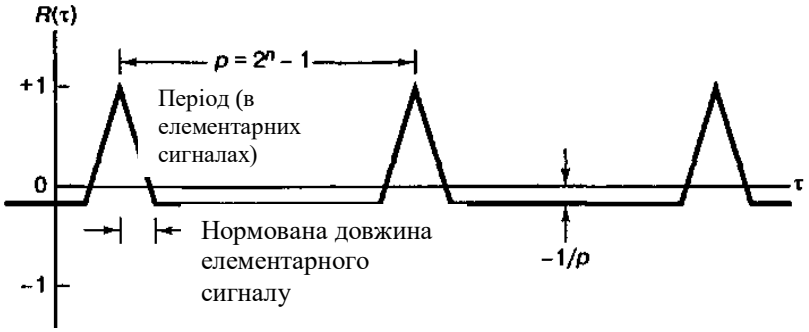


Рисунок 2.2 – Автокореляційна функція псевдовипадкової цифрової послідовності

Виконаємо перевірку якості кореляції для псевдовипадкової послідовності, згенерованої показаним регістром зсуву на рис.2.3.

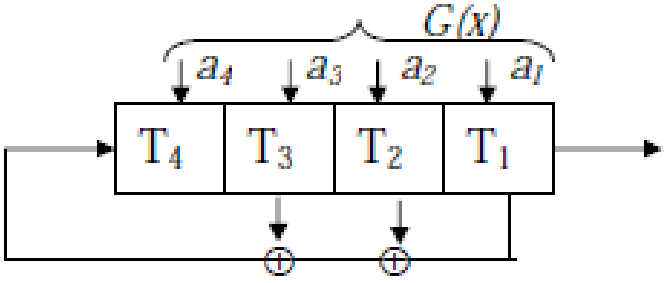


Рисунок 2.3 – Приклад лінійного регістру зсуву зі зворотним зв'язком

Припустимо, що цифровий розряд X_1 містить одиницю, проте інші розряди є нулями, тобто. початковий стан регістру 1000. Відповідно до змісту рис. 2.3, наступні стани регістру зсуву будуть такими:

1000 0100 0010 1001 1100 0110 1011 0101

1010 1101 1110 1111 0111 0011 0001 1000

Оскільки останній стан регістра 1000, ідентично початковому стану, можна бачити, що наведена цифрова послідовність повторюється на виході регістра через кожні 15 тактів. Вихідна послідовність регістру визначається вмістом розряду X_4 на кожному такті зсуву. Ця цифрова послідовність матиме такий вигляд:

000100110101111.

Вихідна послідовність та її модифікація зі зрушенням на один регістр вправо така

0	0	0	1	0	0	1	1	0	1	0	1	1	1	1
1	0	0	0	1	0	0	1	1	0	1	0	1	1	1
d	*a*	*a*	*d*	*d*	*a*	*d*	*a*	*d*	*d*	*d*	*d*	*a*	*a*	*a*

Збіг цифр у послідовності позначено символом **a**, а розбіжність — символом **d**. Відповідно до рівняння (2.6) автокореляційна функція сигналу при подібному зрушенні на один елементарний символ така:

$$\mathrm{R}(\tau = 1) = \frac{1}{15}(7 - 8) = -\frac{1}{15}.$$

Будь-яке циклічне зрушення, що призводить до відхилення від ідеальної синхронізації, забезпечує значення автокореляційної функції. Отже, третю властивість псевдовипадкової послідовності в даному випадку обов'язково буде виконано [10].

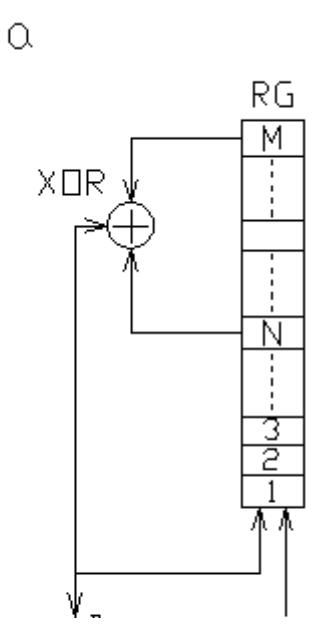
2.7 Генератори псевдовипадкових бітових послідовностей

Скремблери та дескремблери інформаційних систем зазвичай побудовані на основі генераторів псевдовипадкових бітових послідовностей. Один із прикладів такого генератора наведено на рис. 2.4. Цей генератор виконаний з використанням кільцевого регістру зсуву RG з логічним елементом Виключне АБО (XOR), включеним в ланцюги зворотного зв'язку. Якщо у вихідному стані в регістрі є деякий ненульовий код, то під дією синхросигналу CLK ця послідовність буде безперервно циркулювати в регістрі і одночасно видозмінюватися. Як вихід генератора ПВП можна використовувати вихід будь-якого іншого розряду даного регістру зсуву.

Загалом у М-розрядному регістрі зсуву зворотний логічний зв'язок підключається до розрядів з номерами M і N (M > N). Вибір оптимального значення N для заданого числа M дуже непросте завдання.

Варіант таблиці вибору значення N наведено на рис. 2.4. Ця таблиця визначає сукупність генераторів різної розрядності. Кожен генератор буде формувати послідовність бітів з максимальним періодом повторення, що дорівнює 2^M- 1. У такій цифровій послідовності зустрічаються всі М-розрядні коди, крім чисто нульового коду. Такий код є своєрідною «пасткою» для даної структурної схеми: якщо нульовий код з'явиться в регістрі зсуву, то подальша послідовність бітів буде тільки нульовою. При нормальній роботі генератора зсуву потрапляння в пастку зазвичай немає.

Послідовність максимальної довжини має ряд таких властивостей. У повному циклі (2^M – 1 тактів) число логічних одиниць на одну одиницю більше, ніж число логічних нулів. Додаткова логічна одиниця з'являється внаслідок виключення стану, при якому в регістрі є нульовий код. Це можна інтерпретувати так, що ймовірності появи на виході регістра логічного нуля та логічної одиниці практично однакові.



b

M	N
3	2
4	3
5	3
6	5
7	6
9	5
10	7
11	9
15	14
17	14
18	11
20	17
21	19
22	21
23	18
25	22
28	25
29	27
31	28
33	20
35	33
36	25
39	35

а) б)

Рисунок 2.4 – Формувач псевдовипадкової послідовності максимальної довжини:

а - схема; б - таблиця для вибору точки підключення зворотного зв'язку

У повному циклі (2^M-1 тактів) половина серій із послідовних лог. 1 має довжину 1, одна четверта серій -довжину 2, одна восьма - довжину 3 і т.п. Такі ж властивості мають і серії з лог. 0 з урахуванням пропущеного лог. 0. Це говорить про те, що ймовірність появи «орлів» і «решічок» не залежить від результатів попередніх «підкидань». Тому ймовірність того, що серія з послідовних лог. 1 або лог. 0 закінчиться при наступному підкиданні, що дорівнює 1/2 всупереч обивательському розумінню «закону про середнє».

Якщо послідовність повного циклу (2^M-1 тактів) порівнювати з цією ж послідовністю, але циклічно зрушеною на будь-яке число тактів W (W не є нулем або числом, кратним 2^M-1), то кількість розбіжностей буде на одиницю більша, ніж кількість збігів.

Найбільш поширені дві основні схеми побудови пар «скремблер-дескремблер»: з неізольованими та ізольованими генераторами

псевдовипадкових бітових послідовностей. Розглянемо ці схеми та його модифікації [5].

2.8 Скремблер та дескремблер з неізольованими генераторами псевдовипадкових послідовностей

На рис. 2.5 наведено структурні схеми скремблера та дескремблера, які виконані на основі генераторів псевдовипадкових бітових послідовностей. Обидва генератори ПВП мають однакову розрядність та однотипні види структур зворотних зв'язків. Процеси, які у інформаційної системі передачі, синхронізуються одним тактовим генератором (він на рисунку не показаний). Цей генератор розміщений на стороні, що передає, і входить до складу джерела даних або скремблера. На кожному часовому такті на вхід скремблера подається біт даних SD, а в зсувному регістрі RGI сформований код зсувається на один розряд вправо.

Якщо припустити, що джерело даних посилає в скремблер довгу логічні послідовність 0, то елемент структури XOR1 слід розглядати як повторювач сигналу Y1 з виходу елемента XOR2. У цій ситуації регістр зсуву RG1 замкнутий в кільце і генерує таку ж псевдовипадкову послідовність бітів, як і в розглянутій схемі, представленої на рис. 2.4. Якщо джерело даних видає довільну бітову послідовність, вона взаємодіє з послідовністю бітів на виході XOR2. В результаті буде сформовано нову (скрембльовану) послідовність бітів SCRD, за структурою дуже близьку до випадкової. Ця послідовність далі просувається регістром зсуву RG1, формуючи потік бітів на виході елемента структури XOR2.

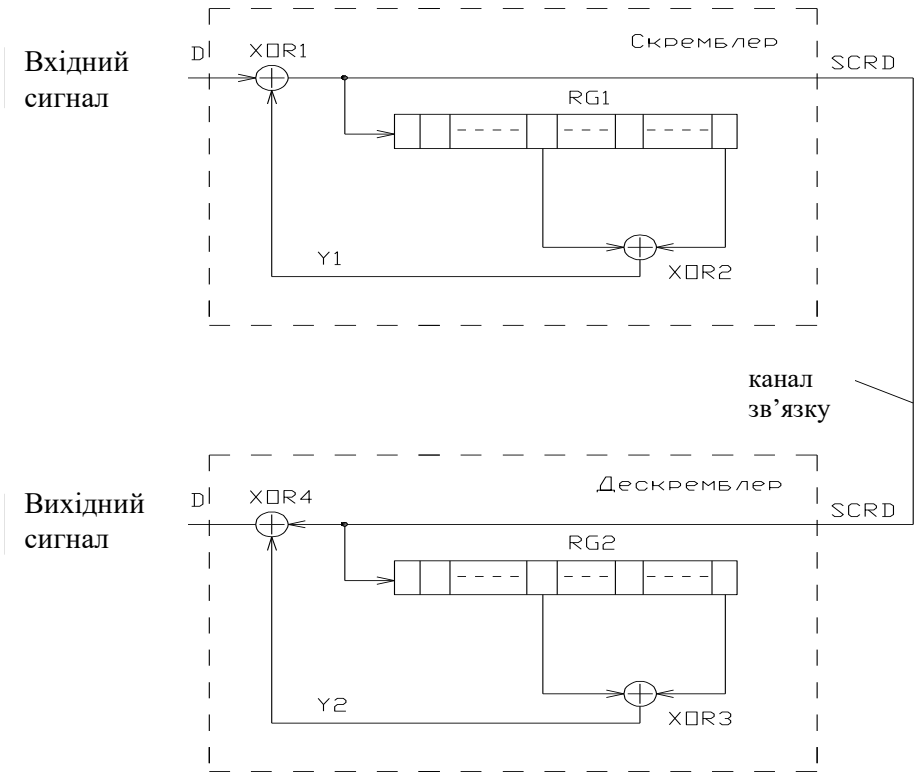


Рисунок 2.5 – Система передачі інформації, в якій скремблер та дескремблер включають неізольовані генератори ПВП

Скрембльована послідовність бітів SCRD передається далі по каналу зв'язку і надходить у дескремблер. За допомогою генератора з фазовим автопідстроюванням частоти (цей генератор на рисунку не показаний) з вхідного сигналу виділяється деякий тактовий сигнал. Під управлінням отриманого тактового сигналу біти послідовності SCRD просуваються в регістрі RG2, а в приймальний пристрій даних надходять дескрембльовані символи RD.

Потоки даних послідовностей RD і SD збігаються з точністю до затримки передачі лінії зв'язку. У режимі в зсувних регістрах RG1 і RG2 присутні однакові коди, оскільки на входи цих регістрів подано одні і ті ж дані символів SCRD, а тактова частота є загальною. Тому послідовності Y2 = Y1, і далі маємо RD = SCRD $\oplus$ Y2 = SD $\oplus$ Y1 $\oplus$ Y2 = SD $\oplus$ Y1 $\oplus$ Yl = SD $\oplus$ 0 = SD.

Розглянута система передачі не вимагає застосування будь-якої спеціальної процедури початкової синхронізації. Після заповнення символами зсувного регістру RG2 генератори псевдовипадкових бітових послідовностей працюють практично синхронно та їх стани завжди будуть однаковими. При появі одиночної помилки лінії зв'язку синхронізація нетривале порушується, але потім автоматично відновлюється, оскільки правильні дані знову заповнять регістр зсуву RG2.

Однак у процесі просування помилкового біта по зсувному регістру RG2, у періоди часу його потрапляння спочатку перший, а потім другий вхід елемента XOR3 сигнал Y2 двічі приймає неправильне значення. Внаслідок цього відбувається розмноження одиночної помилки - вона з'являється в сигналі RD в момент надходження з лінії зв'язку і потім виникає ще два рази при наступному дворазовому спотворенні сигналу Y. Ще один недолік суттєвий розглянутої системи передачі даних обумовлений тим, що є деякі несприятливі кодові ситуації, з якими скремблер "не може впоратися" [5].

2.9 Скремблер-дескремблер із ізольованими генераторами ПВП

У схемі, розглянутій на рис. 2.6 генератори ПВП включені так, що вони ізольовані від будь-яких небажаних зовнішніх перешкодових впливів. Генератори, як і в розглянутій раніше попередній схемі, працюють практично синхронно, тому скремблюючий Z1 і дескремблюючий Z2 сигнали будуть однакові. Помилки лінії зв'язку не розмножується дескремблером, і вони потрапляють у зсувний регістр RG2. Недолік цієї схеми - відсутність самосинхронізації генератора псевдовипадкової бітової послідовності дескремблера (у попередній схемі така синхронізація є) [5].

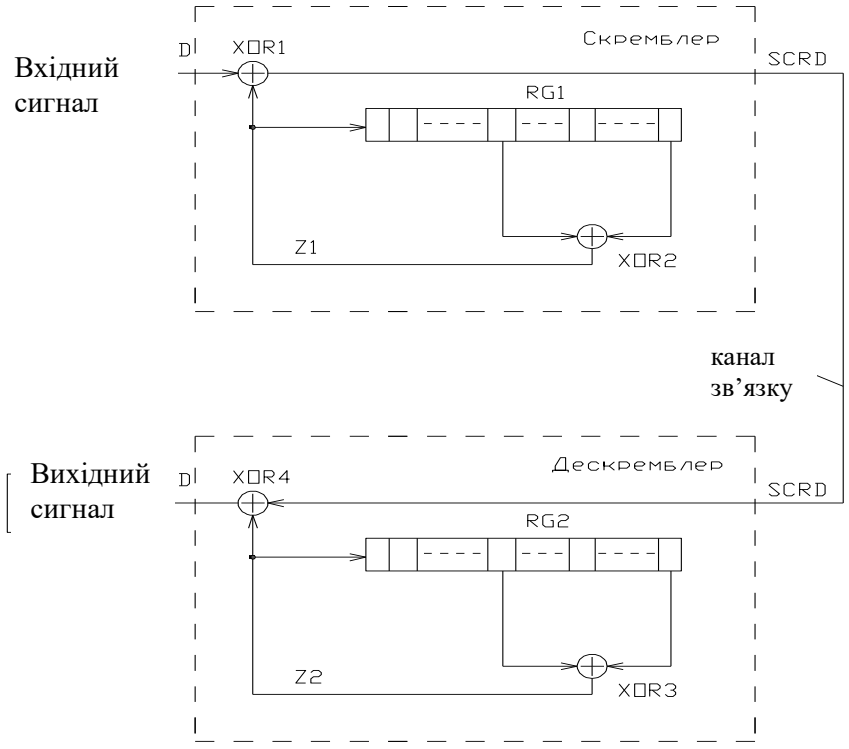


Рисунок 2.6 – Система передачі даних, в якій скремблер та дескремблер містять ізольовані генератори ПВП

2.10 Адаптивний скремблер з ізольованим генератором псевдовипадкових бітових послідовностей

Навіть при виконанні операції скремблювання повністю уникнути на практиці довгих послідовностей 1 або 0 у вихідному сигналі скремблера не вдається, внаслідок того, що у вихідному коді можуть бути фрагменти, які повністю збігаються з ПСП генератора М-послідовності або протилежні їй по фазі. Тому в ряді випадків використовують *адаптивне скремблювання*, при якому структура скремблеру змінюється відповідно до вхідного сигналу таким чином, щоб у перетвореному сигналі мати мінімально довгі послідовності нулів або одиниць.

Структурну схему адаптивного скремблера з паралельним аналізом наведено нижче на рис. 2.7. Вхідний цифровий інформаційний сигнал поділяється на окремі блоки, що необхідно для захисту від помилок, що

виникають, в суматорі ∑1 відбувається підсумовування по модулю 2 з декількома ПВП, після чого підраховується максимальне число однотипних комбінацій з нулів і одиниць кожної отриманої скрембльованої послідовності. За допомогою блоку управління БУ та логічного пристрою ЛУ відбувається вибір кращої ПВП за критерієм мінімуму нулів та одиниць поспіль в отриманому сигналі. При підсумовуванні у суматорі ∑*1* цієї ПВП по модулю 2 з вихідним сигналом, затриманим у блоці УЗБ на час, що дорівнює тривалості блоку, формується вихідна скрембльована послідовність. У такому випадку повністю усунути небажані кодові комбінації теж не можна, але ймовірність їхньої появи стає при цьому дуже незначною, і пристрої виділення тактової частоти сигналу функціонують надійно.

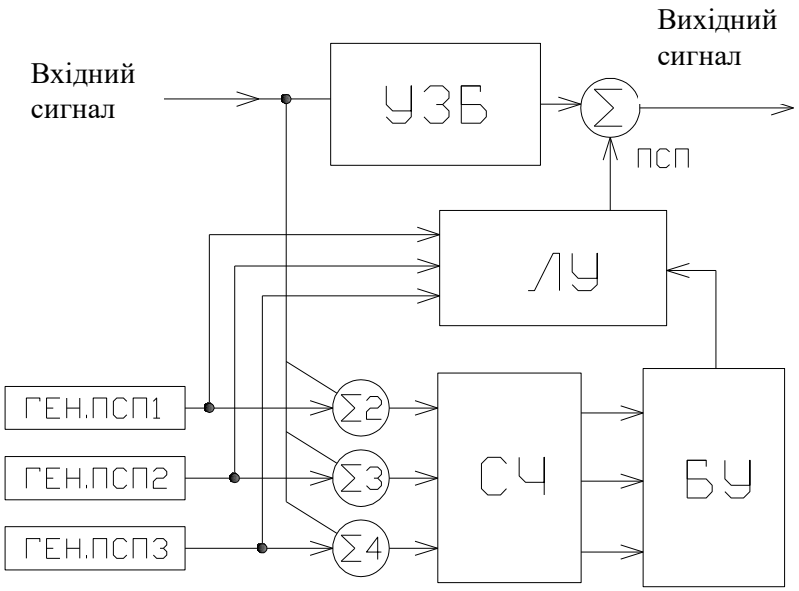


Рисунок 2.7 – Структурна схема пристрою адаптивного скремблювання

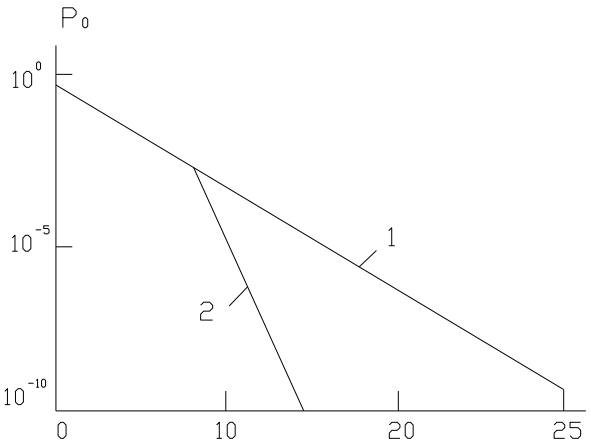
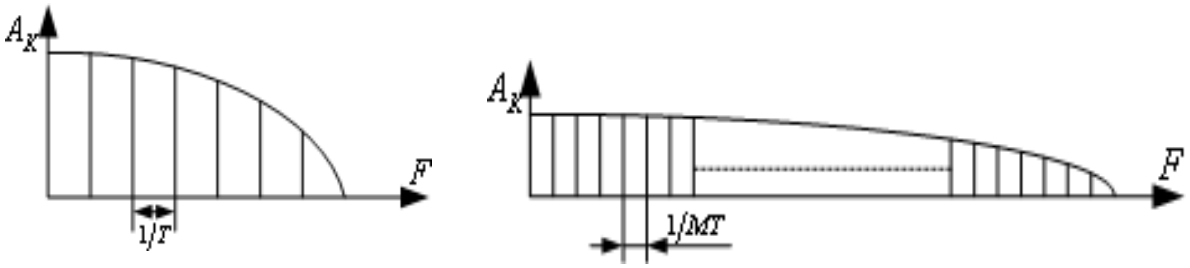


Рисунок 2.8 – Ймовірності появи серій з k нулів для простого (1) та адаптивного (2) пристроїв скремблювання

На рис. 2.8 представлені залежності ймовірностей появи серій з нулів підряд для простого скремблювання (коли до вихідного коду додається М-послідовність) і для адаптивного скремблювання (коли до вихідного коду додається одна з чотирьох М-послідовностей, що логічно вибираються). У першому випадку вихідний цифровий сигнал набуває властивостей псевдовипадкового, в якому ймовірності появи 1 і 0 однакові, внаслідок цього існує ймовірність утворення серії з *k* нулів або одиниць поспіль $P_k = 0,5^k$ (наприклад, при k = 10 $P_{10} = 0,97*10^{-3}$, при k = 15 $P_{15} = 0,3*10^{-4}$**).** У другому випадку внаслідок вибору найбільш підходящої з кількох некорельованих М-послідовностей вдається знизити ймовірність появи довгих однотипних кодових комбінацій. Порядок зменшення залежить від статистичних властивостей вхідного сигналу, властивостей скремблюючої М-послідовності, і навіть від числа М-послідовностей, у тому числі здійснюється вибір. За даними [4], при виборі з чотирьох М-послідовностей ймовірність появи серій з 10 нулів становитиме 10^{-5}, а з 15 нулів - менше 10^{-10}. За таких малих значеннях ймовірностей система виділення тактової частоти сигналу працює практично без значних збоїв [11].

Скремблірування також впливає на енергетичний спектр двійкового сигналу (рис 2.9).



а) б)

Рис. 2.9 - Спектр сигналу:

а) до скремблювання; б) після скремблювання

Після скремблювання інформаційного сигналу ПВП з 2^M-1 елементами спектр сигналу істотно «збагачується» (2.9, б): число складових спектру збільшилося в М разів. А сам спектр становиться більш рівномірним.

3 МОДЕЛЮВАННЯ АДАПТИВНОГО СКРЕМБЛЕРА У СЕРЕДОВИЩІ MATLAB

3.1 Постановка задачі та розробка алгоритму моделювання

При прийомі сигналів цифрового телебачення виникає завдання виділення сигналів тактової частоти прийнятого сигналу. Тактові імпульси окремо не передаються лінією зв'язку, а відновлюються в приймачі з прийнятого сигналу за допомогою петлі ФАПЧ. Для надійної роботи петлі автопідстроювання сигнал не повинен містити довгих послідовностей нулів та одиниць.

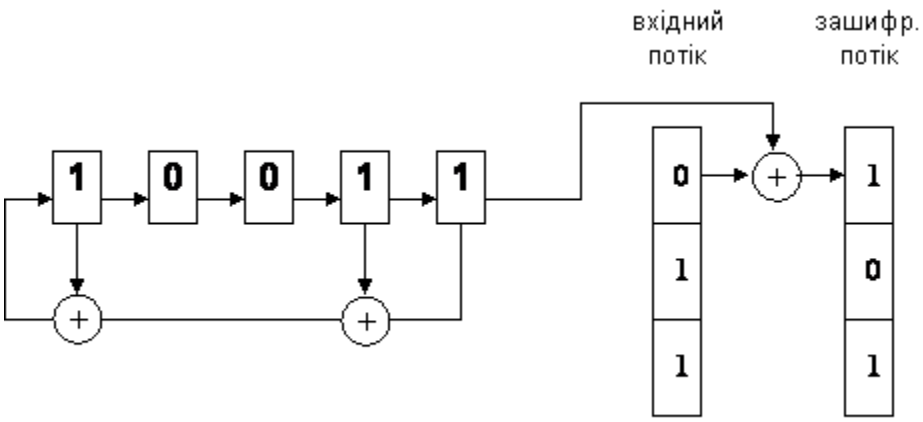
Істотно знизити ймовірність появи довгих однотипних кодових комбінацій дозволяє застосування методу та процесу адаптивного скремблювання, яке здійснюється адаптивним скремблером з ізольованим генератором псевдовипадкових бітових цифрових послідовностей. Структура такого адаптивного скремблера змінюється відповідно до вхідного сигналу так, щоб у перетвореному сигналі мінімізувати довгі послідовності 0 або 1. Відповідно до схеми такого скремблера (рис. 2.7), вхідний цифровий сигнал поділяється на окремі блоки, що необхідно для захисту від помилок, і надходить на суматори за модулем два ∑2, ∑3 и ∑4. У ці ж самі суматори надходять і згенеровані генераторами ГЕН. ПВП1, ГЕН. ПВП2 та ГЕН. ПВП3, псевдовипадкові цифрові послідовності ПВП1, ПВП2 та ПВП3 відповідно.

Кожна послідовність ПВП формується відповідно до алгоритму, що описується невеликою кількістю параметрів, одним з яких є поліном, що утворює послідовність ПВП. Згенеровані псевдовипадкові послідовності ПВП1, ПВП2 та ПВП3 будуть різними. У кожному із трьох генераторів ГЕН. ПВП використовувалися різні поліноми, що утворюють. Для генератора ГЕН. ПВП1 використовувався утворючий поліном [22 21 0] з довжиною ПВП1, яка

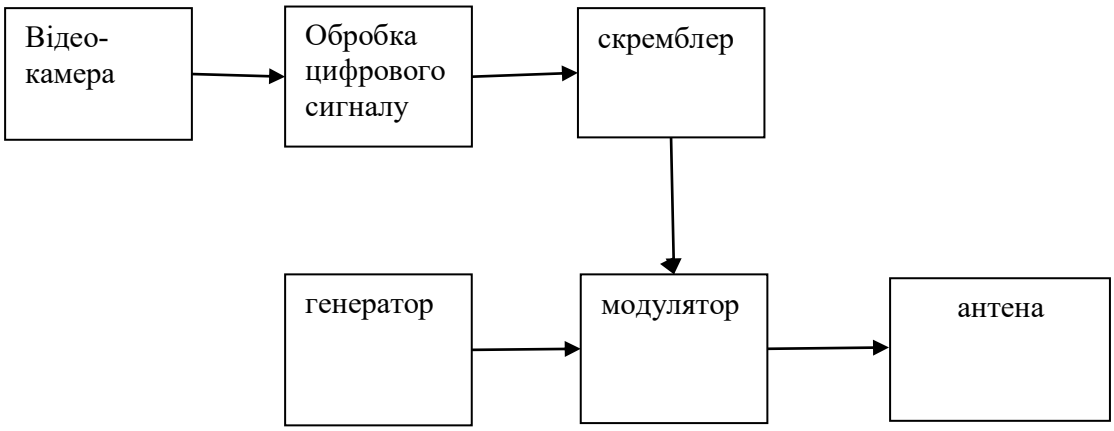
дорівнює 2^{22} біт. Для генератора ГЕН. ПВП2 - поліном [21 19 0] з довжиною ПВП2, яка дорівнює 2^{21} біт, а для третього генератора ГЕН. ПВП3 - поліном [20 17 0] з довжиною ПВП3 - 2^{20} біт.

У суматорах ∑2, ∑3 и ∑4 власне і відбувається процес скремблювання. Після виконання операції скремблювання вхідного цифрового інформаційного сигналу псевдовипадковими послідовностями ПВП1, ПВП2 і ПВП3, цифровий скрембльований сигнал надходить на двійковий лічильник СЧ. У лічильнику проводиться підрахунок максимального числа однотипних комбінацій з нулів та одиниць у кожній скрембльованій послідовності. Далі за допомогою блоку управління *БУ* та логічного пристрою *ЛП* вибирається найкраща послідовність ПВП (за критерієм мінімуму нулів та одиниць поспіль у скрембльованому сигналі). В результаті підсумовування у суматорі ∑*1* цієї ПВП по модулю 2 з вихідним цифровим сигналом, затриманим у блоці *УЗБ* на час, що дорівнює тривалості одного блоку, утворюється вихідна скрембльована послідовність.

В результаті скремблювання сигналу в передавачі число однакових біт, що йдуть поспіль, скорочується. Повністю уникнути довгих послідовностей все ж таки не вдається. Вони виникають, коли сигнальна та псевдовипадкова послідовності збігаються. Імовірність такого збігу досить мала, проте в складних умовах прийому з доплерівським зрушенням, що змінюється, це може призвести до зриву синхронізації. Така ситуація характерна, наприклад, для систем передачі зображення із космічних станцій, розташованих на орбіті. Тому в даній роботі в програмному середовищі MATLAB було досліджено ефективність роботи адаптивного скремблера з паралельним аналізом (рис. 3.1). Для ефективного вирішення цього завдання було розроблено алгоритм моделювання (рис. 3.2).



а)



б)

Рисунок 3.1 – Принцип дії а) і структурна схема передавача з використанням скремблера б)

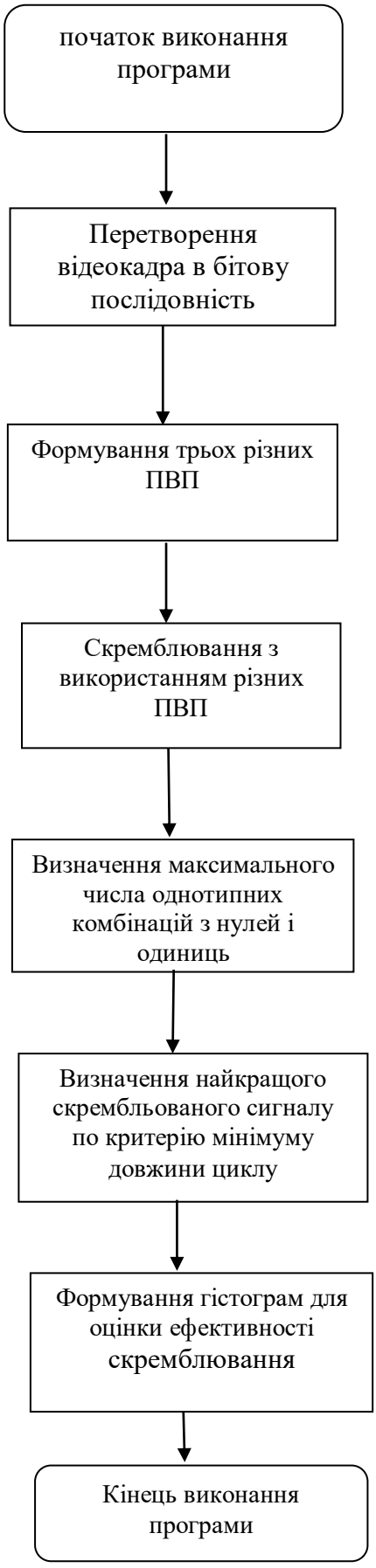


Рисунок 3.2 – Алгоритм моделювання

3.2 Програма для моделювання адаптивного скремблера

Дослідження адаптивного скремблера виконувалося методом математичного імітаційного моделювання в середовище MATLAB.

MATLAB (скорочення від англ. "Matrix Laboratory") - термін, що відноситься до пакета прикладних програм для вирішення завдань технічних обчислень, а також до мови програмування, що використовується в цьому пакеті. MATLAB використовують понад 1 000 000 інженерних та науковців, він працює на більшості сучасних операційних комп'ютерних систем, включаючи GNU/Linux, Mac OS, Solaris та Microsoft Windows.

MATLAB як мову програмування було розроблено Клівом Моулером (англ. Cleve Moler) наприкінці 1970-х років, коли він працював деканом факультету комп'ютерних наук в Університеті Нью-Мексико. Мова MATLAB є високорівневою мовою програмування, що інтерпретується (це мова програмування, в якій вихідний код програми не перетворюється на комп'ютерний код для безпосереднього виконання процесором, а виконується за допомогою спеціальної програми-інтерпретатора). Він включає засновані на матрицях структури даних, широкий спектр математичних функцій, інтегроване середовище розробки, об'єктно-орієнтовані різноманітні можливості та інтерфейси до програм, написаних іншими мовами програмування [11, 14].

Програми, написані на MATLAB, бувають двох типів – функції та скрипти. Функції мають вхідні та вихідні аргументи, а також власний робочий простір для зберігання проміжних результатів обчислень та змінних. Скрипти ж використовують загальний робочий простір. Як скрипти, і функції не компілюються під час виконання програми в машинний код і зберігаються як текстові файли. Існує також можливість зберігати та реалізовувати так звані pre-parsed програми – функції та скрипти, оброблені у вигляді, зручному для машинного комп'ютерного виконання. Загалом такі програми

виконуються швидше за звичайні програми, особливо якщо функція містить команди побудови різних графіків. Основною особливістю мови MATLAB є його широкі можливості для роботи з різними матрицями.

Застосування:

1. Математика та обчислення – MATLAB надає користувачеві велику кількість (кілька сотень) різноманітних функцій для аналізу даних практично у всіх галузях математики, зокрема:

- матриці та лінійна алгебра - алгебра матриць, лінійні рівняння, власні значення та вектори, сингулярності, факторизація матриць та інші;

- багаточлени та інтерполяція - коріння багаточленів, операції над багаточленами та їх диференціювання, інтерполяція та екстраполяція кривих та інші;

- математична статистика та аналіз даних - статистичні функції, статистична регресія, цифрова фільтрація, швидке перетворення Фур'є та інші;

- обробка даних - набір спеціальних функцій, включаючи побудову графіків, оптимізацію, пошук нулів, чисельне інтегрування (у квадратурах) та інші;

- диференціальні рівняння - розв'язання диференціальних та диференціально-алгебраїчних рівнянь, диференціальних рівнянь із запізненням, рівнянь з обмеженнями, рівнянь у приватних похідних та інші;

- розріджені матриці - спеціальний клас даних пакета MATLAB, що використовується у спеціалізованих додатках;

- цілочисленна арифметика - виконання операцій цілочисленної арифметики в середовищі MATLAB.

2. Розробка алгоритмів – MATLAB надає зручні засоби розробки алгоритмів, включаючи високорівневі з використанням концепцій об'єктно-орієнтованого програмування. У ньому є всі необхідні засоби інтегрованого середовища розробки, включаючи налагоджувач та профайлер. Функції до

роботи з цілими типами даних полегшують створення алгоритмів для мікроконтролерів та інших додатків, де це необхідно.

3. *Візуалізація даних* – у складі пакету MATLAB є велика кількість функцій для побудови різноманітних графіків, у тому числі тривимірних, візуального аналізу даних та створення анімованих роликів.

Вбудоване середовище розробки дозволяє створювати графічні інтерфейси користувача з різними елементами керування, такими як кнопки, поля введення та інші. За допомогою компонента MATLAB Compiler ці графічні інтерфейси можуть бути перетворені на самостійні програми, для запуску яких на інших комп'ютерах необхідно встановлювати бібліотеку MATLAB Component Runtime.

4. Зовнішні інтерфейси – пакет MATLAB включає різні інтерфейси для отримання доступу до зовнішніх підпрограм, написаних іншими мовами програмування, даним, клієнтам та серверам, які спілкуються через технології Component Object Model або Dynamic Data Exchange, а також периферійним пристроям, які взаємодіють безпосередньо із середовищем MATLAB. Багато із зазначених можливостей відомі під назвою MATLAB API.

5. COM – пакет MATLAB надає доступ до функцій, що дозволяють створювати, маніпулювати та видаляти COM-об'єкти (як клієнти, так і сервери). Також підтримується технологія ActiveX. Усі COM-об'єкти належать до спеціального COM-класу пакету MATLAB. Всі програми, що мають функції контролера автоматизації (англ. Automation controller) можуть мати доступ до MATLAB як сервер автоматизації (англ. Automation server).

6. DDE – пакет MATLAB містить функції, які дозволяють йому отримувати доступ до інших програм середовища Windows, так само як і цим програмам отримувати доступ до даних середовища MATLAB, за допомогою технології динамічного обміну даними (DDE). Кожна програма, яка може бути DDE-сервером, має своє унікальне ідентифікаційне ім'я. Для MATLAB це ім'я – Matlab.

7. Веб-сервіси – у MATLAB існує чудова можливість викликати методи веб-сервісів. Спеціальна функція створює клас, ґрунтуючись на методах API веб-сервісу. MATLAB взаємодіє з клієнтом веб-сервісу за допомогою прийняття від нього посилок, їх обробки та посилок відповіді. Підтримуються такі технології: Simple Object Access Protocol (SOAP) та Web Services Description Language (WSDL).

8. COM-порт – інтерфейс для послідовного порту пакету MATLAB забезпечує прямий доступ до периферійних пристроїв, таких як модеми, принтери та наукове обладнання, що підключається до комп'ютера через порт (COM-порт). Інтерфейс працює шляхом створення об'єкта спеціального класу для послідовного порту. Наявні методи цього класу дозволяють записувати дані до послідовного порту, використовувати події та обробники подій, а також записувати інформацію на диск комп'ютера в режимі реального часу. Це буває необхідно при проведенні фізичних експериментів, симуляції систем реального часу та виконання інших додатків.

9. MEX- файли – пакет MATLAB включає інтерфейс взаємодії із зовнішніми програмами, написаними мовами C та Фортран. Здійснюється ця взаємодія через MEX-файли. Існує можливість виклику підпрограм, написаних на C або Фортрані з MATLAB, як це вбудовані функції пакета. MEX-файли являють собою бібліотеки, що динамічно підключаються, які можуть бути завантажені і виконані інтерпретатором, вбудованим в MATLAB. MEX-процедури забезпечують можливість викликати вбудовані команди MATLAB.

10. DLL – інтерфейс MATLAB, що відноситься до загальних DLL дозволяє викликати функції, що знаходяться в звичайних бібліотеках, що динамічно підключаються, прямо з MATLAB. Ці функції повинні мати C-інтерфейс. Крім того, у MATLAB є можливість отримати доступ до його вбудованих функцій через C-інтерфейс, що дозволяє використовувати функції пакету у зовнішніх додатках, написаних на C. Ця технологія в MATLAB називається C Engine.

Набори інструментів – для MATLAB є можливість створювати спеціальні набори інструментів (toolbox), що розширюють його функціональність. Набори інструментів є колекцією функцій, написаних мовою MATLAB для вирішення певного класу завдань. Mathworks постачає набори інструментів, які використовуються в багатьох областях, включаючи наступні:

Цифрова обробка сигналів, зображень та даних: DSP Toolbox, Image Processing Toolbox, Wavelet Toolbox, Communication Toolbox, Filter Design Toolbox — набори функцій, що дозволяють вирішувати широкий спектр завдань обробки сигналів, зображень, проектування цифрових фільтрів та систем зв'язку.

Системи управління: Control Systems Toolbox, μ-Analysis and Synthesis Toolbox, Robust Control Toolbox, System Identification Toolbox, LMI Control Toolbox, Model Predictive Control Toolbox, Model-Based Calibration Toolbox — це набори функцій, що полегшують аналіз та синтез динамічних систем, проектування, моделювання та ідентифікацію систем управління, включаючи сучасні алгоритми управління, такі як робастне управління, H-управління, ЛМН-синтез, μ-синтез та інші.

Фінансовий аналіз: GARCH Toolbox, Fixed-Income Toolbox, Financial Time Series Toolbox, Financial Derivatives Toolbox, Financial Toolbox, Datafeed Toolbox — це набори функцій, що дозволяють швидко та ефективно збирати, обробляти та передавати різну фінансову інформацію.

Аналіз та синтез географічних карт, включаючи тривимірні: Mapping Toolbox.

Збір та аналіз експериментальних даних: Data Acquisition Toolbox, Image Acquisition Toolbox, Instrument Control Toolbox, Link for Code Composer Studio — набори функцій, що дозволяють зберігати та обробляти дані, отримані в ході експериментів, у тому числі в реальному часі. Підтримується широкий спектр наукового та інженерного вимірювального обладнання.

Візуалізація та подання даних: Virtual Reality Toolbox — дозволяє створювати інтерактивні світи та візуалізувати наукову інформацію за допомогою технологій віртуальної реальності та мови VRML.

Засоби розробки: MATLAB Builder for COM, MATLAB Builder for Excel, MATLAB Builder for NET, MATLAB Compiler, Filter Design HDL Coder — набори функцій, що дозволяють створювати незалежні програми із середовища MATLAB.

Взаємодія із зовнішніми програмними продуктами: MATLAB Report Generator, Excel Link, Database Toolbox, MATLAB Web Server, Link for ModelSim — набори функцій, що дозволяють зберігати дані різних видів таким чином, щоб інші програми могли з ними працювати.

Бази даних: Database Toolbox - інструменти роботи з базами даних.

Наукові та математичні пакети: Bioinformatics Toolbox, Curve Fitting Toolbox, Fixed-Point Toolbox, Fuzzy Logic Toolbox, Genetic Algorithm and Direct Search Toolbox, OPC Toolbox, Optimization Toolbox, Partial Differential Equation Toolbox, Spline Toolbox, Statistic Toolbox, RF Toolbox — набори спеціалізованих математичних функцій, що дозволяють вирішувати широкий спектр наукових та інженерних завдань, включаючи розробку генетичних алгоритмів, розв'язання задач у приватних похідних, цілі проблеми, оптимізацію систем та інші.

Нейронні мережі: Neural Network Toolbox — інструменти для синтезу та аналіз нейронних мереж.

Нечітка логіка: Fuzzy Logic Toolbox - інструменти для побудови та аналізу нечітких множин.

Символьні обчислення: Symbolic Math Toolbox — інструменти для символьних обчислень із можливістю взаємодії із символьним процесором програми Maple.

Крім перелічених вище, існують тисячі інших наборів інструментів для MATLAB, написаних іншими компаніями-розробниками [13].

Для математичного моделювання процесів скремблювання на мові MATLAB було написано основну програму та п'ять підпрограм *.m файлів, а саме:

1. модель адаптивного скремблера (основна програма):

```
clear
% джерело сигналу
I1=imread('D:/didgest 4.bmp'); % зчитуємо картинку
I=rgb2hsv(I1); %переводимо у формат HSV
Y(:,:)=255*I(:,:,3); % виділяємо яскравість
N=length(Y); % визначаємо розмір картинки
n=0;
Y=Y(:);
Ybin(:,:)=dec2bin(Y,8);
Ybin=Ybin';
Ybin1=Ybin(:);
Z = zeros(size(Ybin1));
k = logical(Ybin1=='1');
Z(k) = 1;

%PSP1
registr1=zeros(1,22);
% завдання початкової умови
registr1(3)=1;
registr1(5)=1;
registr1(10)=1;
% формування psp1
zzz=psp(registr1);

z1=zzz(1:3840000);

%PSP2
registr2=zeros(1,21);
% завдання початкової умови
registr2(4)=1;
registr2(7)=1;
registr2(13)=1;
% формування psp2
zzz2=psp2(registr2);
z2=zzz2(1:3840000);

%PSP3
registr3=zeros(1,20);
% завдання початкової умови
registr3(5)=1;
registr3(6)=1;
registr3(15)=1;
% формування psp3
zzz3=psp3(registr3);
z3=zzz3(1:3840000);
```

```
%скремблювання
C1=xor(Z,z1');
C2=xor(Z,z2');
C3=xor(Z,z3');
%счетчик
N1 = max_seria(C1);
N2 = max_seria(C2);
N3 = max_seria(C3);
N0 = max_seria(Z);
% визначення кращої ПСП (за критерієм
  мінімуму нулів та одиниць поспіль у скрембльованому сигналі)
if (N1<=N2)&(N1<=N3)
    OUT=C1;
    numberpsp=1;
elseif (N2<N1)&(N2<=N3)
    OUT=C2;
    numberpsp=2;
else
    OUT=C3;
    numberpsp=3;
end

% створення матриці нулів
  розмірністю 25x3
H=zeros(25,3)
%запис значень у матрицу
H(1:25,1)=seria(C1);
H(1:25,2)=seria(C2);
H(1:25,3)=seria(C3);

% побудова гістограм для
  аналізу ефективності
  адаптивного скремблювання
bar(H,'group');
```

2. модель генератора ПВП 1:

```
function zz = psp(registr)

zz=zeros(1,3841000);
for hh=1:3841
for kk=1:1000
    zz(kk-1000+1000*hh)=registr(22);
    x11=xor(registr(21),registr(22));

    registrm=circshift(registr',1);
    registr(1,2:22)=registrm(2:22);
    registr(1,1)=x11;
end
end
```

3. модель генератора ПВП 2:

```
function zz2 = psp2(registr12)

zz2=zeros(1,3841000);
for hh=1:3841
for kk=1:1000
    zz2(kk-1000+1000*hh)=registr12(21);
    x12=xor(registr12(19),registr12(21));

    registrm2=circshift(registr12',1);
    registr12(1,2:21)=registrm2(2:21);
    registr12(1,1)=x12;
end
end
```

4. модель генератора ПВП 3:

```
function zz3 = psp3(registr13)

zz3=zeros(1,3841000);
for hh=1:3841
for kk=1:1000
    zz3(kk-1000+1000*hh)=registr13(20);
    x13=xor(registr13(17),registr13(20));

    registrm3=circshift(registr13',1);
    registr13(1,2:20)=registrm3(2:20);
    registr13(1,1)=x13;
end
end
```

5. модель лічильника 0 або 1 для визначення кращої ПВП:

```
function n = max_seria(c)

temp = 0;
state = 0;
n = 0;
for i = 1:length(c)
   if(c(i)==state)
       n = n+1;
   else
       temp = max(n,temp);
       n = 1;
       if(state==1)
           state = 0;
       else
           state = 1;
       end
   end
end
```

```
n = max(n,temp);
```

6. модель лічильника 0 та 1 для побудови гістограм:

```
function hist = seria(c)

hist0 = zeros(25,1);
state = 0;
n = 0;
for i = 1:length(c)
   if(c(i)==state)
       n = n+1;
   else
       if n>0
       hist0(n) = hist0(n)+ 1;
       n = 0;
       end
   end

end

hist1 = zeros(25,1);
state = 1;
n = 0;


for i = 1:length(c)
   if(c(i)==state)
       n = n+1;
   else
       if n>0
       hist1(n) = hist1(n)+ 1;
       n = 0;
       end
   end

end

hist=hist0+hist1;
```

Кожен крок, що виконується в основній програмі ”модель адаптивного скремблера“, досить докладно розписаний у вигляді текстових коментарів, наприклад:

```
clear
%джерело сигналу
I1=imread('D:/didgest 4.bmp'); %зчитуємо картинку
I=rgb2hsv(I1); %переводимо у формат HSV
Y(:,:)=255*I(:,:,3); % виділяємо яркість
N=length(Y); % визначаємо розмір картинки
```

.....

В результаті математичного імітаційного комп'ютерного моделювання з використанням розробленої програми адаптивного скремблеру отримані результати, що дозволяють оцінити ефективність тих чи інших алгоритмів адаптивного скремблювання. Аналіз отриманих результатів, поданий у вигляді гістограм, і обґрунтування зроблених за результатами моделювання висновків наведено в наступному розділі роботи.

4 РЕЗУЛЬТАТИ МОДЕЛЮВАННЯ АДАПТИВНОГО СКРЕМБЛЕРА

При виконанні математичного моделювання як джерело цифрового сигналу в середовищі MATLAB були використані 12 кадрів з роздільною здатністю 1280×720 (відповідає стандарту HD) зі співвідношенням сторін 16:9, які потім були розкладені на послідовність пікселів. Скремблювання цифрового сигналу проводилося для компоненти яскравості отриманих зображень відповідно до алгоритму, представленому на рисунку 3.2, в якому використовуються три різні псевдовипадкові послідовності ПВП.

Після виконання скремблювання кадрів псевдовипадковими послідовностями ПВП1, ПВП2 і ПВП3 оцінювалися довжини циклів скрембльованого сигналу відповідно N1, N2 і N3. Була визначена також довжина циклу нескрембльованого сигналу N0. Під довжиною циклу розуміємо кількість символів у послідовності, яка періодично повторюється. Виходячи з отриманих даних, для кожного кадру було визначено найкращий скрембльований сигнал за критерієм мінімуму довжини циклу.

Результати моделювання адаптивного скремблера представлені у таблиці 4.1. У даній таблиці для кожного використаного кадру було визначено його роздільну здатність, визначено довжину циклу нескрембльованого сигналу N0 і сигналу скрембльованого трьома різними ПВП N1, N2 і N3, а також визначено кращу ПВП за критерієм мінімуму довжини циклу скрембльованого кадру.

Таблиця 4.1 Результати моделювання адаптивного скремблера

N	Кадри	Розрізнення	Нескрембльований сигнал	Скрембльований сигнал			Найкраща ПСП за критерієм мінімуму
			N0	N1	N2	N3	
1	didgest 4.bmp	1280×720	303	22	22	23	2
2	didgest 30.bmp	1280×720	127	24	21	22	2
3	didgest 36.bmp	1280×720	118	22	20	24	2
4	didgest 38.bmp	1280×720	63	19	23	21	1
5	didgest 48.bmp	1280×720	41	22	24	24	1
6	didgest 56.bmp	1280×720	55	20	25	19	3
7	didgest 69.bmp	1280×720	74	23	23	20	3
8	didgest 82.bmp	1280×720	480	22	23	22	1
9	didgest 86.bmp	1280×720	343	21	21	21	1
10	didgest 87.bmp	1280×720	3606	22	21	21	2
11	didgest 88.bmp	1280×720	158	21	23	22	1
12	Waterfall.bmp	1280×720	21	21	24	22	1

З метою аналізу ефективності адаптивного скремблювання за отриманими даними було побудовано гістограми. На рисунках 4.1 – 4.12 представлені результати скремблювання сигналів трьома різними послідовностями ПВП (1 ПВП - синий колір, 2 ПВП - зелений колір, 3 ПВП- оранжевий колір), а на гістограмах 4.13 та 4.14 – порівняння найкращого скрембльованого сигналу з нескрембльованим сигналом.

На рисунках 4.2, 4.4, 4.6, 4.8, 4.10 та 4.12 представлений обраний діапазон значень від 15 до 25 символів, що дозволяє чіткіше побачити та оцінити перевагу одного з трьох скрембльованих сигналів N1, N2 та N3 за критерієм мінімуму довжини циклу. Так на гістограмах 4.1 і 4.2 для кадру didgest 4.bmp видно, що довжина циклу сигналу, скрембльованого другою послідовністю ПСП, менше порівняно з довжиною циклу сигналу скрембльованого першою і третьою ПВП, а отже кращої ПВП за критерієм мінімуму наступних нулів і одиниць скрембльованого сигналу є друга ПВП.

З гістограм 4.3 і 4.4 для кадру didgest 69.bmp видно, що довжина циклу сигналу скрембльованого третьою послідовністю ПВП менша в порівнянні з довжиною циклу сигналу скрембльованого першою і другою ПВП, а отже кращою ПВП за критерієм мінімуму нулів і одиниць поспіль у скрембльованому сигналі є третя послідовність.

За результатами моделювання, представлених на гістограмах 4.5 і 4.6 для кадру didgest 82.bmp видно, що довжина циклу скрембльованого сигналу другої ПВП менше в порівнянні з довжиною циклу сигналу скрембльованого першої і третьої послідовністю ПВП. З цього випливає, що найкращою ПВП за критерієм мінімуму нулів і одиниць, що випливають поспіль у скрембльованому сигналі, є друга послідовність ПВП.

На гістограмах 4.7 і 4.8 для кадру didgest 87.bmp видно, що довжина циклу скрембльованого сигналу другої ПВП менша в порівнянні з довжиною циклу сигналу скрембльованого першої і третьої ПВП, з чого слід, що кращої ПВП за критерієм мінімуму нулів і одиниць поспіль в скрембльованому є друга послідовність. При цьому кадр didgest 87.bmp у нескрембльованому вигляді має довжину циклу 3606 символів (табл.4.1), що майже в 172 рази більше за довжину циклу скрембльованого сигналу, тобто циклу довжиною 21 символ. Найменшу довжину циклу без скремблювання має досліджуваний кадр Waterfall, який збігається з довжиною циклу цього кадру після скремблювання кращої ПВП за критерієм мінімуму і становить 21 символ.

На гістограмах 4.13, 4.14 представлено порівняння довжини циклів скрембльованого сигналу, отриманого з використанням найкращої ПСП (синій колір) та сигналу без скремблювання (помаранчевий колір) у збільшеному масштабі. Як бачимо, використання скремблювання при обробці сигналів дозволяє суттєво зменшити довжини фрагментів цифрового сигналу з однаковою структурою в цифрової бітової інформаційної послідовності, що дозволяю суттєво підвищити якість передавання інформаційного відеосигналу каналом зв’язку.

У результаті можна дійти висновку, що перевагою схеми адаптивного скремблера проти простого скремблеру є істотне зниження ймовірності появи довгих однотипних комбінацій. Ступінь зменшення цього структурного параметра залежить від статистичних властивостей вхідного цифрового сигналу, і навіть від властивостей скремблюючої М-послідовності, тобто залежить від обраного утворюючого полінома (утворюючий поліном впливає на довжину псевдовипадкової послідовності, що скремблює).

Додатковою перевагою адаптивного скремблювання є забезпечення значно більшої надійності роботи петлі фазового автопідстроювання частоти ФАПЧ, що у свою чергу при прийомі сигналів цифрового телебачення покращить відновлення та виділення в приймальному пристрої з прийнятого сигналу імпульсів тактової частоти, що визначають значною мірою ефективність прийому всього телевізійного сигналу .

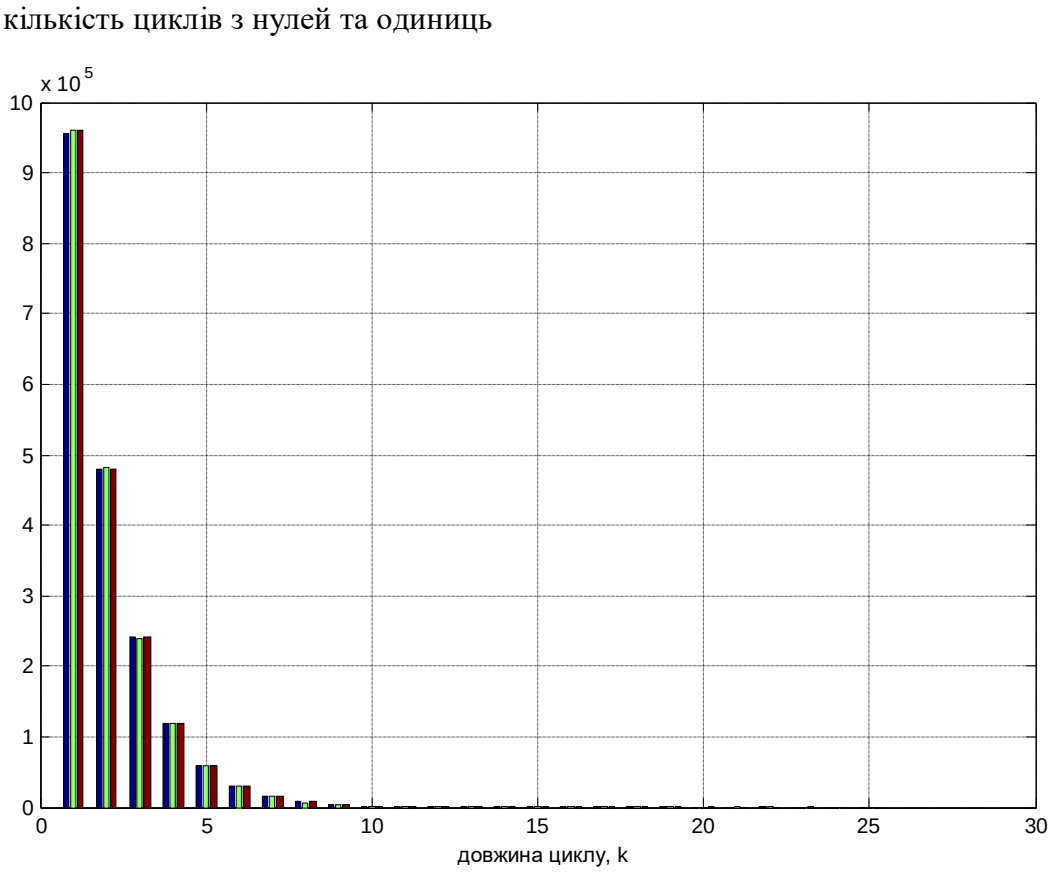


Рисунок 4.1 – Гістограма для кадру didgest 4

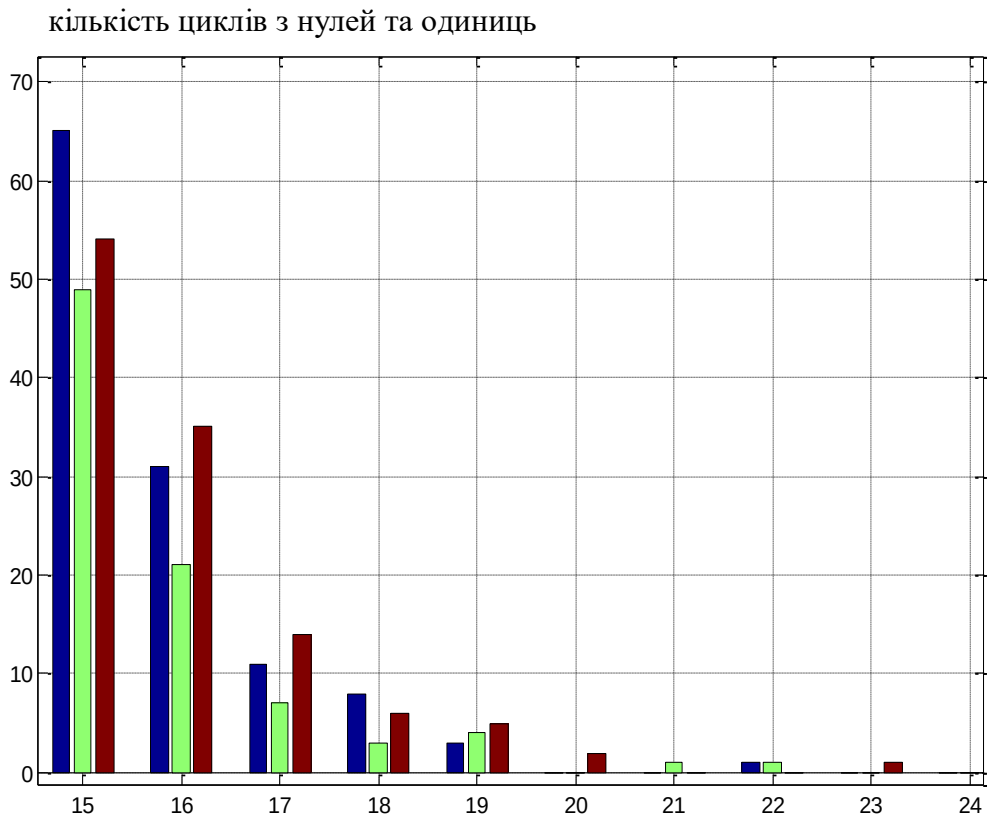


Рисунок 4.2 – Вибірка гістограми для кадру didgest 4

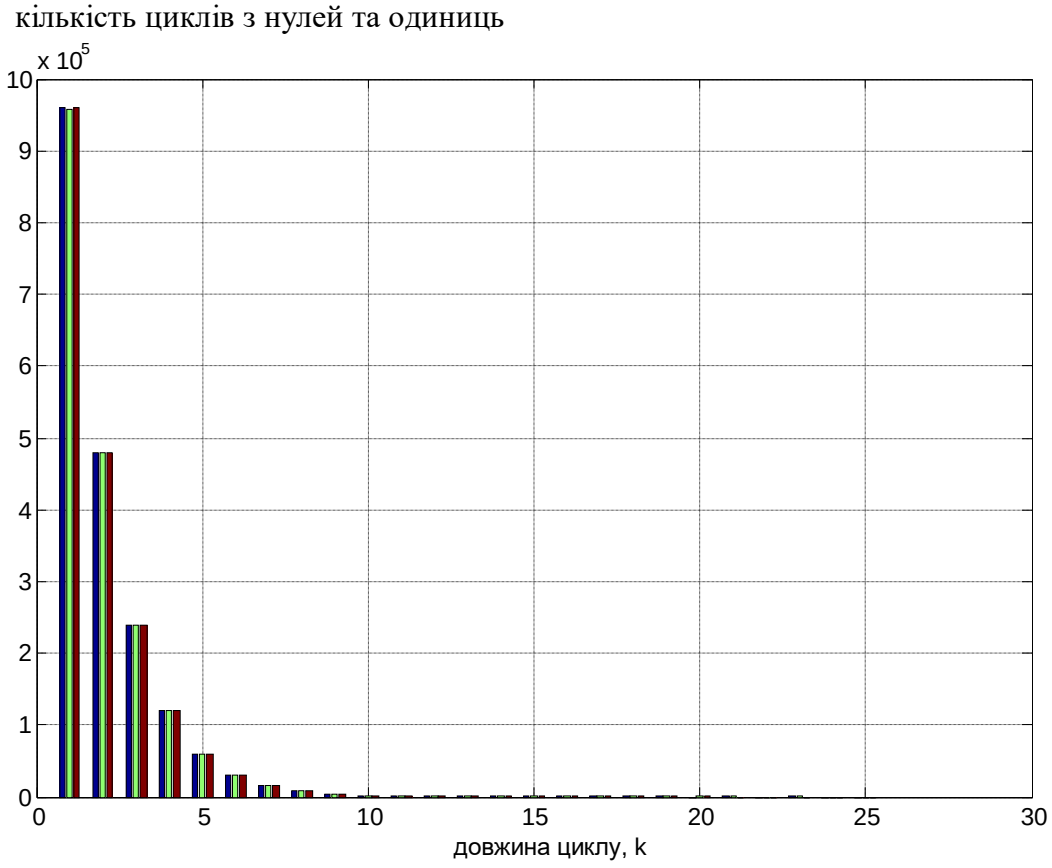


Рисунок 4.3 – Гістограма для кадру didgest 69

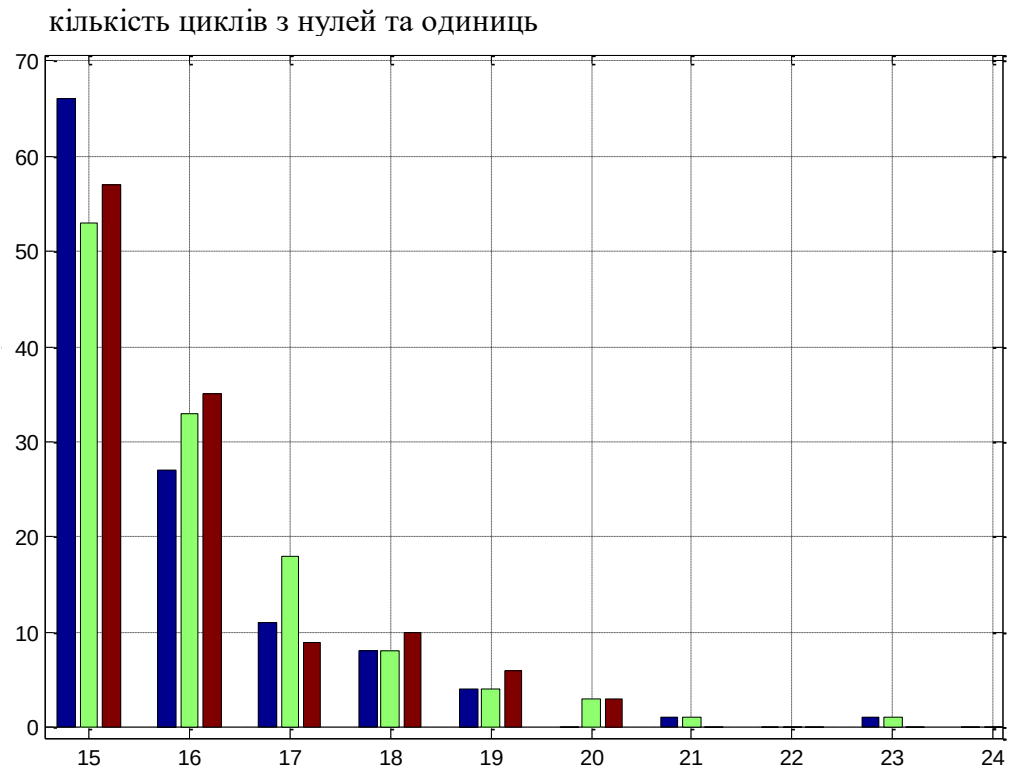


Рисунок 4.4 – Вибірка гістограми для кадру didgest 69

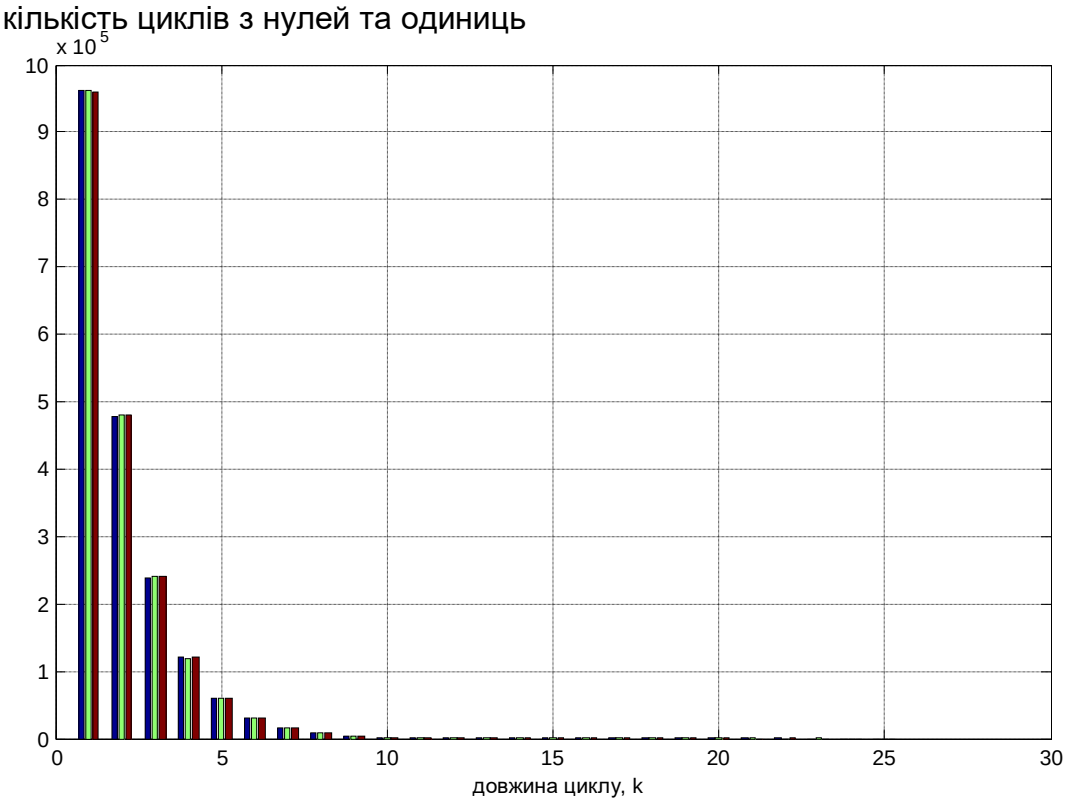


Рисунок 4.5 – Гістограма для кадру didgest 82

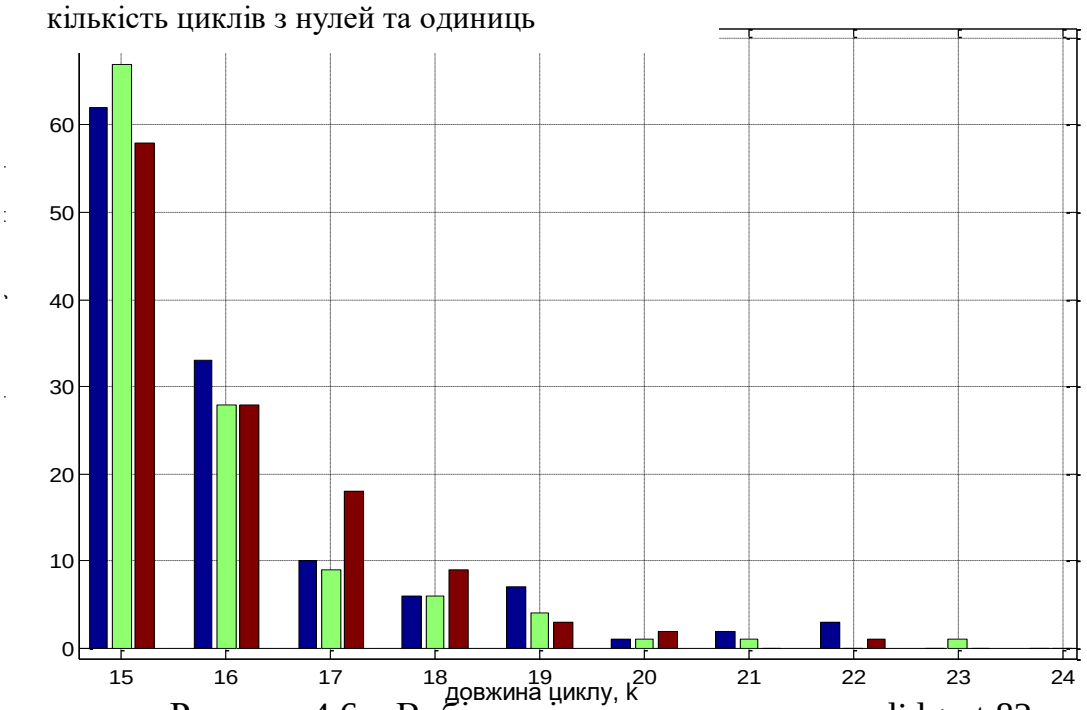


Рисунок 4.6 – Вибірка гістограми для кадру didgest 82

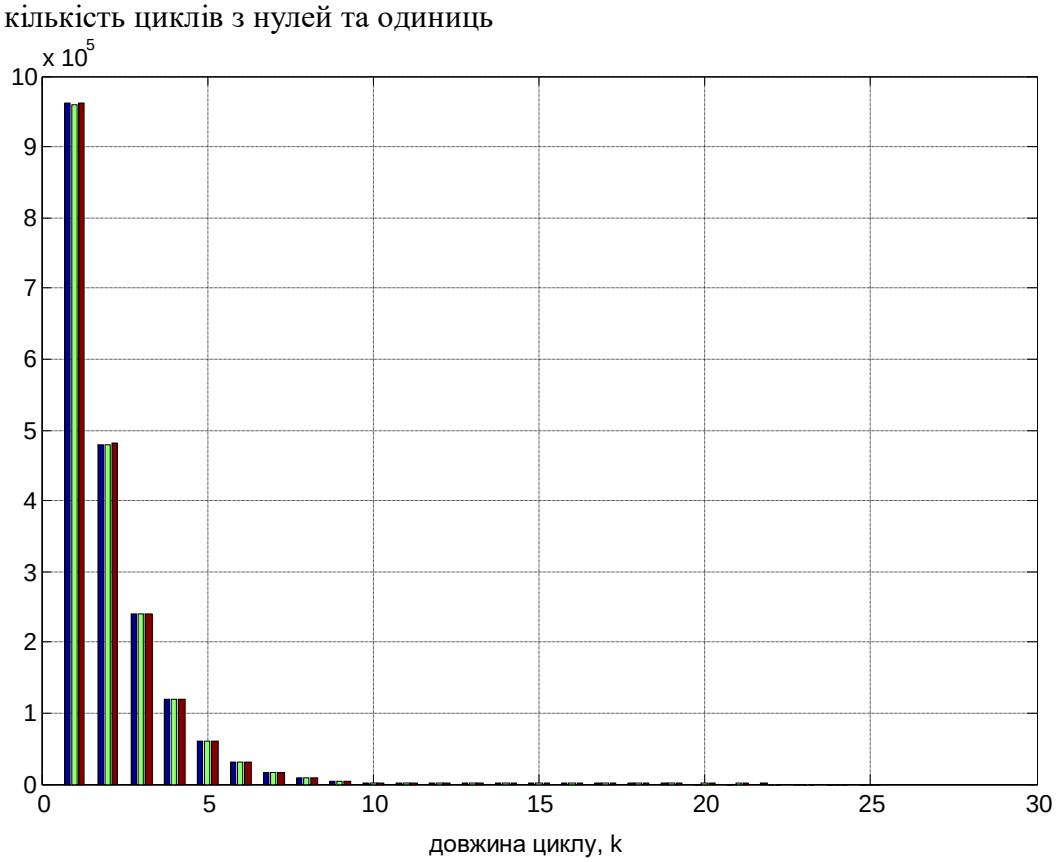


Рисунок 4.7 – Гістограма для кадру didgest 87

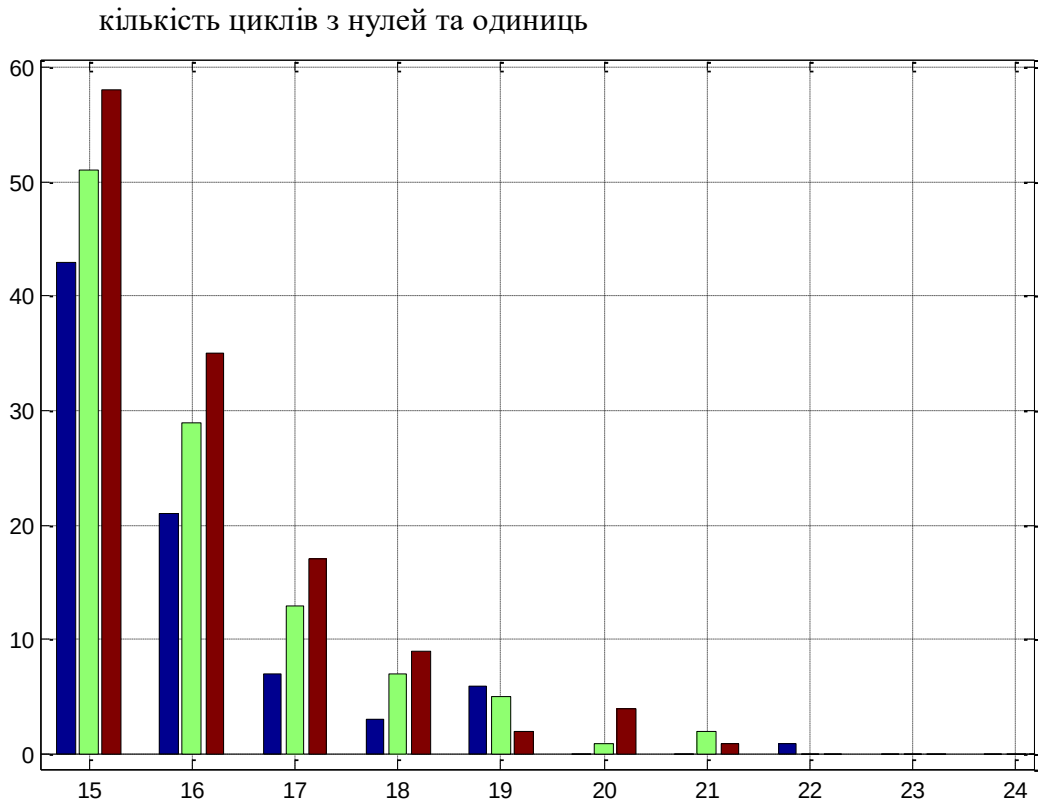


Рисунок 4.8 – Вибірка гістограми для кадру didgest 87

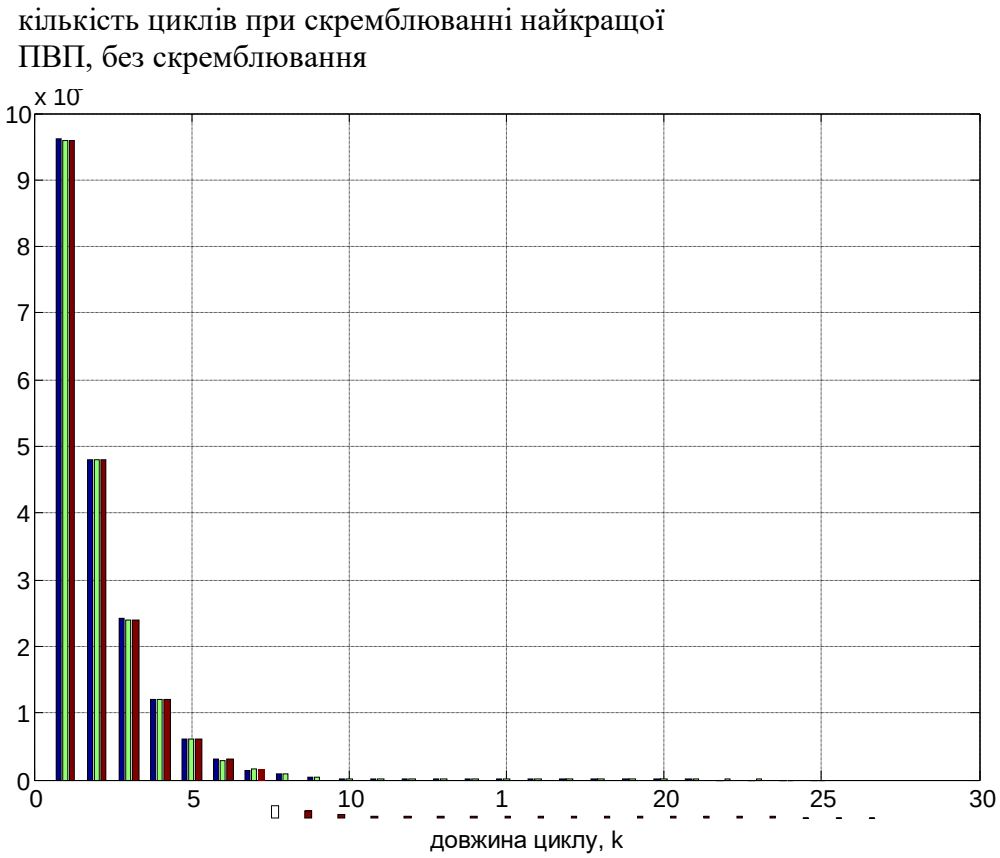


Рисунок 4.9 – Гістограма для кадру didgest 88

кількість циклів з нулей та одиниць

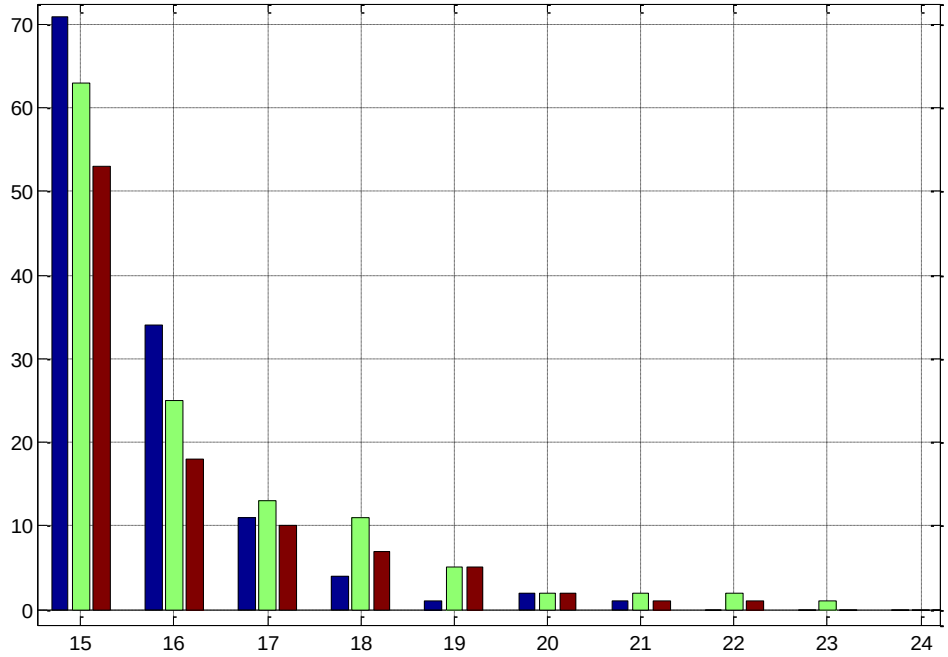


Рисунок 4.10 – Вибірка гістограми для кадру didgest 88

кількість циклів з нулей та одиниць

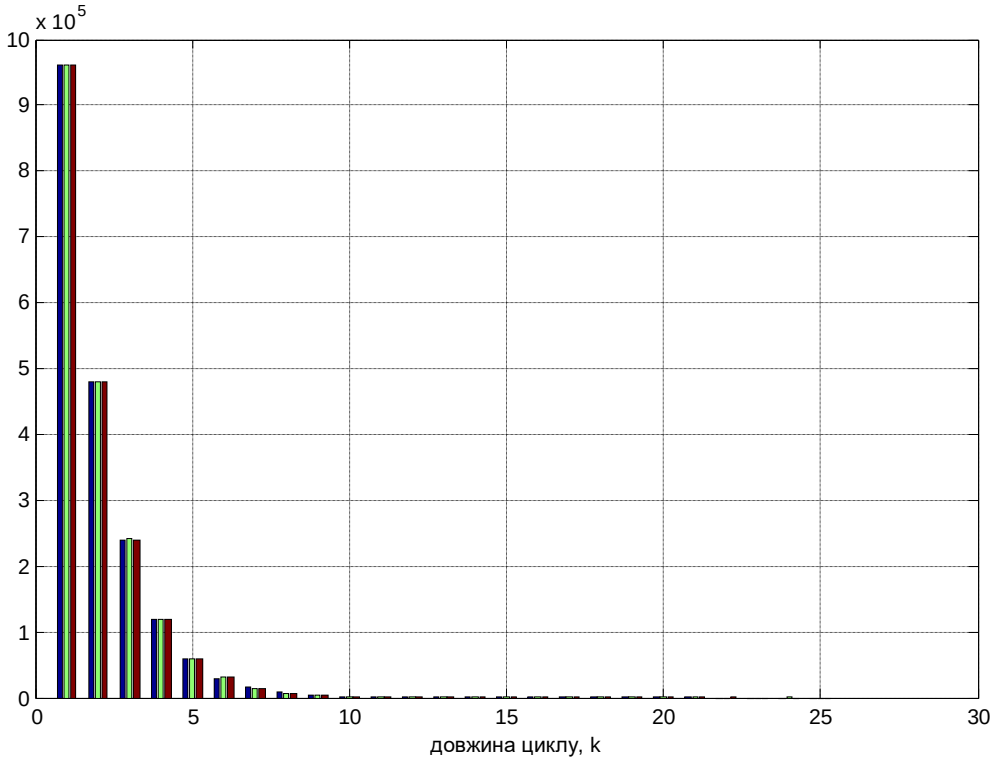


Рисунок 4.11 – Гістограма для кадру Waterfall

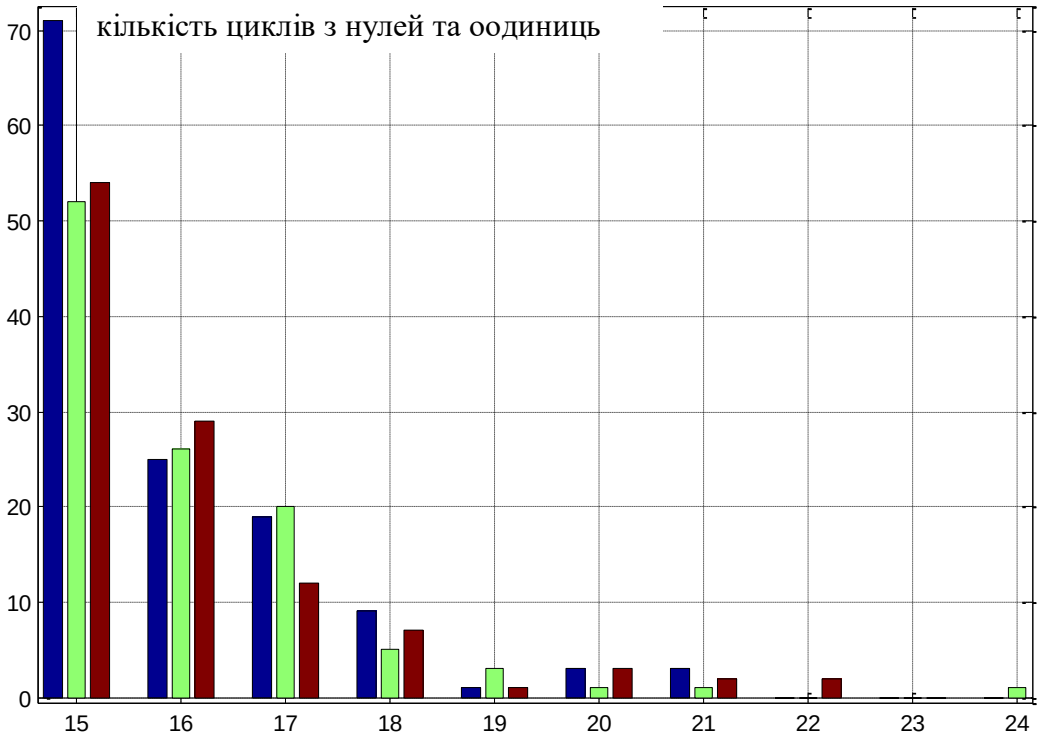


Рисунок 4.12 – Вибірка гістограми для кадру Waterfall

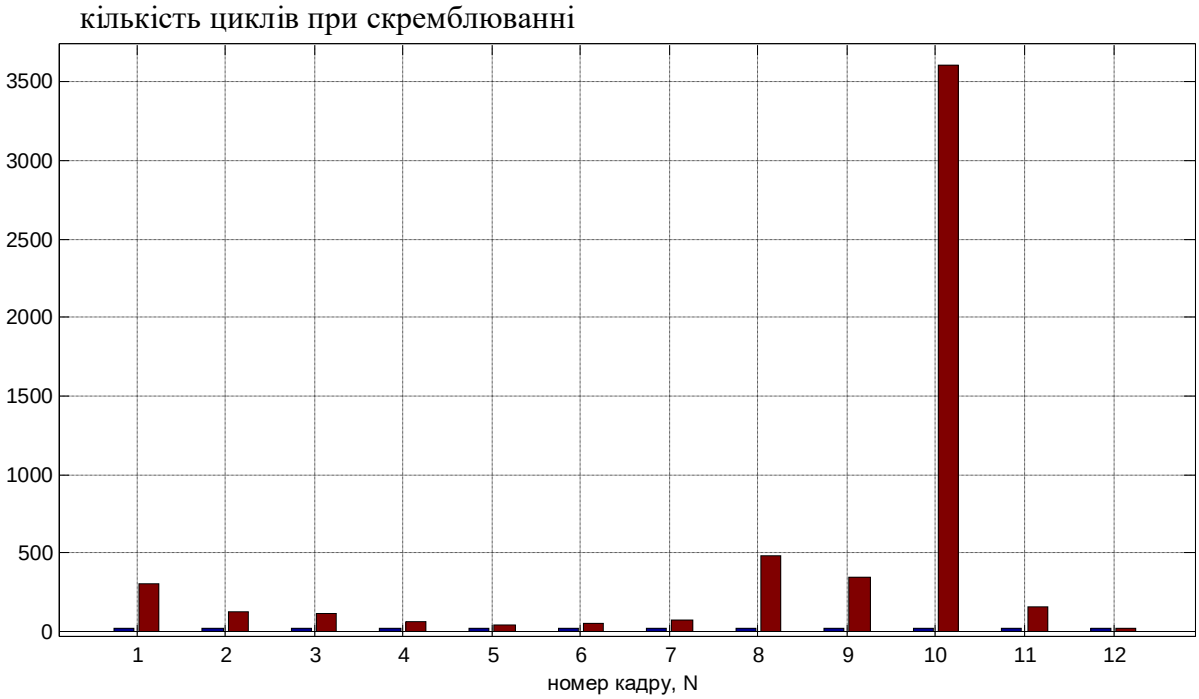


Рисунок 4.13 – Порівняння довжини циклів скрембльованого сигналу, отриманого з використанням найкращої ПСП (синій колір), та сигналу без скремблювання (помаранчевий колір)

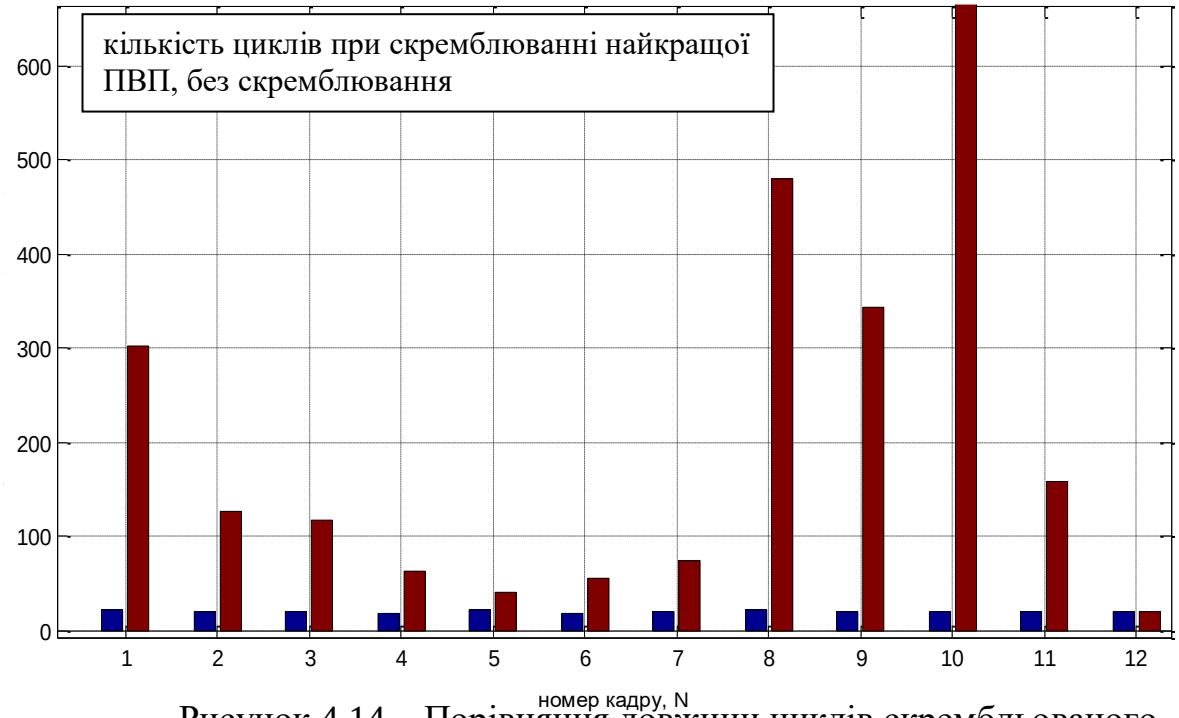


Рисунок 4.14 – Порівняння довжини циклів скрембльованого сигналу, отриманого з використанням найкращої ПВП (синій колір) та сигналу без скремблювання (помаранчевий колір) у збільшеному масштабі

ВИСНОВКИ

У кваліфікаційної магістерській роботі методом математичного комп'ютерного моделювання у середовищі MATLAB досліджено ефективність роботи адаптивного скремблера з паралельним аналізом у різних умовах.

Для виконання дослідження методом моделювання процесів скремблювання на мові MATLAB були написані ряд програм: основна програма, що є алгоритмом роботи адаптивного скремблеру, і п'ять підпрограм у вигляді *.m файлів для моделювання трьох псевдовипадкових послідовностей з різними властивостями, а також дві підпрограми для обробки і якісного представлення одержаних результатів моделювання.

Як джерело цифрового сигналу були використані 12 кадрів з роздільною здатністю 1280×720, які були розкладені на послідовність пікселів. Після проведення скремблювання для кожного кадру з різними ПВП (в даному випадку трьома) отримані різні довжини циклів скрембльованого сигналу, визначено також довжина циклу нескрембльованого сигналу. Виходячи з отриманих даних, для кожного кадру визначено найкращий скрембльований сигнал за критерієм мінімуму довжини циклу. Усі результати моделювання зведені в таблицю та з метою зручності аналізу ефективності адаптивного скремблювання зображені на гістограмах.

В результаті математичного імітаційного комп'ютерного моделювання з використанням розробленої програми адаптивного скремблера отримані результати, що дозволяють оцінити ефективність тих чи інших алгоритмів адаптивного скремблювання.

З результатів можна дійти висновку, що перевагою схеми адаптивного скремблера проти простого скремблеру є істотне зниження ймовірності появи довгих однотипних комбінацій. Ступінь зменшення цього структурного параметра залежить від статистичних властивостей вхідного

цифрового сигналу, а також від властивостей скремблюючої М-послідовності, які визначаються значною мірою обраним поліномом.

Додатковою перевагою адаптивного скремблювання є забезпечення значно більшої надійності роботи петлі фазового автопідстроювання частоти ФАПЧ, що у свою чергу при прийомі сигналів цифрового телебачення покращить відновлення та виділення в приймальному пристрої з прийнятого сигналу імпульсів тактової частоти, що визначають значною мірою ефективність прийому всього телевізійного сигналу .

Таким чином, використання скремблювання при обробці сигналів дозволяє суттєво зменшити довжини фрагментів цифрового сигналу з однаковою структурою в цифрової бітової інформаційної послідовності, що дозволяю суттєво підвищити якість передавання інформаційного відеосигналу каналом зв’язку.

ПЕРЕЛІК ПОСИЛАНЬ

1. Золотарёв В. В., Овечкин Г. В. Помехоустойчивое кодирование. Методы и алгоритмы: Справочник / Под. ред. чл.-кор. РАН Ю. Б. Зубарева. - М.: Горячая линия-Телеком, 2004. - 126 с: ил.
2. Науменко М.І., Стасев Ю.В., Кузнецов О.О. Теоретичні основи та методи побудови алгебраічних блокових кодів. – Х.: ХУ ПС, 2005. – 267 с.
3. Банкет В. Л., Дорофеев В. М. Цифровые методы в спутниковой связи. - М.: Радио и связь, 1988. - 240 с.
4. Зубарев Ю. Б., Овечкин Г. В. Помехоустойчивое кодирование в цифровых системах передачи данных - М.: Горячая линия-Телеком, 2008. – 16с.
5. Р. Блейхут. Теория и практика кодов, контролирующих ошибки: Пер. с англ. – М.: Мир, 1986. – 576 с., ил.
6. Птачек М. Цифровое телевидение. – М.: Радио и связь, 1990. – 528 с.
7. Цифровое телевидение: метод. разработка/сост. Ю.В. Беляев, Ю.И. Галочкин – Владивосток: Изд-во ДВГТУ, 2005. – 91 с.
8. Yokoyama K., Nakagava S., Katayama H. An experimental digital videotape recorder //SMPTE J. – 1980. – 89, N 3. – P. 173.180.
9. Сухов С.М., Бернов А.В., Шевкопляс Б.В. Синхронизация в телекомуникационных системах. Анализ инженерных решений. - М.: Эко-Трендз, 2003г. - 272с.
10. Бернард Скляр Цифровая связь. Теоретические основы и практическое применение. Изд. 2-е, испр.: Пер.с англ.- М.: Издательский дом «Вильямс», 2003.- 1104с.
11. Смирнов А.В. Пескин А.Е. Цифровое телевиденье: от теории к практике.- М.: Изд. Горячая линия- Телеком, 2005. – 349с.
12. Oleynikov V. N , Zubkov O. V., Kartashov V. M., Korytsev I. V., Babkin S. I., Sheiko S. A. Investigation of detection and recognition efficiency of small

unmanned aerial vehicles on their acoustic emission; Telecommunications and Radio Engineering, 2019, Volume 78, Issue 9; pp. 759-770.

13. Kartashov, V., Oleynikov, V., Koryttsev, I., Zubkov, O., Babkin S., Sheiko, S. Processing and Recognition of Small Unmanned Vehicles Sound Signals. 2018 International Scientific-Practical Conference on Problems of Infocommunications. Science and Technology (PIC S and T 2018) – Proceedings, 31 January 2019; pp. 392-396.
14. Kartashov V., Oleynikov V., Koryttsev I., Sheyko S., Zubkov O., Babkin S., Selieznov I. Use of Acoustic Signature for Detection, Recognition and Direction Finding of Small Unmanned Aerial Vehicles; 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), 25-29 Feb. 2020; pp. 1-4.
15. Kartashov, V.M., Oleynikov V.N, Zubkov, O.V., Korytsev I.V., Babkin, S. I., Sheiko, S.A., Kolendovskaya, M.M. Spatial-temporal Processing of acoustic Signals of Unmanned Aerial Vehicles; Telecommunications and Radio Engineering, 2020. Vol. 79, Iss, 9; pp. 769-780.
16. V. Oleynikov, O. Zubkov, V. Kartashov, I. Koryttsev, S. Sheiko, S. Babkin, "Experimental estimation of direction finding to unmanned air vehicles algorithms efficiency by their acoustic emission"; 2019 International Scientific-Practical Conference: Problems of Infocommunications. Science and Technology (PIC S and T 2019) – Proceeding, 2019, pp. 175–178.
17. V.V. Semenets, V.M. Kartashov, V.I. Leonidov. Features of Acoustic Noise of Small Unmanned Aerial Vehicles; Telecommunications and Radio Engineering, 2020. Vol. 79, Iss. 11, pp. 985-995. DOI: 10.1615/TelecomRadEng.v79.i11.80.
18. В.А. Тихонов, В.М. Карташов, В.М. Олейніков, В.И. Леонидов, Л.П. Тимошенко, И.С. Селезнев, Н.В. Рыбников. Обнаружение-распознавание беспилотных летательных аппаратов с использованием составной модели авторегрессии их акустического излучения// Вісник НТУУ «КПІ». Радіотехніка. Радіоапаратобудування. 2020. №81; С. 38-46.

19. Kartashov, V.M., Oleynikov V.N, Zubkov, O.V., Korytsev I.V., Babkin, S. I., Sheiko, S.A., Kolendovskaya, M.M. Spatial-temporal Processing of acoustic Signals of Unmanned Aerial Vehicles; Telecommunications and Radio Engineering, 2020. Vol. 79, Iss, 9; pp. 769-780.

20. Kartashov V. M., Tikhonov V. A. , Voronin V. V. Features of Construction and Application of Complex Systems for the Atmosphere Remote Sounding; Telecommunications and Radio Engineering, 2017, Volume 78, Issue 8; pp.743-749.

21. Карташов В.М., Олейников В.Н., Колендовская М.М., Тимошенко Л.П., Капуста А.И., Рыбников Н.В. Комплексирование изображений при обнаружении беспилотных летательных аппаратов// Радиотехника. (Харьков). 2020. Вып. 201; С.120-129.

22. Карташов В.М. Модели и методы обработки сигналов систем радиоакустического и акустического зондирования атмосферы. -Харьков: ХНУРЭ, 2011. - 234 с.

23. Avalos-Gonzalez, D., Sergiyenko, O., Hernandez-Balbuena, D., Tyrsa,V., Kartashov V.M., V.,Rivas-Lopes, M., Murrieta-Rico, F.N. Constraints definition and application optimization based on geometric analysis of the frequency measurement method by pulse coincidence// Measurement: Journal of the International Measurement Confederation (USA). - 2018. –V.126. - P. 184-193.

24. Карташов В.М., Корытцев И.В., Олейников В.Н., Зубков О.В., Шейко С.А., Бабкин С.И. Оптико-электронные методы обнаружения воздушных объектов и измерения их координат // Радиотехника. (Харьков). — 2020. — Вып. 202. — С. 153-59. DOI:10.30837/rt.2020.3.202.16

25. Ситнік О.В., Карташов В.М., Радіотехнічні системи. Навч. Посібник. Х.: Сміт, 2009. 448 с.

26. Oleksandr Sotnikov, Vladimir Kartashov, Oleksandr Tymochko, Oleg Sergiyenko, Vera Tyrsa, Paolo Mercorelli, Wendy Flores-Fuentes. Methods for Ensuring the Accuracy of Radiometric and Optoelectronic Navigation Systems of Flying Robots

in a Developed Infrastructure Chapter 16// Machine Vision and Navigation. pp.537-578. Editors: Sergiyenko, Oleg, Flores-Fuentes, Wendy, Mercorelli, Paolo (Eds.) DOI: 10.1007/978-3-030-22587-2_16.

27. Murrieta-Rico, F.N., Sergiyenko, O.Y., Petranovskii, V., Hernandez-Balbuena D., Linder, L., Tyrsa V., Nieto-Hipolito, J.I., Rivas-Lopez, M., Karthashov, V.M. Pulse width influence in fast frequency measurements using rational approximations// Measurement: Journal of the International Measurement Confederation . - 2016. –V.86. - P. 67-78.
28. Kartashov V.M., Tikhonov V.A., Voronin V.V. and Tymoshenko L.P. Complex model of random signal in problems of acoustic sounding of atmosphere // Telecommunications and Radio Engineering.- New York. - 2016.- Vol. 75, №20.- P.1885-1892. (стаття).
29. Sergiyenko O. Yu., Kartashov V.M., Ivanov M.V., Rivas-Lopez M. Data transferring model determination in robotic group// Robotics and autonomous Systems. - Host journal for the Intelligent Autonomous Systems Society. – Amsterdam-Boston-London-New York. –Vol. 83. – 2016. –P. 251-260. (стаття).
30. I. Koryttsev, S. Sheiko, V. Kartashov, O. Zubkov, V. Oleynikov, M. Anohin, I. Selieznov. Practical Aspects of Range Determination and Tracking of Small Drones by Their Video Observation. 2020 International Scientific-Practical Conference. Problems of Infocommunications. Science and Technology. Kharkiv, Ukraine. October 6-9, 2020. –5 p.
31. Kartashov V.M., Pososhenko V.O., Kolesnik V.I., Sheiko S.O., Yegorov A.B., Rybnikov N.V., Pershyn Y.V., Kapusta A.I., Ryabukha V.P., Sergiyenko O.Y. Aircraft Flight Modeling in the Area of Critically Important Infrastructure Facilities. 2019 International Scientific-Practical Conference «Problems of Infocommunications – Science and Technology, PIC S and T 2021 - Proceeding». -2021. – 4 p.