УДК 004.716
Орлова М.М. к.т.н. доцент, Гудименко В.С. магістрант
Національний технічний університет України «Київський політехнічний інститут»

СПОСІБ ЗАХИСТУ ДАНИХ В МЕРЕЖАХ LTE

Орлова М.М., Гудименко В.С. Спосіб захисту даних в мережах LTE. У статті розкрито проблему підвищення завадостійкості в сучасних безпроводових мережах LTE. Запропоновано спосіб підвищення завадостійкості інформаційного каналу, при незмінній надлишковості інформації в каналі.
Ключові слова: безпроводові мережі, LTE, завадостійкість, надлишковість, інформаційний канал

Орлова М.Н., Гудыменко В.С. Способ защиты данных в сетях LTE. В статье раскрыто проблему повышения помехоустойчивости в современных беспроводных сетях LTE. Предложен способ повышения помехоустойчивости информационного канала, при неизменной избыточности информации в канале.
Ключевые слова: беспроводные сети, LTE, помехоустойчивость, избыточность, информационный канал

Orlova M.M., Gudimenko V.S. The method of protecting data in the LTE networks. The article reveals the problem of increasing noise immunity in modern wireless networks LTE. The method for improving noise immunity of the information channel with the same information redundancy in the channel is provided..
Keywords: wireless networks, LTE, noise immunity, redundancy, information channel

Постановка наукової проблеми. Науковий прогрес надає більші можливості для розвитку та вдосконалення, але створює проблеми для вже впроваджених технологій. Це питання особливо актуальне для новітніх швидкісних безпроводових мереж, таких, як LTE.

В сучасних безпроводових швидкісних мережах важливою складовою передачі інформації є її захист при передачі від пристрою до пристрою, оскільки похибки, що виникають в таких мережах, призводять до значно більшого спотворення інформації, ніж в проводових мережах. При цьому, при збільшенні швидкості передачі інформації в мережах зростає часовий інтервал впливу похибок на інформаційний потік, що призводить вже не до одиничних, а до групових помилок. Корекція таких помилок призводить до необхідності збільшення надлишковості завадостійких коригувальних кодів, що у свою чергу збільшує надлишковість інформаційного потоку та навантаження на канал передачі. Таким чином, виникає потреба у розробці способу підвищення завадостійкості, при збереженні, по можливості, розміру інформаційного потоку.

Аналіз досліджень.

Питанню підвищення завадостійкості у безпроводових мережах приділяється чимала увага, зокрема, розробкою способів та методів для вирішення цього питання займаються провідні компанії, що розробляють мережеве обладнання, такі як Еріксон, Самсунг, Йота, ZTE та інші.

Мета даної статті - запропонувати спосіб підвищення завадостійкості інформації, що передається в безпроводових мережах LTE, при незмінній надлишковості та завантаженості каналу.

Виклад основного матеріалу. *Зменшення надлишковості*. В сучасних каналах безпроводових мереж LTE використовуються тільки процедури завадостійкого кодування. Як відомо, завадостійкі коди базуються на збільшенні інформаційного потоку, оскільки вносять надлишкову інформацію, за допомогою якої потім можливо буде перевірити та\або відновити спотворену інформацію [2]. Отже, використовуючи лише завадостійке кодування неможливо уникнути надлишковості інформації. Проте, як вже було відмічено раніше, виникає необхідність у модифікації існуючих методів таким чином, щоб завадостійкіть була підвищена, а розмір інформаційного потоку, по можливості, залишився незмінним.

Для того, щоб зменшити надлишковість, необхідно зменшити розмір низхідного інформаційного потоку шляхом його ущільнення, а звільнений після ущільнення інформаційний простір, в такому разі, може бути використаний для відповідного завадостійкого кодування. Таким чином, збільшується завадостійкість інформаційного потоку, залишаючи однакову завантаженість каналу передачі даних. Це покладає додаткове навантаження на кодер\декодер інформації, що, призводить до зменшення швидкості обробки, але, з огляду на швидкість обробки інформації в сучасних мобільних пристроях зв'язку (яка, в середньому, вже досягла швидкостей обробки інформації настольного ПК 2004 року [9]), це більш прийнятно, ніж збільшення навантаження на канал передачі.

Ущільнення. Для ущільнення інформації використовується один з алгоритмів ущільнення без втрат, оскільки такі алгоритми дозволяють повністю відновити дані, які були до ущільнення [7].

Також необхідно врахувати розмір словника, який потрібно передавати разом з ущільненою інформацією, оскільки він також вносить надлишковість і може буде спотворений. Отже, необхідно обрати якомога менший розмір словника, який буде передаватися.

Одними з найбільш оптимальних алгоритмів ущільнення, що підпадають під задані критерії, є алгоритми сімейства Лемпеля-Зива LZ, зокрема LZW (Lempel-Ziv-Welch), який наразі використовується як базовий для багатьох сучасних методів ущільнення [3, 4]. Згідно цього універсального алгоритму, процес стиснення виглядає наступним чином. Спочатку таблиця перетворення заповнюється всіма можливими односимвольними фразами, потім послідовно зчитуються символи вхідного потоку і відбувається перевірка, чи існує в таблиці перетворення такий рядок. Якщо такий рядок існує, зчитується наступний символ, а якщо ні, - в потік заноситься код для попередньо знайденого рядку, неіснуючий рядок заноситься в таблицю і пошук починається знову.

Наприклад, якщо стискають текст (байтові дані), то початкових рядків у таблиці виявиться 256 (від «0» до «255»). Тоді при використанні 10-бітного коду, підкоди для рядків приймають значення в діапазоні від 256 до 1023. Нові рядки формують таблицю послідовно, тобто можна вважати індекс рядка його кодом. При декодуванні потрібно знати тільки початкові рядки та закодований текст, оскільки можливо відтворити відповідну таблицю перетворення безпосередньо по закодованому тексту. Алгоритм генерує кожний наступний код за рахунок того, що коли генерується новий код, новий рядок додається в таблицю. LZW постійно перевіряє, чи рядок вже відомий, і, якщо так, виводить існуючий код без генерації нового. Таким чином, кожен рядок буде зберігатися в єдиному екземплярі і мати свій унікальний номер. Отже, під час декодування, при отриманні нового коду генерується новий рядок, а при отриманні вже відомого, використовується рядок зі словника [5]. Графічно алгоритм зображеній на рис.1. Основні фази алгоритму наступні.

1. Ініціалізація словника всіма можливими односимвольними фразами. Ініціалізація вхідної фрази ω (K) першим символом повідомлення.
2. Зчитати черговий символ K з кодованого повідомлення.
3. Якщо кінець повідомлення, то видати код для ω, інакше перейти до п. 4.
4. Якщо фраза ω (K) вже є в словнику, присвоїти вхідний фразі значення ω (K) і повернутися до п. 2, інакше видати код ω, додати ω (K) в словник, присвоїти вхідний фразі значення K і повернутися п. 2.
5. Кінець

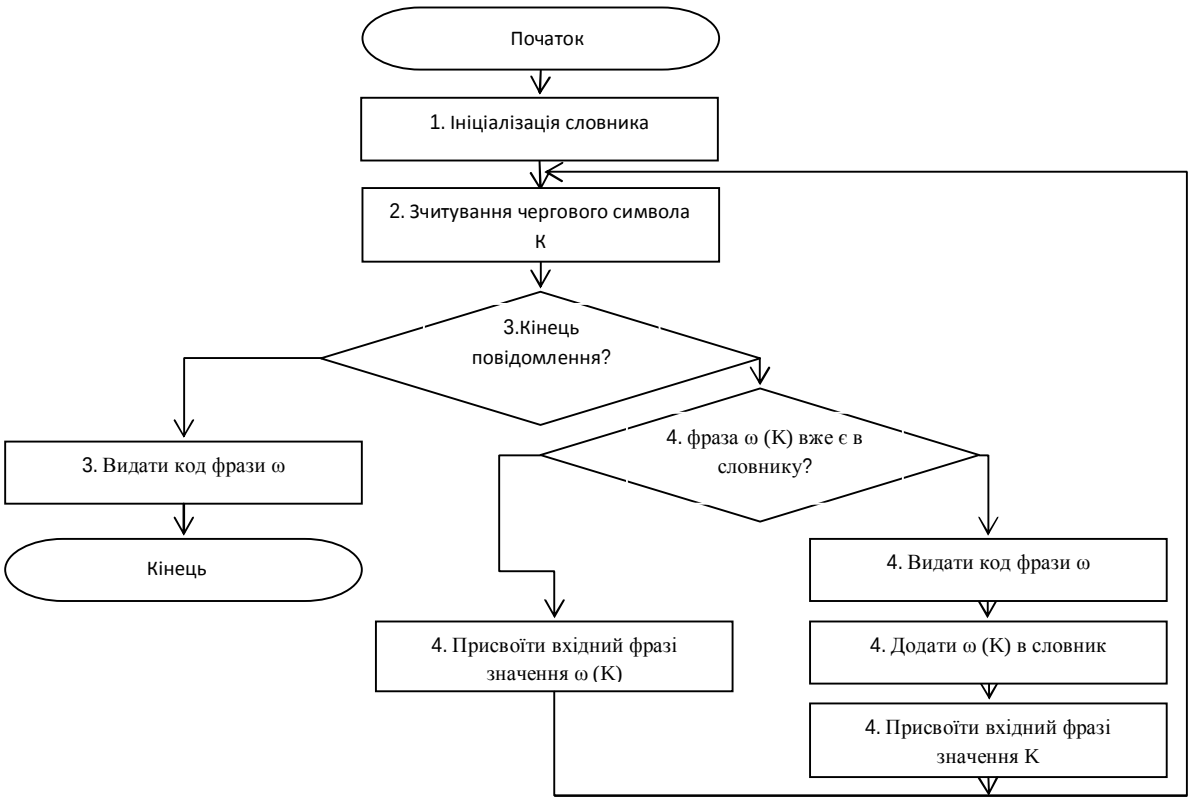

Рис.1. Алгоритм LZW (Розроблено за [5])

Оскільки необхідно буде ущільнювати слова, що складаються з двійкових символів, то словник, який потрібно буде передавати разом з ущільненою інформацією, буде містити лише кількість двійкових розрядів, для яких декодер сам побудує таблицю початкових слів. Це зменшить надлишковість та, завдяки розмірам, ймовірність спотворення інформації необхідної для декодування ущільнення.

Обробка та кодування інформаційного потоку в низхідному каналі стандарту LTE. Для сучасних систем цифрової передачі інформації, формування сигналу в низхідному каналі мереж LTE є досить стандартним (рис. 2) і включає процедури канального кодування, скремблювання, формування символів модуляції, їх розподілу по антенним портам і ресурсним елементам (процедура попереднього кодування) і синтезу OFDM символів [1, 8].

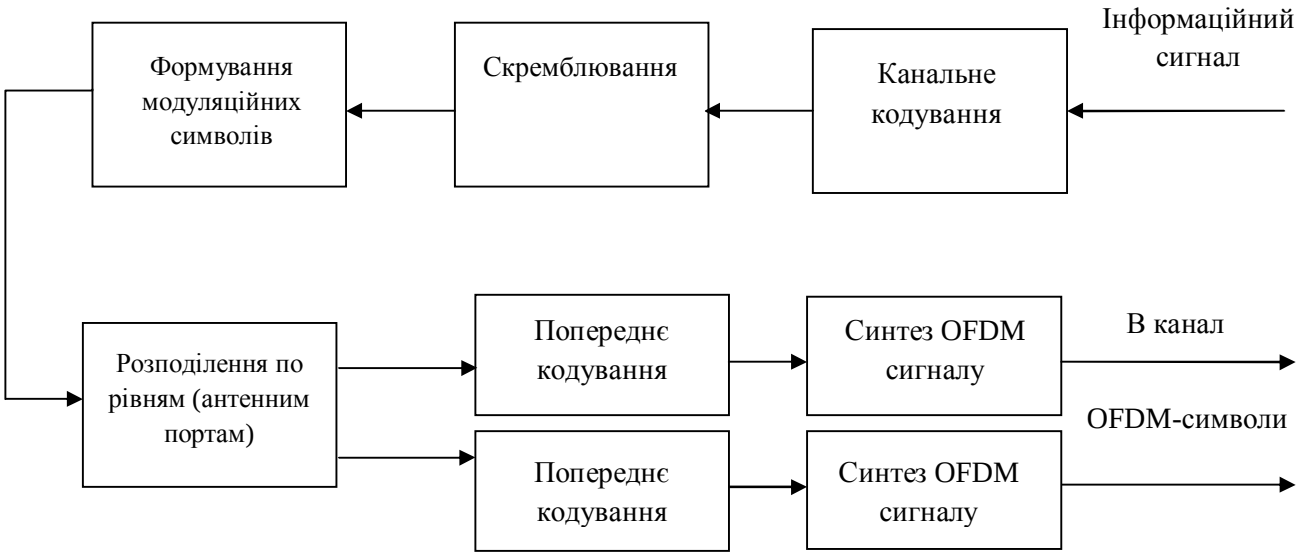

Рис. 2. Схема обробки інформаційного потоку в низхідному каналі стандарту LTE
(Розроблено за [1])

При обробці інформаційного потоку в процесі канального кодування для безпроводових мереж LTE використовується процес сегментації низхідного інформаційного потоку. Ця процедура має місце, якщо розмір транспортного блоку перевищує максимально допустимий розмір кодового блоку. Тоді транспортний блок розбивається на кодові блоки, і до кожного кодового блоку додається поле контрольної суми довжиною 24 біта, при цьому максимальний розмір кодового блоку складає 6144 біта [7].

Блоки з приєднаними контрольними сумами обробляються за допомогою турбо-кодера (рис.3) зі швидкістю кодування 1/3 [1]. Турбо-кодер реалізує завадостійке кодування яке називається «згорткове кодування».

В телекомунікаціях згорткове кодування — вид коригуючого кодування, сутність якого полягає у введенні надмірності в повідомлення, що буде передаватися, тобто у перетворенні m-бітної вхідної послідовності в n-бітну вихідну ($n \geq m$).

При цьому кодуванні кожні n символів містять m інформаційних і k перевірочних. Згорткові коди можуть мати різну надлишковість, але найбільш просто вони реалізуються при $m = k$, тобто коли $n = 2m = 2k$, а надмірність $Rk = m/n = 0,5$. Тоді відносну швидкість передачі R можна записати у вигляді:

$$R = 1 - Rk = m/n = m/2m = 0,5 \quad (1)$$

Значення кожного біта вихідної послідовності залежить від декількох значень вхідних бітів. Для того, щоб значення вихідного біта залежало від декількох вхідних у згортковому кодері застосовуються комірки пам'яті та логічні елементи XOR.

Безперечною перевагою згорткових кодів є можливість виявляти та виправляти групові спотворення, а певним недоліком — звуження області застосування лише потоковими кодами, що при передачі, наприклад, коротких повідомлень в умовах зашумленого каналу створює певні

труднощі. Ці труднощі полягають у неможливості формування відомими методами контрольних та перевірочних символів для символів, які записані на початку та в кінці інформаційних блоків [6].

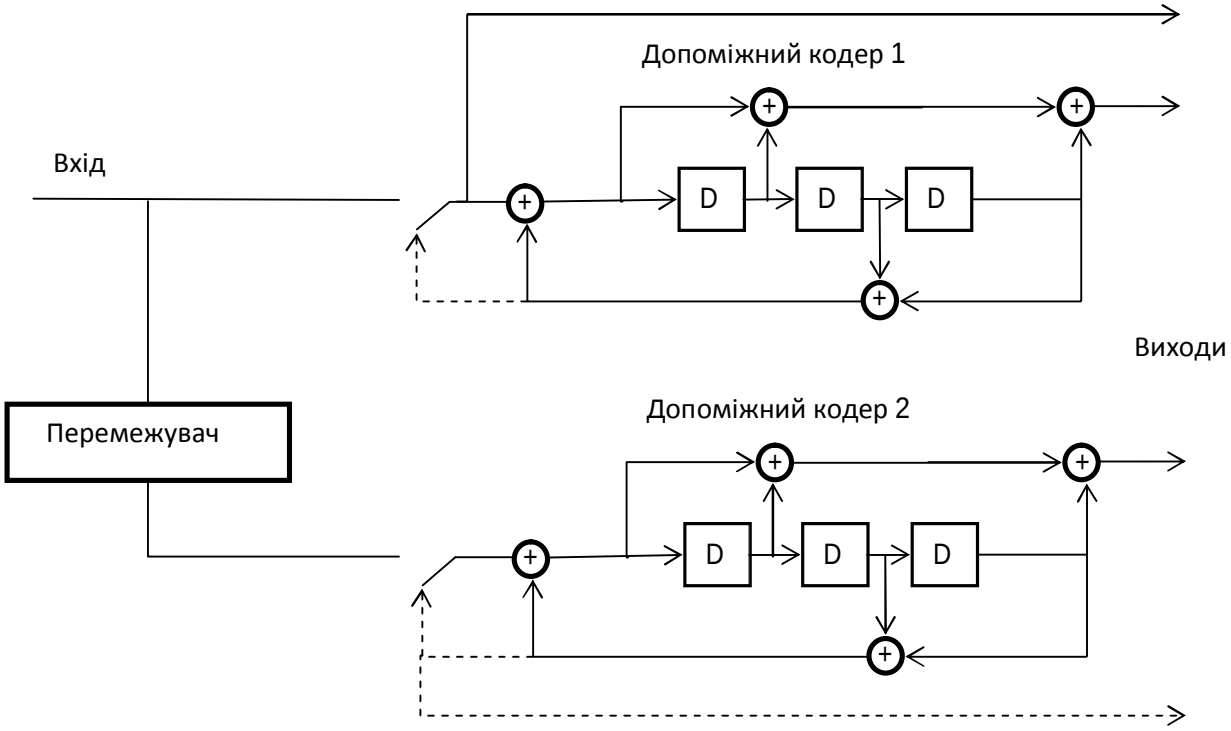

Рис.3 Турбо-кодер
(Розроблено за [1])

Модифікований спосіб обробки інформаційного потоку в низхідному каналі стандарту LTE. Для підвищення завадостікойсті при збереженні, по можливості, завантаженості каналу, пропонується застосувати модифікований спосіб обробки обробки інформаційного потоку в низхідному каналі стандарту LTE, який полягає в тому, що інформаційний потік попередньо ущільнюється, а звільнений після ущільнення інформаційний простір, використовується для відповідного завадостійкого кодування.

Таким чином, для застосування даного способу обробки інформаційного потоку до наведеної вище схеми обробки інформаційного потоку в низхідному каналі стандарту LTE (рис. 2), додається блок, який містить модулі ущільнення та кодування (рис. 4).

Додаткове завадостійке кодування буде залежати від успішності ущільнення. Як алгоритм додаткового кодування доцільно використати згорткове кодування, оскільки для цього вже є фізична реалізація турбо-кодера. Надлишковість, яку додасть кодування повинна дорівнювати звільненим після ущільнення бітам, не змінюючи таким чином загальної довжини інформаційного потоку.

Оскільки заповнення низхідного інформаційного потоку не визначене, то неможливо обрати єдину правильну довжину слова, яка забезпечить найкраще ущільнення.

Отже, необхідно інформаційний потік розбити на кодові слова (сегменти), які будуть початковими словами таблиці ущільнення, а потім ущільнити інформацію для усіх варіантів слів, довжиною 1-9 біт і порівняти отримані результати, обравши найкращий.

Необхідно врахувати, що ущільнення базується на повторенні послідовностей біт, при цьому, для довжини кодового блоку (6144 біт), ми матимемо гарантовані повторення для слів довжиною від 1 (2 різні слова) до 9 біт (512 різних слів). Для слів довжиною 10 і більше біт не гарантується повторень, оскільки слово довжиною 10 біт вже матиме 1024 різних комбінацій слів в початковому словнику. Для отримання гарантованих повторень необхідне виконання умови:

$$2^n < L,$$
(2)

де: n – довжина слова у бітах, а L – кількість слів довжиною n, на які можна розбити кодовий блок.

Разом з цим, кожне збільшення довжини слова до n+1 біт призводить до збільшення кількості різних комбінацій слів початкового словнику (від 2^n до 2^{n+1}), відповідаючи експоненціальному зростанню кількості початкових слів, що призводить до додаткових часових втрат навіть на сучасних потужних пристроях. Отже, створювати варіанти ущільнення доцільно лише для довжин слів, при яких гарантовані повторення. Відповідно, будувати варіанти ущільнення для довжини слова 10 та більше біт надлишково.

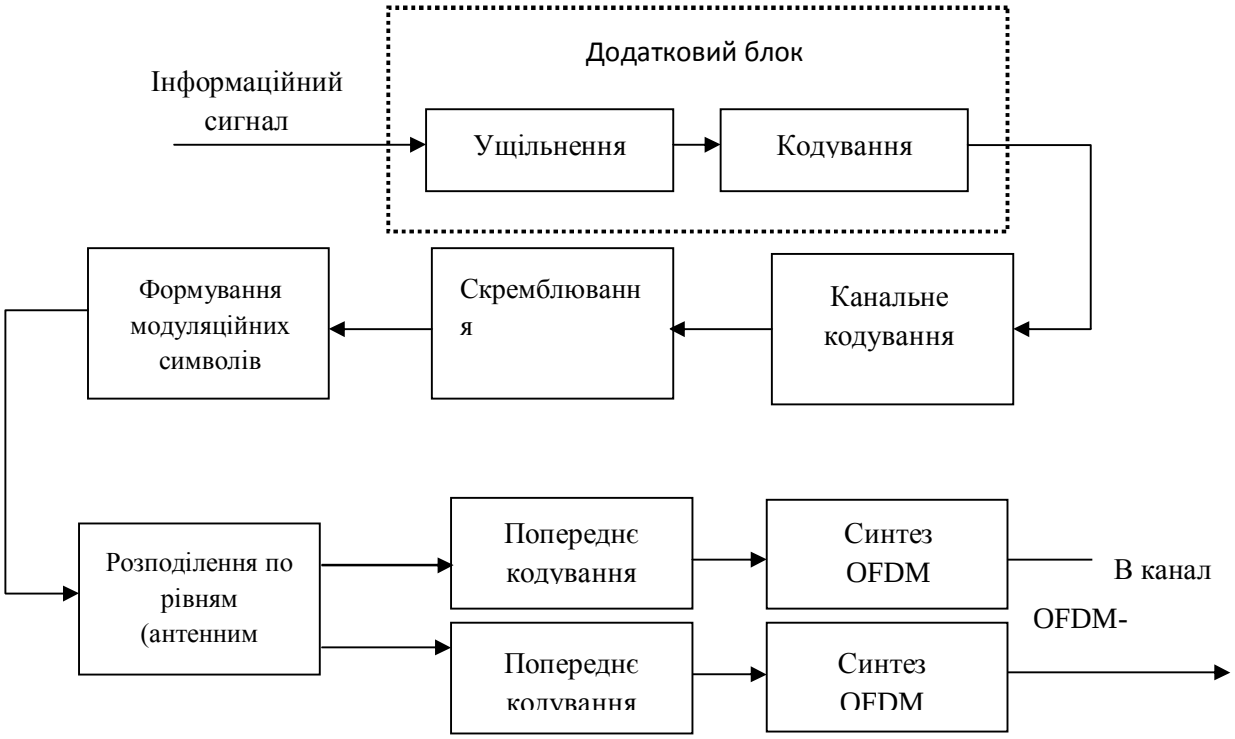

Рис. 4. Модифікована схема обробки інформаційного потоку в низхідному каналі стандарту LTE (Авторська розробка)

Проте якщо відокремити всі слова довжиною 10 біт з кодового блоку і кожне слово буде починатися з одного чи більше нулів, то такий кодовий блок можна ущільнити, оскільки в такому разі для його ущільнення буде достатньо лише половини комбінацій слів довжиною 10 біт, а кількість звільнених біт буде дорівнювати кількості слів, помноженому на кількість нулів, з яких починається кожне слово. Те ж саме справедливо для довжини слова 11 і більше біт, що надає додаткові можливості по швидкій оцінці ефективності ущільнення для довжини слова 10 та більше біт.

Висновки. Таким чином, використовуючи наведений вище спосіб обробки інформаційного потоку в низхідному каналі стандарту LTE, що об'єднує ущільнення та кодування можна досягти підвищення завадостійкості повідомлення для певних варіантів інформаційного потоку в безпроводових мережах LTE, збільшивши навантаження на кодер\декодер, але не збільшуючи навантаження на канал передачі даних. Наприклад, для слова довжиною 6 біт можна отримати мінімально 960, а максимально 1023 повторень на один кодовий сегмент, що надасть можливість ущільнити вхідну інформацію в найкращому випадку з 6144 біт до 1024 біт, а звільнені 5120 біт використати для завадостійкого кодування.

1. Система связи стандарта LTE / Центр Микроэлектронного Проектирования и Обучения [Електронний ресурс]. Режим доступу: http://cmpo.vlsu.ru/edu/2013/A7.pdf

2. Электронные средства сбора, обработки и отображения информациитронные средства сбора, обработки и отображения информаци / Кафедра промышленной электроники ТУСУР [Електронний ресурс]. Режим доступу: http://www.ie.tusur.ru/books/COI/page_08.htm
3. Какие алгоритмы сжатия данных использует RAR? / RARLAB WinRAR [Електронний ресурс]. Режим доступу: http://www.win-rar.ru/support/knowledge/detail.php?ID=952
4. LZMA / Википедия [Електронний ресурс]. Режим доступу: https://ru.wikipedia.org/wiki/LZMA
5. JagaJaga. Алгоритмы LZW, LZ77 и LZ78 / Хабрахабр [Електронний ресурс]. Режим доступу: http://habrahabr.ru/post/132683/
6. Згорткове кодування / Вікіпедія [Електронний ресурс]. Режим доступу: https://uk.wikipedia.org/wiki/%D0%97%D0%B3%D0%BE%D1%80%D1%82%D0%BA%D0%BE%D0%B2%D0%B5_%D0%BA%D0%BE%D0%B4%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F
7. Сжатие без потерь / Википедия [Електронний ресурс]. Режим доступу: https://ru.wikipedia.org/wiki/%D0%A1%D0%B6%D0%B0%D1%82%D0%B8%D0%B5_%D0%B1%D0%B5%D0%B7_%D0%BF%D0%BE%D1%82%D0%B5%D1%80%D1%8C
8. 3GPP TS 36.211 V8.7.0 Technical Specification 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Physical Channels and Modulation(Release 8)
9. Nate Swanner. Old PC Graphics compared to modern SoC's / Android Authority [Електронний ресурс]. Режим доступу: http://www.androidauthority.com/old-pc-graphics-compared-to-modern-tech-185038/