

УДК 621.3

ВИБІР АЛГОРИТМУ КОДУВАННЯ ПРИ ПЕРЕДАВАННІ ІНФОРМАЦІЇ В РОЗПОДІЛЕНИХ КОМП'ЮТЕРНИХ СИСТЕМАХ

*А.Я. Кулик, д-р техн. наук, доцент,
Вінницький національний технічний університет*

У статті розглянуто питання вибору методу та алгоритмів кодування. Визначено критерії вибору, які базуються на оцінюванні ефективної швидкості передавання. Проведено розрахунки ефективності кодування і визначено послідовність дій для забезпечення адаптивного вибору методу кодування або їх комбінації.

Ключові слова: *передавання інформації, кодування.*

В статье рассматриваются вопросы выбора метода и алгоритмов кодирования. Определены критерии выбора, базирующиеся на оценке эффективной скорости передачи. Проведены расчёты эффективности кодирования и определена последовательность действий для обеспечения адаптивного выбора метода кодирования или их комбинации.

Ключевые слова: *передача информации, кодирование.*

ВСТУП

Питанням передавання інформації присвячено багато праць різного наукового рівня [1, 2], оскільки вони складовими частинами входять до наукових праць, де розглядаються більш загальні питання.

Покращання якості передавання може бути досягнуто або за рахунок використання певного способу виявлення та виправлення помилок (FEC – Forward Error Connection), або за допомогою повторного передавання з мажоритарним декодуванням (ARQ – Automatic Repeat Request).

Для виявлення та виправлення помилок використовують різні способи кодування, що базуються на введенні надлишковості. Використовуються коди Хеммінга, Голея, БЧХ тощо, які можуть виправляти різні комбінації помилок залежно від ступеня надлишковості [3]. Ці методи розглядаються для різних умов передавання [4 – 6].

Способи ARQ-кодування також широко використовуються як у класичному вигляді [7], так і з використанням завадозахищених кодів простим повторюванням передавання інформації, якщо виправити помилки неможливо [8].

ПОСТАНОВКА ЗАДАЧІ

Виходячи з цього необхідно провести аналіз особливостей здійснення процедур завадозахищеного кодування/декодування для забезпечення ефективного використання каналу зв'язку і побудувати комплекс математичних моделей. Потрібно визначити основні характеристики

блоку даних, що передається, при використанні (n, k) -кодів, зв'язавши їх з параметрами каналу зв'язку. Необхідно визначити оптимальну кількість повторів при використанні методу мажоритарного декодування з урахуванням параметрів каналу та на підставі отриманих співвідношень вибрати критерії використання необхідного методу кодування. Доцільно визначити перспективні методи завадозахищеного кодування при забезпеченні необхідних умов передавання і оцінити їх ефективність як з точки зору використання каналу зв'язку, так і з точки зору криптографічної стійкості без використання додаткових алгоритмів шифрування даних.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

У літературі [9] докладно розглянуті особливості передавання інформації в цьому режимі, але відкритим залишається питання щодо кількості повторювань кодової комбінації для забезпечення завданої імовірності передавання. Крім цього, там розглядаються алгоритми з двократним передаванням, що, в принципі, виключає мажоритарність виправлення помилок.

Відомі два варіанти реалізації алгоритму передавання інформації з повторюванням [10, 11]. У першому випадку r разів повторюється кожний елемент кодової комбінації, а в другому – r разів повторюється кодова комбінація. Для цих випадків формуються матриці, які дозволяють здійснювати декодування прийнятої комбінації.

$$x_{1,i}^T = (x_1, x_2, x_3, \dots, x_r). \quad (1)$$

Декодування реалізується за принципом двійкового додавання

$$x_{1,i} = x_1 \oplus x_2 \oplus x_3 \oplus \dots \oplus x_r. \quad (2)$$

У другому випадку матриця має вигляд

$$x_2 = \begin{pmatrix} x_{11} & x_{12} & \dots & x_{1n} \\ x_{21} & x_{22} & \dots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{r1} & x_{r2} & \dots & x_{rn} \end{pmatrix} \quad (3)$$

і відповідно декодування здійснюється як

$$x_2 = (x_1, x_2, x_3, \dots, x_n), \quad (4)$$

де

$$x_{1,i} = x_{11} \oplus x_{21} \oplus x_{31} \oplus \dots \oplus x_{r1};$$

$$x_{2,i} = x_{12} \oplus x_{22} \oplus x_{32} \oplus \dots \oplus x_{r2};$$

$$x_{n,i} = x_{1n} \oplus x_{2n} \oplus x_{3n} \oplus \dots \oplus x_{rn}.$$

Відмінність у цих методах полягає лише в апаратних витратах для зберігання значень, отриманих з каналу зв'язку. У першому випадку це r елементарних комірок пам'яті, а в другому – $n \times r$. З урахуванням особливостей передавання інформації, які характеризуються використанням процесорної техніки та обробленням інформації в режимі реального часу, такі апаратні витрати суттєвого значення не мають і на складність побудови пристрою приймання практично не впливають,

оскільки оброблення доцільно здійснювати в програмному режимі [12]. Ефективна швидкість передавання знижується в r разів:

$$R_C = \frac{\nu}{r \cdot n}. \quad (5)$$

Особливістю алгоритму передавання інформації з повторюванням є те, що він забезпечує декореляцію помилок, тобто імовірність виникнення помилки описується формулою Бернуллі для каналу з незалежними помилками. Визначивши імовірність правильного приймання кодової комбінації

$$p_{np} = 1 - p_{ном} = 1 - \sum_{i=1}^n C_n^i \cdot p_0^{i \cdot r} \cdot (1 - p_0)^{(n-i)r}, \quad (6)$$

взявши окрему похідну $\left(\frac{\partial p_{np}}{\partial r}\right)$ і прирівнявши її до нуля, можна отримати рівняння

$$\begin{aligned} \left(\frac{\partial p_{np}}{\partial r}\right) = & - \sum_{i=1}^n C_n^i \cdot i \cdot p_0^{i \cdot r} \cdot (1 - p_0)^{(n-i)r} \cdot \ln p_0 + \\ & + (n - i) \cdot p_0^{i \cdot r} \cdot (1 - p_0)^{(n-i)r} \cdot \ln(1 - p_0). \end{aligned} \quad (7)$$

Розв'язання цього рівняння дає змогу визначити кількість повторювань r кодової комбінації довжини n , оптимальну для імовірності спотворення елементарного сигналу p_0 . Результати розрахунків зведені в табл. 1.

Таблиця 1 - Співвідношення параметрів передавання

Імовірність помилки, p_0	Розраховане значення r
10^{-6}	0,899
10^{-5}	1,078
10^{-4}	1,346
10^{-3}	1,69
10^{-2}	2,466
10^{-1}	3,015

Використання у вигляді кодових комбінацій, що передаються, надлишкових (n, k) -кодів дозволяє суттєво збільшити імовірність передавання. Оброблення таких повторюваних кодових комбінацій за критерієм “один з двох” або “два з двох” [13] призводить або до зменшення імовірності передавання (у першому випадку), або до часткової втрати інформації (у другому). Це пов'язано з тим, що за наявності помилки в одній із кодових комбінацій знищуються обидві. Такий недолік призводить до порушення пріоритетності параметрів – імовірність передавання інформації завжди повинна мати вищий пріоритет, ніж швидкість або час передавання, оскільки головною метою побудови системи є саме імовірне передавання інформації.

Для цього випадку імовірність правильного приймання кодової комбінації становить

$$p_{np} = 1 - p_{ном} = 1 - \sum_{i=t+1}^n C_n^i \cdot p_0^{i \cdot r} \cdot (1 - p_0)^{(n-i)r}. \quad (8)$$

Аналогічно, наведеному вище, взявши окрему похідну $\left(\frac{\partial p_{np}}{\partial r}\right)$ і прирівнявши її до нуля, можна отримати рівняння

$$\left(\frac{\partial p_{np}}{\partial r}\right) = - \sum_{i=t+1}^n C_n^i \left(i \cdot p_0^{i \cdot r} \cdot (1 - p_0)^{(n-i)r} \cdot \ln p_0 + (n-i) \cdot p_0^{i \cdot r} \cdot (1 - p_0)^{(n-i)r} \cdot \ln(1 - p_0) \right). \quad (9)$$

Розв'язання цього рівняння дає можливість визначити кількість повторювань r кодової комбінації довжини n , оптимальну для імовірності спотворення елементарного сигналу p_0 при використанні у вигляді кодової комбінації, що передається, надлишкових (n, k) -кодів. Результати розрахунків зведені в табл. 2. Аналіз показує, що суттєва різниця у необхідній кількості повторювань визначається лише для $p_0 = 10^{-3}$, хоча співвідношення (кількість інформаційних розрядів) / (загальна кількість розрядів) для розглянутих випадків відрізняється дуже суттєво.

Таблиця 2 - Співвідношення параметрів передавання

Імовірність помилки, p_0	Розраховане значення r ($t = 1$)	Розраховане значення r ($t = 2$)
10^{-6}	0,56	0,425
10^{-5}	0,671	0,49
10^{-4}	0,801	0,612
10^{-3}	1,066	0,815
10^{-2}	1,503	1,162
10^{-1}	2,258	1,902

Отримане з рівнянь (7) або (9) значення r необхідно округлити зверху до найближчого непарного числа. Лише в цьому випадку буде зберігатися принцип мажоритарності [10].

Для цього випадку ефективна швидкість передавання буде складати

$$R_C = \frac{k_0 \cdot \nu}{n \cdot r}. \quad (10)$$

На рис. 1 та 2 подані залежності помилок передавання від довжини кодової комбінації відповідно при триразовому та п'ятиразовому повторюванні.

Відповідно до цього доцільно визначити процедуру зміни алгоритму кодування, як це подано на рис. 3. Оскільки передавання інформації з повторюванням використовується в складних ситуаціях, то за критерій зміни алгоритму кодування доцільно вибрати досягнення імовірністю безпомилкового передавання p_{np} мінімально вибраного граничного значення.

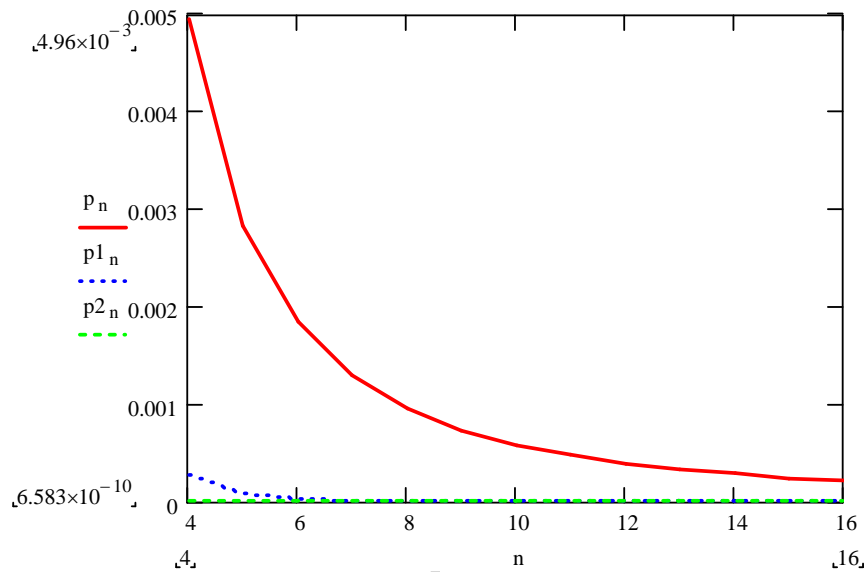


Рисунок 1 - Залежності імовірностей безпомилкового передавання від довжини кодової комбінації при триразовому повторюванні: p – передавання інформаційних k розрядів; p_1 – використання кодової комбінації з виправленням однієї помилки; p_2 – використання кодової комбінації з виправленням двох помилок

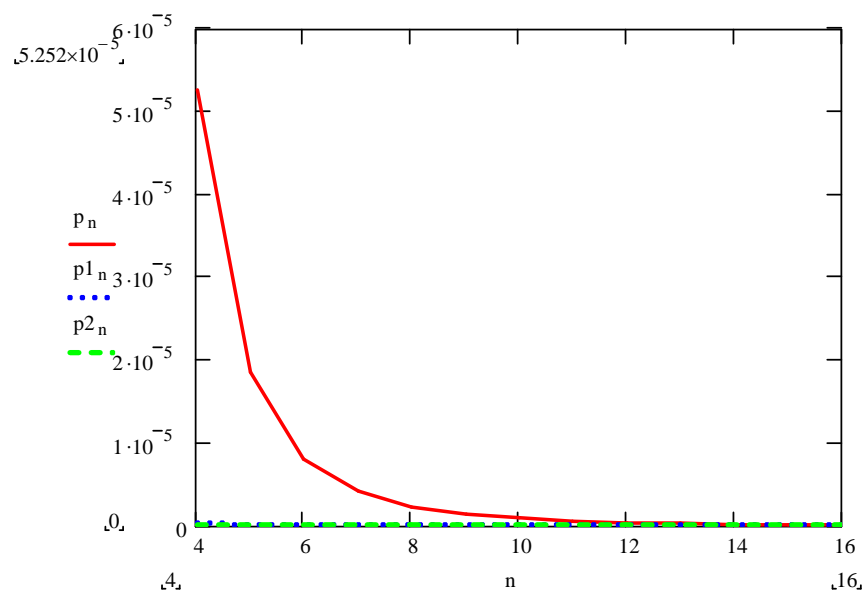


Рисунок 2 - Залежності імовірностей безпомилкового передавання від довжини кодової комбінації при п'ятиразовому повторюванні

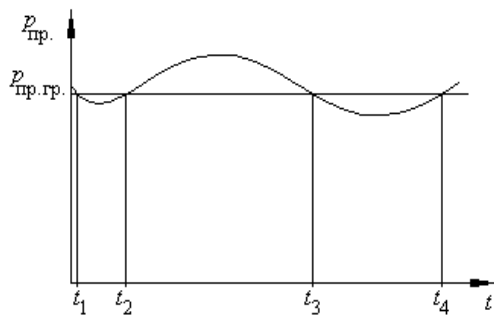


Рисунок 3 - Процедура зміни методу кодування під час передавання інформації з повторюванням та мажоритарним декодуванням

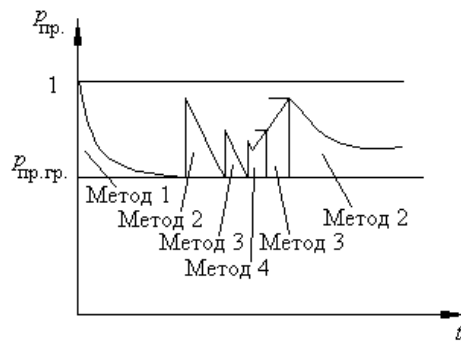


Рисунок 4. - Загальна процедура зміни методу кодування під час передавання інформації

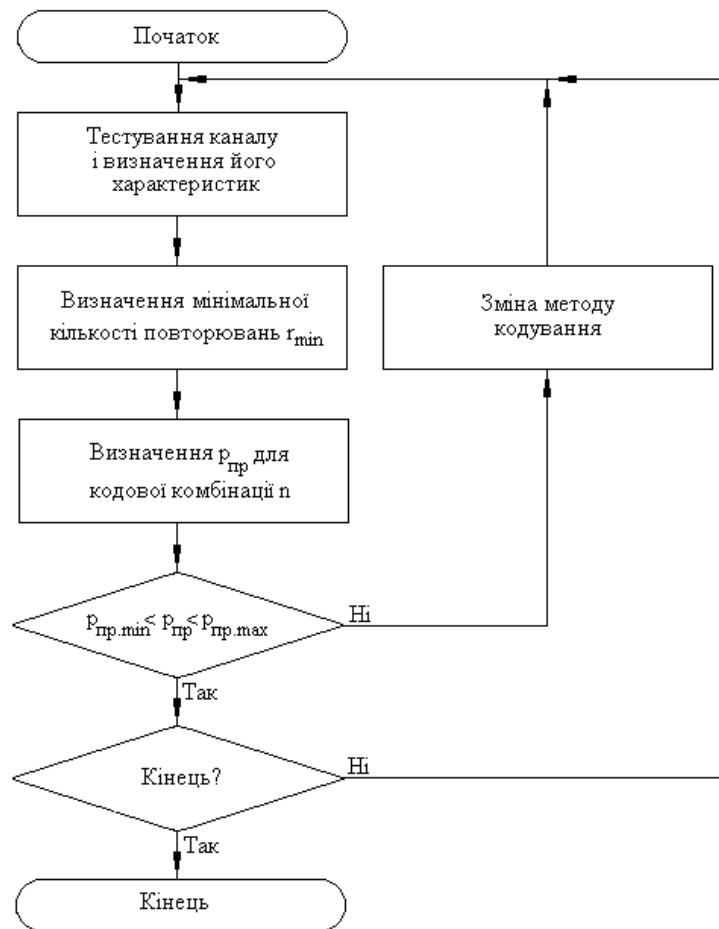


Рисунок 5 - Послідовність дій для вибору методу з повторюванням кодової комбінації за імовірності її безпомилкового передавання

Якщо просте збільшення кількості повторювань інформаційних розрядів не дає позитивного ефекту, то необхідно у вигляді кодової комбінації використовувати код (n, k) .

Наведений аналіз дозволяє визначити процедуру адаптивного вибору методу кодування. Критерієм вибору методу доцільно вважати імовірність безпомилкового передавання p_{np} (рис. 4), оскільки співвідношення середнього значення кількості інформації k/n на одну кодову комбінацію пов'язано з цим параметром.

На рис. 5 подана послідовність дій для вибору методу з повторюванням кодової комбінації за імовірністю її безпомилкового передавання. Як і для (n, k) -кодів вибір може здійснюватися як у прямому, так і в зворотному напрямку – із збільшенням або із зменшенням коригувальної здатності коду.

Досягнення мінімально допустимого граничного значення $p_{np,gr}$ вимагає зміни методу кодування, причому з усіх методів, які здатні забезпечити задану імовірність безпомилкового передавання, потрібно вибирати метод, який забезпечує максимальну ефективну швидкість R_C .

Аналіз наведених графіків безпомилкового передавання інформації (рис. 7) для вищезазначених методів залежно від імовірності спотворення елементарного сигналу кодової комбінації p_0 показує, що границя мінімально допустимого значення pp чітко визначає різницю у потенційній коригувальній здатності методів кодування, що дозволяє ввести їх чітку градацію за цим показником:

- коди з повторюванням і використанням (n, k) -кодів у вигляді кодової комбінації;
- коди з повторюванням інформаційних розрядів кодової комбінації;
- (n, k) -коди з виправленням різної кількості помилок.

На жаль, найбільш ефективні щодо імовірності передавання методи кодування мають низьку ефективну швидкість передавання, що ілюструє рис. 8. Але, враховуючи пріоритетність задач, про яку було зазначено вище, необхідно вибирати той метод кодування, який забезпечує необхідну імовірність безпомилкового передавання. Якщо це забезпечують декілька методів, то доцільно здійснювати подальший вибір вже за критерієм найбільшої швидкості передавання, як це ілюструє рис. 9. Допоміжними критеріями вибору методу кодування можуть також бути складність програмної, апаратної чи комбінованої реалізації або інші аналогічні показники.

Таким чином, отримано математичні моделі, які пов'язують імовірність ідентифікації інформативного сигналу зі співвідношенням $сигнал/шум$, та математичні моделі, які дозволяють визначити максимальне значення ефективної швидкості передавання для реальних умов, метод та параметри кодування. Це характеризує локальні оптимуми цільової функції, яка описує процес передавання інформації і відповідає поставленій задачі.

Отримані параметри використовуються для розробленої моделі комп'ютерної системи передавання інформації, яка піддається аналізу з використанням класичних методів теорії автоматичного управління.

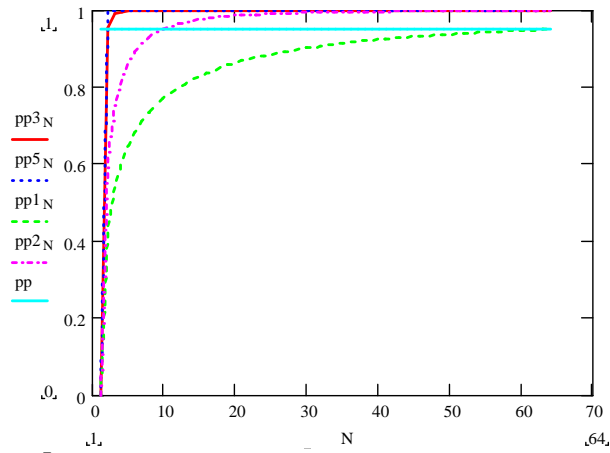


Рисунок 6 - Імовірності виникнення помилок залежно від довжини кодової комбінації: pp_3 – трикратне передавання інформаційних розрядів; pp_5 – п'ятикратне передавання інформаційних розрядів; pp_1 – виправлення однієї помилки; pp_2 – виправлення двох помилок

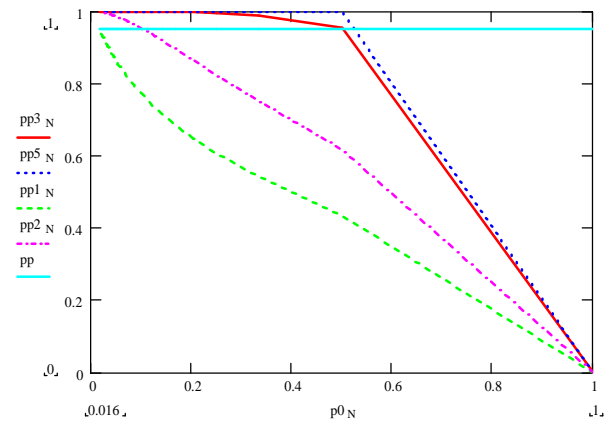


Рисунок 7 - Імовірності безпомилкового передавання залежно від імовірності спотворення елементарного сигналу кодової комбінації

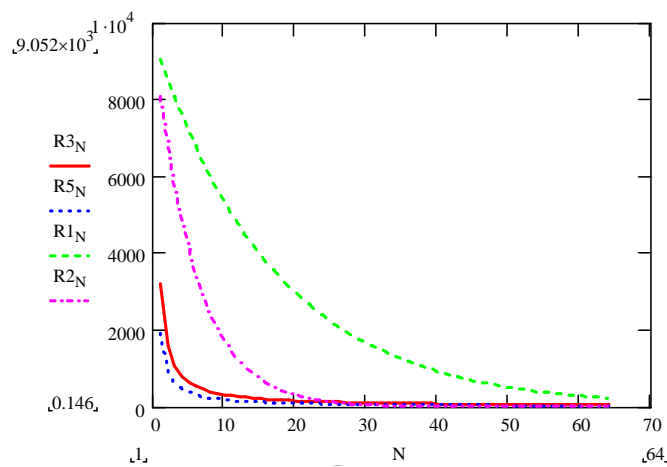


Рисунок 8 - Ефективна швидкість передавання залежно від довжини кодової комбінації: R_3 – триразове передавання інформаційних розрядів; R_5 – п'ятиразове передавання інформаційних розрядів; R_1 – виправлення однієї помилки; R_2 – виправлення двох помилок

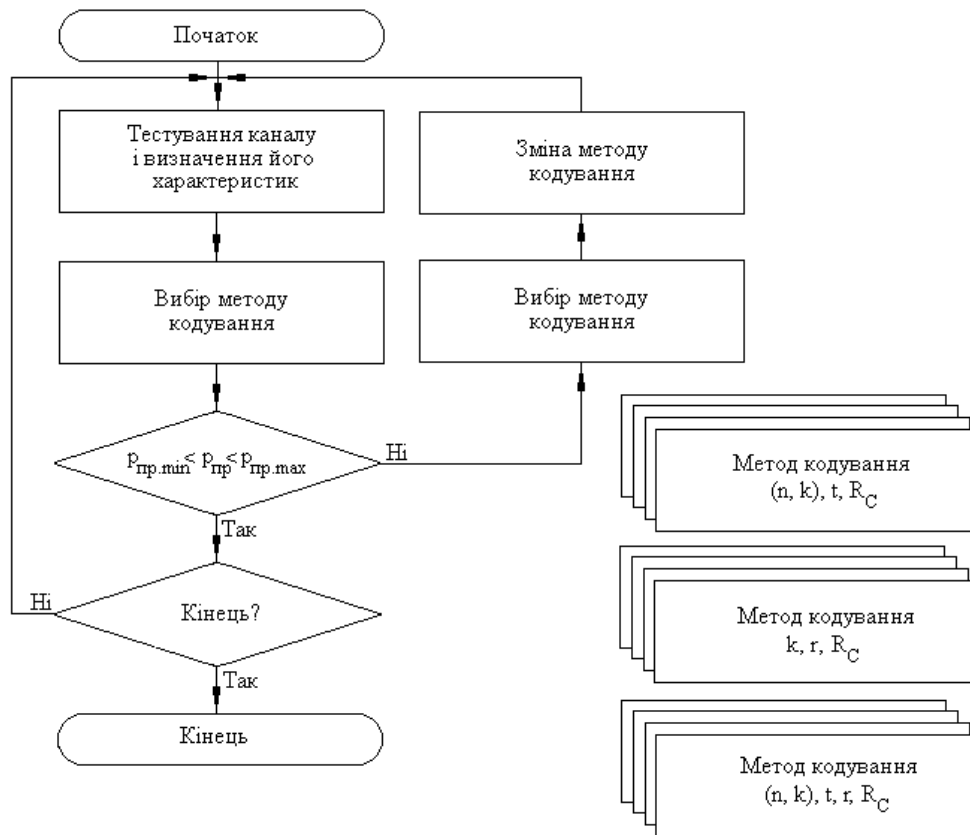


Рисунок 9 - Послідовність дій для вибору методу кодування за основним та допоміжним критеріями

ВИСНОВКИ

Таким чином, розв'язано задачу оцінювання ефективності кодування з урахуванням можливості вибору методів побудови і параметрів кодів для використання у проблемно-орієнтованих розподілених комп'ютерних системах та мережах на каналному рівні взаємодії відкритих систем. Розроблено математичну модель, співвідношення якої пов'язують ефективну швидкість передавання з параметрами каналу, передавання і необхідною кількістю повторювань при мажоритарному декодуванні. На відміну від існуючих класичних, запропоновано комбіноване кодування завадозахищеним (n, k) -кодом з мажоритарним і визначені умови ефективного використання завадозахищеного, мажоритарного і комбінованого кодування в умовах адаптивного передавання інформації.

SUMMARY

CHOICE OF ALGORITHM OF CODING BY TRANSFER OF THE INFORMATION IN THE ALLOCATED COMPUTER SYSTEMS

Kulyk A.Y.

In the article the questions of a choice of a method and algorithms of coding are considered. The criteria of a choice based on an estimation of effective speed of transfer are determined. The calculations of efficiency of coding are carried out and the sequence of actions for maintenance of an adaptive choice of a method of coding or their combination is determined.

Key words: transfer of the information, coding.

СПИСОК ЛІТЕРАТУРИ

1. Мак-Вильямс Ф.Дж. Теория кодов, исправляющих ошибки / Ф.Дж. Мак-Вильямс, Н.Дж. Слоэн. – М.: Связь, 1979. – 744 с.
2. Муттер В.М. Основы помехоустойчивой телепередачи информации / В.М. Муттер. – Л.: Энергоатомиздат, 1990. – 288 с.
3. Березюк Н.Т. Кодирование информации (двоичные коды) / Н.Т. Березюк, А.Г. Андрущенко, С.С. Мощицкий. – Харьков: Вища школа, 1978. – 252 с.
4. Давидов А.В. Сравнительный анализ характеристик сверточных кодов, использующих мягкие и жесткие метрики / А.В. Давидов, А.А. Мальцев // Радиотехника: научн. конф. по радиотехнике, Нижний Новгород, 2002. – Н.Новгород: ННГУ, 2002. – С. 261-262.
5. Моделирование вероятности ошибок кодирования ФМ сигналов с логнормальными амплитудными флуктуациями в гауссовом шуме: тр. 5-й Междунар. конф. «Цифровая обработка сигналов и её применение (DSPА-2003)» [Электронный ресурс] / Г.А. Андреев, М.Н. Андрианов. – СПб.: ЗАО АВТЭКС, 2003. – Режим доступа: <http://www.autex.spb.ru>
6. Закономерность изменения эффективности накопления сигнала двоичного кода [Электронный ресурс] / В. Ручкин. – Режим доступа: http://www.otwet.ru/study/raznoe/zakon_eff.html
7. Тесля В.Я. Современные подходы к построению сетевых структур связи и управлению трафиком / В.Я. Тесля, А.Л. Бабосюк // Зв'язок. – 2004. – № 4. – С. 67 – 69.
8. Развитие информационных технологий на новых математических принципах, обеспечивающих гарантированный уровень обслуживания [Электронный ресурс] / С.А. Осмоловский. – Режим доступа: <http://www.stokos.ru/stat13.htm>
9. Кузьмин И.В. Кодирование и декодирование в информационных системах / И.В. Кузьмин, В.И. Ключко, В.А. Литвин. – К.: Вища школа, 1985. – 190 с.
10. Кулик А. Алгоритм адаптації до умов передавання інформації каналом зв'язку / А.Кулик, С.Кривогубченко, М.Компанець, Д.Кривогубченко // Контроль і управління в складних системах: VI міжнар. конф., Вінниця, 8 – 12 жовтня 2001 р. – Вінниця: ВДТУ, 2001. – С. 151 – 152.
11. Пат. 48411 А України, МПК⁷ Н 03 М 13/00. Спосіб передавання дискретної інформації з адаптацією параметрів каналу зв'язку та пристрій для його реалізації / Кветний Р.Н., Кулик А.Я., Кривогубченко С.Г. та ін. (Україна); ВДТУ. – № 2001064414; заявл. 23.06.2001; опубл. 15.08.2002; Бюл. № 8. – 8 с.
12. Проектування мікропроцесорних засобів автоматики і управління: навч. посіб. [для студ. вищ. навч. закл.] / А.Я. Кулик, С.Г. Кривогубченко, М.М. Компанець. – Вінниця: ВДТУ, 2001. – 130 с.
13. Элементы теории передачи дискретной информации / под ред. Пуртова Л.П. – М.: Связь, 1972. – 232 с.

Надійшла до редакції 20 серпня 2010 р.