

УДК 004.75

В. В. ЯЦКІВ

Тернопільський національний економічний університет, Тернопіль

**МОДИФІКОВАНІ КОРЕКТУЮЧІ КОДИ СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ ТА ЇХ ЗАСТОСУВАННЯ**

**Анотація.** В статті розроблено модифікований коректуючий код системи залишкових класів, який має спрощену процедуру кодування; показано можливість використання даного коду у протоколах передавання даних безпроводних сенсорних мереж.

**Ключові слова:** безпроводні сенсорні мережі, стандарт IEEE 802.15.4, система залишкових класів, коректуючі коди.

**Аннотация.** В статье разработан модифицированный корректирующий код системы остаточных классов, который имеет упрощенную процедуру кодирования. Показана возможность использования данного кода в протоколах передачи данных беспроводных сенсорных сетей.

**Ключевые слова.** беспроводные сенсорные сети, стандарт IEEE 802.15.4, система остаточных классов, корректирующая коды.

**Abstract.** The modified corrective code in Residue Number System with simplified coding procedure is elaborated in the article. The possibility of the use of this code in data transmission protocols in wireless sensor network is shown.

**Key words:** Wireless Sensor Networks; IEEE 802.15.4; Residue Number System; Correcting Code.

**Вступ**

Безпроводні сенсорні мережі (БСМ) використовуються в системах екологічного, технічного та медичного моніторингу [1]. Основним стримуючим фактором впровадження БСМ в системах промислової автоматизації є низька надійність передавання даних спричинена в першу чергу високим рівнем перешкод на промислових підприємствах. Отже, підвищення надійності та зменшення часу затримки передавання повідомлень є основними вимогами для успішного функціонування БСМ в системах автоматизації промислових підприємств, які працюють в реальному часі. Для підвищення надійності роботи БСМ використовують процедуру виявлення помилок та повторну передачу спотворених пакетів або коректуючі коди. Однак використання повторної передачі пакетів в умовах каналу з високою ймовірністю помилок призводить до зменшення загальної пропускну здатності і не може гарантувати жорсткі вимоги до часу затримки передачі [2, 3].

Контроль цілісності пакетів даних в БСМ, які відповідають стандарту IEEE 802.15.4, здійснюється на основі циклічного надлишкового коду (Cyclic Redundancy Check, CRC). Перевірочна послідовність Frame check sequence (FCS) має довжину 16 біт і розраховується по MAC header (MHR) і MAC payload частині кадру (рис.1). Розрахунок FCS проводиться на основі стандартного полінома генератора степені 16 [4]:

$$G_{16}(x) = x^{16} + x^{12} + x^5 + 1.$$

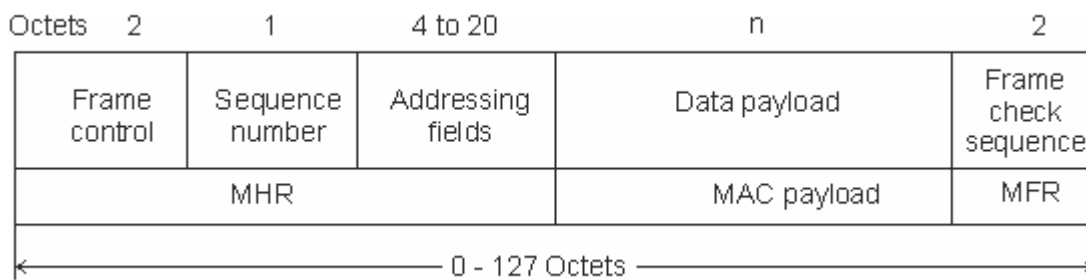


Рисунок 1 – IEEE 802.15.4 Data Frame structure

Використання циклічного надлишкового коду дозволяє тільки виявити наявність помилки в зазначених блоках даних. При виявленні помилки відсилається запит на повторну передачу пошкодженого (спотвореного) пакету.

Враховуючи обмежені функціональні характеристики безпроводних сенсорів, актуальною є проблема вибору коректуючих кодів для застосування в БСМ.

До коректуючих кодів в БСМ висуваються наступні вимоги:

- низька складність алгоритмів кодування / декодування;
- низькі апаратні вимоги до реалізації алгоритмів (швидкодія мікроконтролера, обсяг пам’яті);
- адаптивна зміна кількості перевірочних символів при зміні параметрів каналу.

В [2, 5] запропоновано використовувати для виправлення помилок в БСМ коди Ріда – Соломона. Однак при використанні кодів Ріда-Соломона існує проблема зміни (збільшення /зменшення) числа перевірюваних символів. Наприклад, при переході від  $g$  перевірюваних символів до більшого числа  $g'$  всі перевірювані символи необхідно перерахувати [6].

В даній роботі розроблено модифіковані коди СЗК, які пропонується використати для підвищення надійності передачі даних в БСМ.

#### Коректуючі коди системи залишкових класів

Оброблення та передавання даних в системі залишкових класів (СЗК) має ряд переваг, завдяки незалежності, малорозрядності та рівноправності залишків, можливості паралельного виконання арифметичних операцій. Незважаючи на це, в даний час, СЗК використовується тільки при вирішенні деяких спеціалізованих задач, що обумовлено необхідністю перетворення двійкового коду, в якому працюють універсальні комп'ютери та пристрої оброблення даних в код СЗК та зворотного перетворення при представлення інформації користувачу.

Крім вище названих переваг СЗК для оброблення даних, в СЗК також розроблені ефективні коректуючі коди, здатні виявляти та виправляти пакети помилок [7 - 9]. Однак для їх використання в існуючих цифрових системах передавання даних, зокрема в БСМ, необхідно попередньо конвертувати дані в СЗК, що потребує додаткових затрат часу та обчислювальних ресурсів.

Розглянемо систему з основами  $p_1, p_2, \dots, p_1, \dots, p_n$ , в якій число  $A$  представляється залишками

$$A = (b_1, b_2, \dots, b_i, \dots, b_n),$$

де  $b_i = A \pmod{p_i}$ ,

і введемо додаткову контрольну основу  $p_{n+1} > p_n$ .

У відомих коректуючих кодах СЗК ( $R$  – коди СЗК) значення контрольного розряду визначається [6]

$$b_{n+1} = A \pmod{p_{n+1}},$$

тобто обчислення контрольного розряду потребує звернення до початкового значення числа  $A$ .

$R$  – коди СЗК мають обмеження, які накладаються умовою вибору зростаючої послідовності взаємно простих модулів. При цьому необхідно щоб перевірювані модулі були однакової розрядності. В іншому випадку виникає проблема ефективного збереження перевірюваних символів. Враховуючи викладене вище, більш доцільним є використання модифікованого коректуючого коду СЗК.

#### Модифікований коректуючий код СЗК

В запропонованих коректуючих кодах СЗК пакет даних в двійковому коді, який підлягає передаванню, розбивається на блоки однакової довжини (тетради або байти)

$$a_j^1 \dots a_3^1 a_2^1 a_1^1 a_0^1, a_j^2 \dots a_3^2 a_2^2 a_1^2 a_0^2, a_j^i \dots a_3^i a_2^i a_1^i a_0^i, \dots, a_j^k \dots a_3^k a_2^k a_1^k a_0^k,$$

де  $a^i$  – розряд даних в двійковому коді,  $j = 4, 8$ .

При цьому значення контрольного розряду визначається

$$\bar{b}_{k+1} = (v_1 \cdot b_1 + v_2 \cdot b_2 + \dots + v_i \cdot b_i + \dots + v_k \cdot b_k) \pmod{p} \quad (1)$$

де  $v_i$  – коефіцієнти лінійної форми взаємно прості з  $p$ ;  $b_i$  – байт даних в двійковій або десятковій системі числення,

$$b_i = a_7^i \dots a_3^i a_2^i a_1^i a_0^i = a_0 \cdot 2^0 + a_1 \cdot 2^1 + a_2 \cdot 2^2 + a_3 \cdot 2^3 + \dots + a_7 \cdot 2^7.$$

Припустимо, що в процесі передавання відбулась помилка в одному з блоків даних (спотворення зазнали від 1 до 8 двійкових розрядів) і замість числа  $A$  отримали  $A'$

$$A' = (b_1, b_2, \dots, b_i', \dots, b_k, \bar{b}_{k+1}).$$

Значення контрольного розряду обчислюємо за формулою

$$\bar{b}_{k+1}' = (v_1 \cdot b_1 + v_2 \cdot b_2 + \dots + v_i \cdot b_i' + \dots + v_k \cdot b_k) \pmod{p}.$$

Знаходимо різницю між розрахованим і прийнятим контрольним символом  $\delta = \bar{b}_{k+1}' - b_{k+1}$ . Отже, при  $\delta = 0$  – помилка відсутня; при  $\delta \neq 0$  – відбулася помилка.

Для виявлення помилки в будь-якому з блоків необхідно, щоб кожному значенню  $\delta_i$  відповідало одне значення помилки  $X_i$ . Для виконання даної умови коефіцієнти лінійної форми повинні бути взаємно прості з  $p$ , а значення контрольного модуля повинно дорівнювати  $p \geq 2^m$ , де  $m$  – кількість двійкових розрядів у вибраному блоці даних (при розбитті пакету даних на байти  $m = 8$ ).

Для оцінки ефективності коректуючого коду необхідно знати зв'язок між надлишковістю і можливістю виявляти або виправляти помилки.

Мінімальна кодова відстань модифікованого коду СЗК  $d_{\min} = n - k + 1$ , де  $n$  – загальна довжина коду,  $k$  – кількість інформаційних блоків. Отже, модифікований код СЗК може виявляти всі сукупності із  $t$  або меншої кількості помилок при умові, що  $d_{\min} \geq t + 1$ ; при значенні  $d_{\min} \geq 2 \cdot t + 1$  – даний код може виправляти всі сукупності із  $t$  або меншої кількості помилок. При введенні двох контрольних розрядів даний код забезпечить гарантоване виправлення помилок в одному блоці даних.

При необхідності використання двох і більше контрольних розрядів є наступні варіанти вибору коефіцієнти лінійної форми:

- 1) однакові контрольні модулі і різні коефіцієнти лінійної форми;
- 2) різні модулі і однакові коефіцієнти лінійної форми.

В таблиці 1 наведено значення коефіцієнтів лінійної форми, необхідних для розрахунку перевірочних чисел, згідно (1). Оскільки модулі  $p_i$  вибрані різні то коефіцієнти мають бути взаємно прості числа з  $p_i$ .

Таблиця 1 – Значення коефіцієнтів модифікованих кодів СЗК при різних значеннях контрольних модулів

Перевірочне число, $b_{k+j}$	Коефіцієнти $v_i$	Модуль $p_i$
$b_{k+1}$	11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73	463
$b_{k+2}$	11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73	467
$b_{k+3}$	11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73	479
$b_{k+4}$	11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73	487
$b_{k+5}$	11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73	491
$b_{k+6}$	11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73	499
$b_{k+7}$	11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73	503
$b_{k+8}$	11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73	509

Другий варіант вибору коефіцієнтів лінійної форми наведено в таблиці 2. В цьому прикладі модулі  $p_i$  вибрані однакові, відповідно, коефіцієнти лінійної форми мають бути різні числа, взаємно прості з  $p_i$ .

Розглянемо приклад виявлення помилок з використанням модифікованого коду СЗК. В якості контрольного модуля виберемо  $p = 16$ ; коефіцієнти лінійної форми:  $v_1 = 3$ ,  $v_2 = 5$ ,  $v_3 = 7$ , інформаційні блоки даних в десятковій системі числення:  $b_1 = 2$ ,  $b_2 = 10$ ,  $b_3 = 9$ . Обчислимо значення контрольного розряду  $\bar{b}_{k+1} = (3 \cdot 2 + 5 \cdot 10 + 7 \cdot 9) \pmod{16} = 7$ ; введемо помилку в першому блоці  $b'_1 = 4$ , при цьому значення контрольного розряду дорівнює  $\bar{b}'_{k+1} = (3 \cdot 4 + 5 \cdot 10 + 7 \cdot 9) \pmod{16} = 13$ . Відповідно,  $\delta = \bar{b}'_{k+1} - b_{k+1} = 13 - 7 = 6$ .

Таблиця 2 – Значення коефіцієнтів модифікованих кодів СЗК при однакових значеннях контрольних модулів

Перевірочне число, $b_{k+j}$	Коефіцієнти $v_1 - v_{17}$	Модуль $P_i$
$b_{k+1}$	7, 71, 151, 239, 13, 79, 163, 251, 17, 83, 167, 257, 67, 137, 227, 281, 41	256
$b_{k+2}$	11, 73, 157, 89, 241, 19, 173, 263, 41, 109, 197, 277, 103, 163, 47, 127, 79	256
$b_{k+3}$	13, 79, 163, 251, 23, 97, 179, 269, 43, 113, 199, 281, 107, 167, 17, 173, 101	256
$b_{k+4}$	17, 83, 167, 257, 29, 101, 181, 271, 47, 127, 211, 239, 41, 79, 151, 13, 67	256
$b_{k+5}$	19, 89, 103, 173, 263, 37, 7, 71, 151, 239, 17, 79, 157, 239, 43, 181, 59, 113	256
$b_{k+6}$	23, 97, 107, 179, 269, 271, 73, 157, 241, 19, 71, 239, 151, 61, 229, 11, 131	256
$b_{k+7}$	29, 101, 241, 59, 181, 271, 73, 163, 89, 251, 23, 67, 43, 277, 19, 109, 137	256
$b_{k+8}$	31, 277, 103, 113, 191, 257, 29, 101, 41, 193, 241, 97, 239, 19, 263, 13, 139	256

Якщо  $\delta \neq 0$ , то помилка виявлена. Модифікований код СЗК з одним контрольним модулем забезпечує 100 % виявлення помилок в одному блоці даних та 87% в двох блоках даних, при цьому коректуючі можливості залежать також від значення контрольного модуля.

#### Виправлення помилок

Для виправлення помилок використаємо поняття альтернативної множини [10]. Альтернативна множина для модифікованих кодів СЗК це множина блоків даних,

$$\Theta = (b_{\delta}^1, b_{\delta}^2, \dots, b_{\delta}^k)$$

помилка в розрядах кожного з яких може привести до певної величини нев'язки –  $\delta_i$ . Значення нев'язки може дорівнювати  $0 < \delta_i < p_{k+1}$ . Для кожного блоку  $b_i$  можна визначити значення помилки  $x_{a_i}^i$  (таблиця 3).

Значення нев'язки обчислюємо за формулою

$$\delta = \bar{b}'_{k+1} - b_{k+1} = (v_1 \cdot b_1 + v_2 \cdot b_2 + \dots + v_i \cdot b'_i + \dots + v_k \cdot b_k) \pmod{p_{k+1}} - (v_1 \cdot b_1 + v_2 \cdot b_2 + \dots + v_i \cdot b_i + \dots + v_k \cdot b_k) \pmod{p_{k+1}} \quad (2)$$

При виникненні помилки в блоці даних значення  $b_i$  дорівнює  $b'_i = b_i + x$ , де  $x$  – значення помилки,  $1 \leq x \leq 2^m - 1$ .

При помилці в блоці даних  $b_i$  за формулою (2) знаходимо нев'язку

$$\delta_i = v_i \cdot x \pmod{p_{k+1}}.$$

Для виправлення однократної помилки (помилки в одному блоці даних) необхідно, щоб для кожного значення нев’язки альтернативна множина  $\Theta$  складалася із одного блоку даних. Значення контрольного модулю вибираємо із умови [10]:

$$p_k \geq \sum_1^m p_i - m + 1, \tag{3}$$

де  $m$  – кількість блоків даних.

Таблиця 3 – Значення помилки для кожного блоку даних

Значення нев’язки: $\delta$	Блок даних: $b_i$					
	$b_1$	$b_2$	...	$b_i$	...	$b_k$
1	$x_{b_1}^1$	$x_{b_2}^1$	...	$x_{b_i}^1$	...	$x_{b_n}^1$
2	$x_{b_1}^2$	$x_{b_2}^2$	...	$x_{b_i}^2$	...	$x_{b_n}^2$
...	...	...	...	...	...	...
$p_k - 1$	$x_{b_1}^{p_k-1}$	$x_{b_2}^{p_k-1}$	...	$x_{b_i}^{p_k-1}$	...	$x_{b_n}^{p_k-1}$

Розглянемо на прикладі використання альтернативної множини для локалізації помилок. Нехай дані складаються з трьох блоків розрядністю три біти кожний, тобто  $m = 3$ , так як дані трьох розрядні, то модуль вибираємо  $p_i = 8$ . Коефіцієнти лінійної форми вибираємо:  $v_1 = 3, v_2 = 5, v_3 = 7$ . Значення контрольного модуля розрахуємо згідно умови (3)  $p_{k+1} \geq (8 + 8 + 8 - 3 + 1) = 22$  і вибираємо найближче просте число  $p_{k+1} = 23$ .

Нев’язку обчислюємо за формулою (2):

$$\delta_i = \bar{b}'_{k+1} - \bar{b}_{k+1} = (3 \cdot b'_1 + 5 \cdot b_2 + 7 \cdot b_3) \pmod{23} - (3 \cdot b_1 + 5 \cdot b_2 + 7 \cdot b_3) \pmod{23},$$

відповідно, нев’язки для кожного блоку даних дорівнюють:

$$\delta_{1i} = 3 \cdot x_{b_i} \pmod{23};$$

$$\delta_{2i} = 5 \cdot x_{b_i} \pmod{23};$$

$$\delta_{3i} = 7 \cdot x_{b_i} \pmod{23}.$$

Альтернативні множини для кожної нев’язки приведені в таблиці 4.

Як видно із таблиці 4, для восьми значень нев’язки (2, 6, 9, 10, 14, 18, 19, 20) альтернативна множина складається із одного блоку даних, що дозволяє відразу виправити помилку. Для п’яти значень нев’язки (3, 5, 7, 15, 21) альтернативна множина складається із двох блоків даних, і для одного значення нев’язки (12) альтернативна множина складається із трьох блоків даних, тобто помилки в одному з трьох блоків даних приводять до одного і того самого значення нев’язки. Отже, якщо альтернативна множина складається з двох і більше блоків даних, то для локалізації помилки необхідно проводити додатковий аналіз контрольних чисел, або збільшувати кількість контрольних модулів.

Модифікований код СЗК планується використовувати для підвищення надійності передавання даних в безпроводних сенсорних мережах систем промислової автоматизації.

Таблиця 4 – Альтернативні множини для кожної нев'язки

Значення нев'язки: $\delta_i$	Блоки даних		
	$b_1$	$b_2$	$b_3$
1	–	–	–
2	–	5	–
3	1	–	7
4	–	–	–
5	–	1	4
6	2	–	–
7	–	6	1
8	–	–	–
9	3	–	–
10	–	2	–
11	–	–	–
12	4	7	5
13	–	–	–
14	–	–	2
15	5	3	–
16	–	–	–
17	–	–	–
18	6	–	–
19	–	–	6
20	–	4	–
21	7	–	3
22	–	–	–

#### Використання та експериментальні дослідження модифікованого коректуючого коду СЗК

В [2] обґрунтовано, що доцільніше перевірочні символи всіх блоків зберігати в кінці пакету. Таке розміщення перевірочних символів дозволить приймати пакети даних безпроводним сенсорам, які не використовують додаткове кодування в СЗК.

Для використання коректуючого коду СЗК на MAC рівні протоколу стандарту IEEE 802.15.4 розділимо дані (поля MHR і MAC payload) на п'ять блоків (D1 –D5) (рис.2). Довжина інформаційного блоку  $k = 17$  байт. Перевірочні блоки R1 – R5 формуються по відповідному блоці даних і зберігаються після останнього блоку даних.

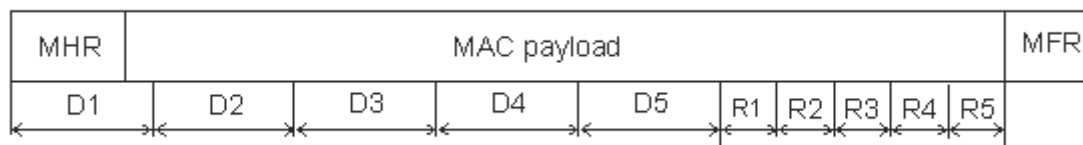


Рисунок 2 – Структура фрейму даних після кодування

При отриманні пакету даних здійснюється перевірка цілісності пакету з використанням CRC кодів. Якщо помилки в пакеті не виявлено, додаткова перевірка з використанням кодів СЗК не здійснюється. При виявленні в пакеті помилок за допомогою CRC кодів здійснюється їх виправлення з використанням запропонованого модифікованого коректуючого коду СЗК.

Експериментальні дослідження часу кодування проводилися в середовищі Matlab для кодів: R – кодів СЗК, M - кодів СЗК та кодів Ріда-Соломона RS (127, 87) з параметрами: загальна довжина коду  $n = 25$  байт; кількість інформаційних символів  $k = 17$  байт; кількість перевірочних символів  $r = 8$ ; кількість помилок  $t = 4$ . Результати дослідження часу кодування приведені в таблиці 5.

Таблиця 5 – Параметри кодів

Код	Час кодування, (мс)	Швидкість коду, $R = \frac{k}{n}$
R – код СЗК	117,5	0,64
RS (127, 87)	109,7	0,685
M – код СЗК	22,5	0,68

Як видно з таблиці 5, коректуючий M – код СЗК дозволяє приблизно в 5 разів підвищити швидкодію кодування порівняно з R – кодом СЗК та кодом Ріда-Соломона RS (127, 87).

#### Висновки

1. Розроблений модифікований коректуючий код СЗК характеризується спрощеною процедурою формування перевірочних символів, що забезпечує підвищення швидкодії кодування приблизно в 5 разів порівняно з іншими коректуючими кодами.

2. Використання модифікованих коректуючих кодів СЗК в безпроводних сенсорних мережах дозволить підвищити надійність та загальну пропускну здатність мережі за рахунок зменшення кількості повторних передач.

3. В наступних роботах планується реалізувати алгоритми завадостійкового кодування/декодування даних в безпроводних сенсорних мережах на основі безпроводних мікроконтролерів JN5148 фірми Jennic та дослідити їх програмну складність.

#### Список літератури

1. Akyildiz I.F., Su W., Sapnkarasubramaniam Y., Cayirci E. Wireless sensor networks: a survey. *Comput. Netw.* 2002, 38. – P.393 – 422.
  2. Kan Yu, Mikael Gidlund, Johan Åkerberg, Mats Bjorkman. Reliable and Low Latency Transmission in Industrial Wireless Sensor Networks. *Procedia Computer Science* 5 (2011). – P. 866–873.
  3. Sikora, V. Groza. Coexistence of ieee802.15.4 with other systems in the 2.4 ghz-ism-band, *Instrumentation and Measurement Technology Conference, IMTC – 2005. Proceedings of the IEEE* 3, 2005. – P. 1786 –1791.
  4. IEEE Standard for Part 15.4: Wireless Medium Access Control Layer(MAC) and Physical Layer (PHY) specifications for Low Rate Wireless Personal Area Networks (LR-WPANs), IEEE Std 802.15.4™-2006.
  5. Vuran M., Akyildiz I. Cross-layer analysis of error control in wireless sensor networks, *Sensor and Ad Hoc Communications and Networks, 2006. SECON '06. 2006 3rd Annual IEEE Communications Society on 2, 2006*, P.585 –594.
  6. Варгаузин В. Помехоустойчивое кодирование в пакетных сетях // *ТелеМультиМедиа*. – 2005. – №9. – С.10-16.
  7. Акушский И. Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. – М.: Сов. радио. – 1968. – 460 с.
  8. Червяков Н. И., Сахнюк П. А., Шапошников А. В., Ряднов С. А. Модулярные параллельные вычислительные структуры нейро- процессорных систем / Под. ред. Н.И. Червякова. – М.: ФИЗМАТЛИТ, 2003 – 288 с.
  9. Яцків В.В. Метод та пристрій кодування мультимедійних даних на основі системи залишкових класів/ В.В. Яцків // *Праці Одеського політехнічного університету. Науковий та науково-виробничий збірник* – 2013. – №1 (40). – С.61 - 66.
  10. Акушский И.Я., Пак И.Т. Вопросы помехоустойчивого кодирования в непозиционном коде // *Вопросы кибернетики*. 1977, Т.28. – С.36-56.
- Стаття надійшла: 28.05.2013.

#### Відомості про автора

**Яцків Василь Васильович**, к.т.н., доцент, доцент кафедри Спеціалізованих комп’ютерних систем Тернопільського національного економічного університету.