УДК 004.056.2

# ВИБІР ПАРАМЕТРІВ КОДУ УМОВНИХ ЛИШКІВ В ЗАДАЧАХ КОНТРОЛЮ ТА ПОНОВЛЕННЯ ЦІЛІСНОСТІ ІНФОРМАЦІЙНИХ ОБ’ЄКТІВ

***Вячеслав Василенко***
*Національний авіаційний університет*

*Анотація:* **Розглянуто вимоги щодо параметрів коду умовних лишків, зокрема щодо величини контрольної основи в задачах захисту цілісності інформаційних об’єктів телекомунікаційних мереж.**
*Summary:* **It is considered requirement in relation to the parameters of koda of conditional tailings, in particular in relation to the size of control basis in the tasks of defence of integrity of information holding objects of telecommunication networks.**
*Ключові слова:* **Завадостійке кодування, лишкові класи, параметри коду, узагальнений код, умовні лишки, цілісність.**

## I Вступ

При використанні в задачах контролю та поновлення цілісності інформаційних об’єктів будь-яких завадостійких кодів постає традиційна для задач цього класу проблема – вибору коду та таких його параметрів, які б забезпечили розрізнення не викривлених (правильних) кодових комбінацій (чисел, базових кодових слів) від викривлених (неправильних) при мінімумі надлишковості. Зрозуміло, що значною мірою цей вибір визначається характеристиками можливих завад в каналах передачі даних та викликаних цими завадами викривлень інформаційних об’єктів. При цьому слід враховувати принаймні дві обставини, які сприяють виникненню, так званих, “пакетів” чи “спалахів” викривлень. Перша з них пов’язана зі здатністю сучасних природних та індустріальних завад мати значну часову тривалість і групуватися в згадані пакети. Друга обставина викликана застосуванням певних заходів підвищення пропускної здатності каналів, в першу чергу таких, як багаторівневі амплітудна, фазова, квадратурно – амплітудна модуляції та інші. Наслідком цього є те, що передача і, відповідно, викривлення одного символу є еквівалентними передачі і, зрозуміло, викривленню одночасно певної кількості інформаційних біт.

З урахуванням уже згаданої можливості мати пакети викривлених символів в подальшому правомочно наголошувати на необхідності застосування методів виявлення (та, можливо, виправлення) спалахів викривлень значної довжини. Такими методами є, насамперед, застосування перемежування (декореляції групових викривлень) та завадостійких кодів, спрямованих на виявлення та виправлення пакетних викривлень. Серед таких завадостійких кодів найбільш відомими є коди Ріда – Соломона, Файра та с контрольним підсумовуванням. Такі коди будемо відносити до узагальнених, оскільки вони застосовуються для виявлення та виправлення викривлень в так званих узагальнених символах.

Метою досліджень, наведених в цій роботі, є розгляд умов та можливостей застосування ще одного із таких кодів – коду умовних лишків [1].

## II Код умовних лишків. Постановка задачі

Нагадаємо, що під узагальненими розумітимемо коди [1, 2], призначені для виявлення (чи виявлення і виправлення) пакетних викривлень, в яких використовуються алгоритми кодування і декодування відносно $b$ – розрядних, узагальнених символів (УС) (інколи аналогічні відповідним алгоритмам двійкових кодів).

В таких кодах початкова двійкова кодова послідовність − базове кодове слово $I_1\ I_2\ \dots\ I_M$ – складається з $m = M/b$ узагальнених $b$ − розрядних символів – груп двійкових розрядів з розрядністю $b$, в яких передбачається виявлення та виправлення викривлень:

$$\underbrace{I_1\dots\dots\dots I_b}_{1\text{ – й УС}},\ \underbrace{I_{b+1}\dots\dots\dots I_{2b}}_{2\text{ – й УС}},\ \dots\dots\dots,\ \underbrace{I_{m-b+1}\dots\dots I_M}_{n\text{ – й УС}}.$$

Двійкові символи, що входять в одну $b$ − розрядну групу, доцільно розглядати як $b$ − значний УС, який може приймати будь-яке із s значень від 0 до s – 1, де

$$s = 2^b.$$

Одним із кодів, здатних виявляти, а при певних умовах, і виправляти викривлення в узагальнених символах є код умовних лишків (лишків умовних код, ЛУ – код) [1]. Для застосування такого коду кожний із таких УС можна розглядати як певний лишок в системі лишкових класів (СЛК). Тобто теоретичною основою ЛУ – коду є теорія лишкових класів. З теорії лишкових класів [3] відомо, що будь-яке число можна представити у вигляді набору лишків від розподілу цього числа на набір взаємно простих чисел, які мають назву основ системи числення, – $p_i$, де $i$ = 1, 2, …, $m$, $m$ – кількість таких основ. Вибір величини $m$ здійснюється згідно з умовою, викладеною нижче. Тоді в коді умовних лишків (ЛУ – коді) кодова комбінація (базове кодове слово) розглядається як деяке (реальне в СЛК чи умовне в ЛУ – коді) число у вигляді сукупності лишків:

$$A = \alpha_1, \alpha_2, \ldots, \alpha_m, \qquad (1)$$

де $\alpha_i = A - [A/p_i]\cdot p_i$ – лишок по $i$ – тій основі, а позначка $[A/p_i]$ означає операцію розрахунку цілої частини від дробового числа $A/p_i$. При цьому між числом А і його уявленням (1) існує взаємна однозначна відповідність, якщо

$$A \le P = \prod_{i=1}^{m} p_i \,.$$

У цьому виразі величина $P$ – діапазон представлення або робочий діапазон чисел, а основи $p_i$ (i =1, 2, …, $m$) – мають назву робочих. Звернемо увагу на те, що величина $\alpha_i$ представляє собою групу двійкових розрядів, кількість яких не перевищує розрядності відповідної основи $p_i$.

Чудовою властивістю системи лишкових класів (СЛК) є те, що в неї легко вводяться властивості виявлення і виправлення викривлень. Відомо, що якщо ввести ще одну, контрольну, основу $p_к$, то уявлення $A$ в розширеному діапазоні $R = P\cdot p_к$, у вигляді

$$A_{СЛК} = \alpha_1, \alpha_2, \ldots, \alpha_m, \alpha_k, \qquad (2)$$

де $\alpha_k$ – лишок по основі $p_k$, є корегуючим кодом, властивості якого залежать від його параметрів. Це означає, що при представленні чисел у вигляді (2) створюється завадостійкий код з можливостями або виявлення викривлень, або і їх корекції.

Код, який задається в СЛК у вигляді (2) має принаймні 2 недоліки. Перший з них пов'язаний з необхідністю роботи з числами в системі числення в залишкових класах, а другий – з тим, що можливі викривлення знаходяться і виправляються (викривлений символ поновлюється) тільки в тому випадку, якщо викривлений лише один з символів $\alpha_i$, тобто викривлення повинні бути фіксованими в межах однієї з груп розрядів. Цей недолік достатньо просто усувається в коді умовних лишків, який вводиться таким чином.

Хай є код деякого числа А, представленого в будь-якій системі числення, зокрема, позиційній, наприклад двійковій. Для визначеності, хай це число А представлено послідовністю з нулів і одиниць. Розіб'ємо цю послідовності певним (у загальному випадку довільним) чином на $m$ груп, як і для решти узагальнених кодів.

Як показано вище, код кожного $i$ – го УС слід розглядати як s – значний УС $\alpha_i$, який може приймати будь-яке з s значень від 0 до s – 1, де $s = 2^b$. Будемо умовно вважати цей код лишком деякого умовного числа А по основі $p_i$. Оскільки величина $\alpha_i$, як елемент початкового числа

$$0 \le \alpha_i \le s - 1,$$

а як лишок від ділення А на $p_i$

$$0 \le \alpha_i \le p_i,$$

то для представлення коду будь-якої групи у вигляді лишку по основі $p_i$ необхідно, щоб виконувалася умова

$$p_i > s - 1 = 2^b - 1, \qquad (3)$$

інакше в групу із $b$ розрядів може бути записаним код $\alpha_i \ge p_i$, що в лишкових класах не допустимо.

При такому підході будь-які комбінації початкового коду числа А "вписуються" в систему числення з основами $p_i$ ($i$ = 1, 2,..., $m$). Якщо розширити систему основ на контрольну $q$ і для одержаного набору умовних лишків $\alpha_i$ ($i$ = 1, 2,...) розрахувати умовний лишок $\alpha_k$, то на одержане умовне число

$$A = \alpha_1, \alpha_2, \ldots, \alpha_m, \alpha_к \qquad (4)$$

розповсюджуються усі можливості СЛК по виявленню і виправленню викривлень.

Тобто, код у вигляді (4) має всі властивості коду (2), але відносно будь-якої двійкової послідовності, а не тільки відносно чисел в лишкових класах. Водночас відзначимо, що таким чином усунений перший недолік коду (2).

Оскільки для отримання контрольної ознаки, тобто для кодування будь-якої послідовності двійкових цифр завадостійким кодом, умовно, не реально, не фізично групи розрядів початкового числа розглядаються як деякі лишки, то такий *код одержав найменування коду умовних лишків*.

Слід звернути увагу на те, що при кодуванні ЛУ-кодом початкова послідовність не змінюється, до неї тільки приформовуються додаткові, обчислені за окремими правилами, контрольні символи.

*Головною задачею для застосування такого коду* при виявленні та (можливо) виправленні викривлень в узагальнених символах, як і в інших завадостійких кодах, є задача узгодження його параметрів із характеристиками можливих викривлень. Отже надалі слід розглянути порядок, вимоги та умови щодо вибору параметрів ЛУ-коду.

## III Вибір параметрів ЛУ – коду

Привабливою властивістю коду (4) є те, що такий код, як узагальнений, дозволяє знаходити і виправляти $b$ – розрядні пакети викривлень, згруповані в межах будь-якого з $n$ УС.

Можливості ЛУ-коду, як і будь-якого іншого, визначаються його параметрами. Задача вибору параметрів коду умовних лишків полягає у визначенні кількості $n$ та величин сукупності із $m$ робочих та $k$ контрольних основ цієї системи, які б забезпечили просте і надійне виявлення факту викривлення, а в корегуючих кодах також – як місця, так і величин можливих викривлень в базових кодових словах.

Що стосується вибору основ, які утворюють робочий діапазон, то вимог до них може бути сформульовано декілька.

*Перша з них* випливає з відомої вимоги до основ в системі лишкових класів – *ці основи повинні бути взаємно простими числами*.

*Друга вимога* визначається потрібною розрядністю викривлень, які є можливими в умовах застосування цього коду і які повинні мати виявленими чи виявленими та викривленими цим кодом. Будемо вважати, що ЛУ – код застосовується в умовах передачі інформаційних об’єктів по каналу із завадами, причому наслідком впливу завад є викривлення певної кількості символів інформаційних об’єктів із імовірністю $P_{викр}$. Нехай інформаційний об’єкт, що підлягає передачі в згаданому каналі, має загальну довжину, що включає як інформаційні, так і надлишкові символи, таку, що дорівнює $N$ . Тоді загальна кількість викривлень може досягнути:

$$N_{\text{викр}} = [N \cdot P_{викр}] + 1$$

символів, де позначка $[x]$ означає обчислення цілої частини від $x$.

Будемо вважати, що ці символи є узагальненими, тобто утворені $b$ − розрядними групами, а за рахунок перемежування із глибиною $\lambda = N_{\text{викр}}$ узагальнений код має забезпечувати виявлення (чи і виправлення) викривлень в межах одного базового кодового слова (БКС) в одній із $b$ − розрядних груп. Тоді загальна кількість узагальнених символів в БКС буде дорівнювати:

$$n = N / \lambda = N / N_{викр}\,.$$

Оскільки, кількість узагальнених символів в БКС $n$ повинна дорівнювати сумарній кількості робочих та контрольних основ ЛУ – коду, то основні параметри цього коду можна вважати визначеними, і саме: загальна кількість узагальнених символів дорівнює $n$, їх розрядність дорівнює $b$. Зрозуміло, що кількість суто інформаційних символів $m$ в межах БКС неважко визначити, якщо відомою є кількість надлишкових узагальнених символів $k$, тоді $m = n – k$.

Однак кількість надлишкових узагальнених символів $k$ якраз і є не відомою, оскільки визначається ще невизначеною величиною контрольної основи $p_k$ (чи $q$). Зрозуміло, що потрібна надлишковість, тобто величина контрольної основи $q$ залежить від задач, які вирішуються із застосуванням ЛУ – коду. Визначимо вимоги щодо цієї надлишковості в задачі контролю цілісності та в задачі контролю та поновлення цілісності.

## IV Визначення величини контрольної основи в задачах контролю цілісності

Відомо [1 – 3], що при застосуванні ЛУ – коду не викривленими вважаються такі числа, величина яких не перевищує визначеного наперед діапазону представлення не викривлених чисел (робочого діапазону) $P = \prod_{i=1}^{m} p_i$ , де $p_i$ ($i$ = 1, 2, …, $m$) – основи системи числення, обрані для даної системи представлення. В цих кодах для завадостійкого кодування, як і в інших кодах, вводиться надлишковість у вигляді реального чи умовного лишку від розподілу вихідного числа А на контрольну основу $p_k$ (чи $q$). Її введення призводить до розширення діапазону представлення до величини $R = P \cdot p_k = P \cdot q$ . При цьому природно вважається, що викривлені (неправильні) числа $\widetilde{A}$ , на відміну від не викривлених, зосереджені за межами робочого діапазону, тобто $\widetilde{A} > P$.

Оскільки, за визначенням, викривлені числа задовольняють умові $\widetilde{A} > P$, то звідси неважко для задач контролю наявності викривлень визначити вимогу до величини контрольної основи цієї системи, а отже, здійснити в подальшому її вибір. Тобто, для виявлення наявності викривлень досить визначити, в якому із діапазонів (робочому чи контрольному) знаходиться число, правильність якого перевіряється. Для цього слід вимагати, щоби викривлення лишку (символу початкового числа А) по будь-якій основі, наприклад, по основі $p_i$ збільшувало б початкове не викривлене число А < Р

$$A = \alpha_1, \alpha_2, \alpha_3, ..., \alpha_i, ..., \alpha_m, \alpha_k$$

на величину, яка забезпечує вихід викривленого числа в контрольний діапазон, тобто на величину

$$\Delta A = l_i \cdot R_i = 0,0,0,...,\Delta\alpha_i,...,0,0 > P\,.$$

В останніх виразах: $\Delta A$ – величина викривлення; $\alpha_i$ – значення не викривленого символу (лишку) по основі з номером $i$; $l_i$ – номер інтервалу, в який потрапляє число, викривлене по основі з номером $i$; $R_i = P \cdot q / p_i$ – величина даного інтервалу.

Тоді, за рахунок цього, викривлене число

$$\widetilde{A} = A^{/} = A + l_i \cdot R_i = \alpha_1, \alpha_2, \alpha_3, ..., \widetilde{\alpha}_i, ..., \alpha_m, \alpha_k\,,$$

перейде із початкового діапазона [0, $P$) в контрольний діапазон (див. рис. 1), наприклад, в діапазон $[\,l_i \cdot R_i,\ (l_i + 1) \cdot R_i)$ величиною $R_i = P \cdot q / p_i$. Таким чином буде забезпечена умова:

$$l_i \cdot R_i = l_i \cdot P \cdot q / p_i > P = P \cdot q / q\,,$$

де $\widetilde{\alpha}_i = (\alpha_i + \Delta\alpha_i) \bmod p_i$ – значення викривленого символу, $\Delta\alpha_i$ – величина викривлення $i$ – го символу.

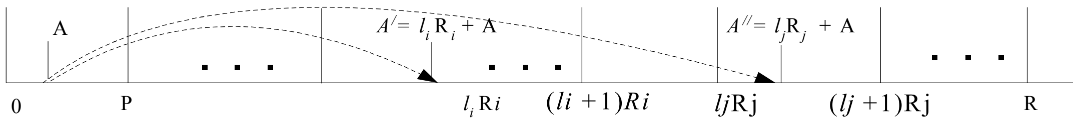


**Рисунок – До виходу викривленого числа за межі робочого діапазону**

Звідси випливає:

$$l_i / p_i > 1 / q\,,$$

а отже, при найменшому значенні $l_i = 1$,

$$q > p_i\,,$$

тобто умовою однозначного визначення наявності викривлень є перевищення величиною контрольної основи величини будь-якої із інших основ, а в загальному випадку

$$q > p_m\,, \qquad (5)$$

де $p_m$ – найбільша із робочих основ.

Із виразу (3) слідує, що до найбільшої із робочих основ $p_m$ загальні вимоги щодо її величини висуваються у вигляді:

$$p_m > \mathrm{s} - 1 = 2^b - 1,$$

тому контрольна основа тим більше повинна перевищувати значення s – 1. За умови, що контрольна основа для свого розміщення потребує цілої кількості символів, надлишковість складе два узагальнених символи.

***Отже*** усі параметри ЛУ – коду в задачах контролю цілісності інформаційних об’єктів є визначеними і загальна кількість символів в БКС складе $m$ інформаційних основ ($b$ – розрядних символів) та $k$ = 2 контрольних (також $b$ – розрядних) символи:

$$n = m + k = m + 2.$$

## V Вибір величин контрольної основи в задачах контролю та поновлення цілісності

В задачах контролю та поновлення цілісності недостатньо лише встановити факт наявності порушення цілісності інформаційного об'єкту, а потрібно визначити місце викривлення та його величину. Зрозуміло, що для вирішення задач виявлення місця та, особливо, величин викривлень, необхідно забезпечити ідентифікацію викривленого числа (чи величини викривлення) із номером основи (для нашого прикладу – *i* чи *j*), по якій таке викривлення має місце, та визначення (в подальшому) величини цього викривлення (відповідно $\Delta\alpha_i$ чи $\Delta\alpha_j$). Для цього можна використати той факт, що аналогічне викривлення по основі $p_j$ переводить викривлене число (див. рис. 1) в діапазон $[l_j \cdot R_j,\ (l_j+1)\cdot R_j)$ величиною $R_j$.

$$\widetilde{A} = A^{//} = A + l_j \cdot R_j = \alpha_1, \alpha_2, \alpha_3, ..., \widetilde{\alpha}_j, ..., \alpha_m, \alpha_k,$$

Із наведеного слідує, що механізми визначення наявності, місця виникнення та величини викривлення мають ґрунтуватися на виявленні тим чи іншим шляхом хоча б однієї з таких взаємно пов'язаних величин як *i*, $p_i$, та, відповідно, $\Delta\alpha_i$, $l_i$, $R_i$, $\Delta A$. Із наведеного випливає також, що для ідентифікації викривленого числа (чи величини викривлення) із номером основи *i* слід забезпечити попадання викривлених по різним основам чисел в різні діапазони, що, в свою чергу, є можливим за умови, що відстань між двома довільними діапазонами, в які можуть потрапити викривлені числа, перевищувала б максимальне значення не викривленого числа *P*.

. Наприклад, при $l_i \cdot R_i > l_j \cdot R_j$ (при зворотному співвідношенні результат не зміниться):

$$l_i \cdot R_i > l_j \cdot R_j + P, \text{ чи } l_i \cdot R_i - l_j \cdot R_j > P.$$

В загальному випадку цей вираз із урахуванням того, що в СЛК операції в діапазоні [0, *R*) здійснюються за модулем *R*, набуде вигляду:

$$(l_i \cdot R_i - l_j \cdot R_j) \bmod R > P.$$

Звідси неважко перейти до визначення загальних вимог щодо величини контрольної основи $q$:

$$l_i \cdot P \cdot q / p_i - l_j \cdot P \cdot q / p_j > P, \tag{6}$$

за умови $l_i \cdot P \cdot q / p_i > l_j \cdot P \cdot q / p_j$,

$$R + l_i \cdot P \cdot q / p_i - l_j \cdot P \cdot q / p_j - [(R + l_i \cdot P \cdot q / p_i - l_j \cdot P \cdot q / p_j)/R] \cdot R > P, \tag{7}$$

чи за умови $l_i \cdot P \cdot q / p_i < l_j \cdot P \cdot q / p_j$. В останньому виразі квадратні дужки означають обчислення цілої частини від відповідного дробового числа.

При визначенні вимог щодо величини контрольної основи $q$, на основі виразу (6), та умови після (6) після скорочення на *P*, одержимо:

$$l_i \cdot q / p_i - l_j \cdot q / p_j > 1,$$

$$q(l_i / p_i - l_j / p_j) > 1,$$

а, отже, в результаті вимога до контрольної основи приймає вигляд нерівності:

$$q > 1/(l_i / p_i - l_j / p_j) = p_i \cdot p_j / (l_i \cdot p_j - l_j \cdot p_i). \tag{8}$$

Звернемо увагу на те, що права частина нерівності (8) в загальному випадку може бути дробовим, а не цілим числом, яким має бути контрольна основа. До того ж, шукане значення контрольної основи має бути цілим. Для розв'язання цієї нерівності із зазначеними обмеженнями спочатку слід визначити максимальне значення чисельника та мінімальне значення знаменника. Зрозуміло, що максимальне значення чисельника в цьому виразі дорівнює добутку двох найбільших із основ системи числення $p_m \cdot p_{m-1}$, а мінімальне значення знаменника (це цілочисленна величина!):

$$l_i \cdot p_j - l_j \cdot p_i = 1,$$

оскільки дорівнювати нулю знаменник може лише тоді, коли

$$l_i \cdot p_j = l_j \cdot p_i.$$

Останнє, в свою чергу, є досяжним лише при $l_i = p_i$, а $l_j = p_j$ , що є неможливим (нагадаємо, що основи системи числення, (це величини $p_i$ та $p_j$), є взаємно простими числами).

Оскільки мінімальне значення знаменника дорівнює одиниці, то граничне значення виразу (8) є цілою величиною. Причому, в разі визначення як величини, так і місця викривлення по факту попадання викривленого числа до інтервалу $l_i$ чи $l_j$, вимога до величини контрольної основи може бути записаною у вигляді:

$$q > p_m \cdot p_{m-1}. \tag{9}$$

При визначенні вимог щодо величини контрольної основи $q$, на основі виразу (6) і (7), після скорочень на $P$ та $q$ одержимо:

$$q + l_i \cdot q / p_i - l_j \cdot q / p_j - [1 + l_i / p_i - l_j / p_j] \cdot q > 1,$$

$$q \cdot (1 + l_i / p_i - l_j / p_j - [1 + l_i / p_i - l_j / p_j]) > 1,$$

а, отже, в результаті вимога до контрольної основи приймає вигляд нерівності:

$$q > 1/(1 + l_i / p_i - l_j / p_j - [1 + l_i / p_i - l_j / p_j]). \tag{10}$$

Звернемо увагу на те, що вираз у знаменнику є дробовим числом, звідси величина контрольної основи є більшою за чисельник, отже більшою за одиницю. Для уточнення цієї величини приведемо вирази у знаменнику до спільного знаменника, яким є величина $p_i \cdot p_j$, та перенесемо останню у чисельник. Тоді нерівність (10) перетвориться на вимогу:

$$q > p_i \cdot p_j /(p_i \cdot p_j + l_i \cdot p_j - l_j \cdot p_i - p_i \cdot p_j \cdot [(p_i \cdot p_j + l_i \cdot p_j - l_j \cdot p_i)/(p_i \cdot p_j)]).$$

Оскільки максимальне значення чисельника дорівнює величині $p_m \cdot p_{m-1}$, знаменник, як і у виразі (10), є меншим одиниці, а величина контрольної основи $q$ має бути цілим, взаємно простим числом із усіма іншими основами з усієї їх множини, то слід зробити висновок, що вимога щодо величини $q$ перетворюються на вимогу виду:

$$q > c \cdot p_m \cdot p_{m-1}, \tag{11}$$

де величина $c$ із урахуванням уже визначеної вимоги (9) може прийняти таке значення $c > 1$, яке є цілим та взаємно простим числом із усіма основами використовуваної системи числення. З іншого боку, слід враховувати, що від величини $q$ залежить можлива надлишковість коду, яку бажано мати найменшою. Виходячи з цього, слід зробити висновок, що сформульованим обмеженням задовольняє вимога, яку із врахуванням викладеного вище можна розглядати як єдину можливу:

$$q > 2 \cdot p_m \cdot p_{m-1}. \tag{12}$$

За умови, що контрольна основа для свого розміщення потребує цілої кількості символів, надлишковість складе, як мінімум, три узагальнених символи.

***Отже*** усі параметри ЛУ – коду і в задачах контролю та поновлення цілісності інформаційних об'єктів є визначеними і загальна кількість символів в БКС складе $m$ інформаційних основ ($b$ – розрядних символів) та $k = 3$ контрольних (також $b$ – розрядних) символи:

$$n = m + k = m + 3.$$

***Таким чином***, при дотриманні умови (5) можливо забезпечити однозначний результат виявлення всіх можливих викривлень в одному із узагальнених символів, а при дотриманні умови (12) – однозначний результат виявлення та виправлення усіх можливих викривлень представлення інформаційних об'єктів при їх циркуляції в сучасних телекомунікаційних мережах. Можливості щодо такого застосування коду умовних лишків уже розглянуті в роботах [1 – 3].

*Література: **1.** Василенко В. С. Использование ВУ - кодов для повышения верности информации в радіоканалах. // Матеріали 28 НТС Асоціації зв'язку України. – К.: КВІРТУ ППО. – 1991. – С. 23 **2.** Василенко В. С., Матов О. Я. Узагальнені завадостійкі коди в задачах забезпечення цілісності інформаційних об'єктів. Код умовних лишків.// К.: Реєстрація, зберігання і обробка даних. - 2006. - том 6, № 4. с. 82 – 93. **3.** Акушский И. Я., Юдицкий Д. И. Машинная арифметика в остаточных классах. // М.: Сов. радио, 1966. – 421 с*

.