УДК 004.056.2

О. Я. Матов[1], В. С. Василенко[2]
[1]Інститут проблем реєстрації інформації НАН України
вул. М. Шпака, 2, 03113 Київ, Україна
[2]Національний авіаційний університет
пр. Космонавта Комарова, 1, 03058 Київ, Україна

Узагальнені завадостійкі коди в задачах забезпечення цілісності інформаційних об'єктів в умовах природних впливів

Для використання в задачах забезпечення цілісності інформаційних об'єктів в умовах природних впливів запропоновано узагальнені завадостійкі коді.

Ключові слова: *виявлення викривлень, виправлення викривлень, контроль цілісності, завадостійкі корегувальні коди.*

Вступ

Для забезпечення контролю та поновлення цілісності інформаційних об'єктів в умовах тих чи інших руйнуючих впливів до складу інформації, яка захищається, включають надмірну інформацію — ознаку цілісності або контрольну ознаку (залежно від прийнятої в задачах контролю цілісності або завадостійкого кодування термінології) — своєрідний образ, відображення цієї інформації, процедура формування якого відома, і який із дуже високою вірогідністю відповідає інформації, що захищається [1].

При цьому між інформацією, що захищається, і ознаками цілісності, або контрольними ознаками встановлюється регулярний (функціональний) односторонній зв'язок (процедури розрахунку контрольної ознаки за початковою інформацією, що захищається, відомі, а процедури розрахунку початкової інформації за контрольними ознаками найчастіше не існує). Контроль цілісності (на відсутність викривлень) зводиться при цьому до тих або інших процедур перевірки наявності вказаного регулярного (функціонального) одностороннього зв'язку між ознаками цілісності та прийнятою з каналу зв'язку (або зчитаною з запам'ятовуючого пристрою (ЗП)) інформацією.

Характерною особливістю випадкових (природних) викривлень є те, що вони, через їхню хаотичність, відсутність навмисності, порушують регулярний (функціональний) односторонній зв'язок між прийнятою (або зчитаною з ЗП) інформацією й ознаками цілісності, сформованими перед передачею (перед записом у ЗП).

Тому при виявленні порушення вказаного зв'язку встановлюється факт наявності таких викривлень, а за певних умов, і їхнього місця та величини (характеру). За відсутності порушення цього зв'язку встановлюється факт відсутності викривлень.

Одним зі способів (механізмів) забезпечення цілісності інформації в умовах природних дій (проблема завадостійкості) для каналів телекомунікаційних мереж (взагалі для мереж передачі даних) є застосування різного роду завадостійких корегувальних кодів (ЗКК), які дозволяють реалізувати програмні, апаратурні або програмно-апаратурні засоби виявлення та усунення викривлень.

Цей спосіб (механізм) забезпечення цілісності інформаційних об'єктів наразі знайшов широке застосування в стандартах радіозв'язку, наприклад, стільникового. Він не потребує зворотного каналу й забезпечує, як правило, прийнятне значення часу затримки передавання інформаційних об'єктів. Тому, чи не єдиною проблемою в цих мережах із використанням радіоканалів є проблема забезпечення цілісності інформаційних об'єктів в умовах впливу навіть природних (не говорячи вже про штучні, навмисні завади) пакетних викривлень як «коротких» (тривалістю 2...10 мс), так і особливо «довгих» (тривалістю 100…200 мс). Це є особливо актуальним для радіоканалів, наприклад, у системах стільникового зв'язку [2]. У цих каналах тривалість пакета викривлень може бути порівняною чи, навіть, значно перевищувати тривалість інформаційного пакета, що може суттєво вплинути на результативність процедур інформаційного обміну.

Як вихід із таких ситуацій може розглядатися можливість [1] збільшення тривалості інформаційних пактів з одночасним застосуванням перемежування потрібної глибини та завадостійких корегувальних кодів, які були б спроможними забезпечити виявлення та виправлення пакетів викривлень значної тривалості. Як такі, у статті пропонуються узагальнені завадостійкі корегувальні коди.

Узагальнені завадостійкі коди. Лишково-Хеммінгові та лишково-матричні коди

Нагадаємо, що під узагальненими [1] розуміються коди, призначені для виявлення (виявлення та виправлення) пакетних викривлень із кратністю b, у яких використовуються алгоритми кодування та декодування по відношенню до узагальнених b-розрядних символів.

У цих кодах початкова двійкова k-бітна кодова послідовність — базове кодове слово (БКС) — $I_1, _2, \ldots, I_k$ розбивається на $n = k/b$ груп двійкових розрядів — узагальнених символів (УС) з розрядністю b, в яких передбачається виявлення та виправлення викривлень:

$$\underbrace{I_1 \ldots\ldots I_b,}_{\text{1-а група}} \quad \underbrace{I_{b+1} \ldots\ldots I_{2b}}_{\text{2-а група}} \quad \underbrace{I_{k-b+1} \ldots\ldots I_k}_{n\text{-а група}}$$

При кодуванні та декодуванні операції над узагальненими символами пропонується виконувати за деяким модулем, тобто розшукувати лишок від розподілу результату операції на деякий модуль. Це дало авторам можливість, у разі засто-

сування алгоритмів, які можуть бути аналогічними відповідним алгоритмам кодування–декодування двійкових кодів, але по відношенню до узагальнених символів, для відмінності відповідних узагальнених кодів від двійкових увести в їхню назву слово «лишок», тобто говорити про лишково-Хеммінгові (ЛХ), лишково-матричні (ЛМ), лишково-згорточні (ЛЗ) чи лишково-ланцюгові (ЛЛ) та інші коди.

Принципи побудови та застосування таких кодів розглянемо на прикладі лише деяких із таких кодів. У разі потреби читач може самостійно застосувати викладені підходи й по відношенню до інших кодів цього класу.

У лишково-Хеммінгових кодах двійкові базові кодові слова, розбиті на b-розрядні УС, записуються у вигляді $\alpha_1, \alpha_2, \ldots, \alpha_n$, де $\alpha_i \le s = 2^b - 1$, а $N = b \cdot n$. Так само, як і у двійковому коді Хеммінга (класична форма запису коду) УС α_i з номерами $i = 2^j$ ($j = 0, 1, \ldots$) є перевірочними, решта символів — інформаційні. Причому для отримання перевірочних символів при кодуванні використовується алгоритм для двійкового коду Хеммінга, але по відношенню до узагальнених символів. При цьому всі необхідні для кодування та декодування операції здійснюються за деяким модулем. Тобто, у ЛХ-коді для отримання першого перевірочного символу необхідно скласти за деяким модулем (одержати лишки від суми) усі УС базового кодового слова, що мають у коді свого номера одиницю в першому (молодшому) розряді; для отримання другого перевірочного символу — скласти за модулем усі символи, що мають у коді свого номера одиницю в другому розряді, й т.д.

Як модуль для отримання контрольних символів досить зручно використовувати величину $s = 2^b$ тобто:

$$\alpha_1 = \{\alpha_3 + \alpha_5 + \alpha_7 + \ldots\ldots\ldots\ldots\ldots\}_s,$$
$$\alpha_2 = \{\alpha_3 + \alpha_5 + \alpha_6 + \alpha_7 + \ldots\ldots\ldots\ldots\}_s,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

При такому значенні модуля потрібна розрядність перевірочних символів не відрізняється від розрядності узагальнених символів b.

При декодуванні зберігається той же алгоритм розрахунку перевірочних α_i символів, що й при кодуванні, але при додаванні за модулем використовуються й контрольні символи. Знов одержані перевірочні символи порівнюються з відповідними перевірочними символами, обчисленими при кодуванні. При їхній відповідності робиться висновок про відсутність викривлення, у решті випадків — про наявність викривлення.

Якщо приписати результатам порівняння значення 0, а результатам непорівняння значення 1, то одержана сукупність нулів і одиниць утворює код, який також, як і у двійковому коді Хеммінга, є номером викривленого символу.

Приклад. Нехай необхідно закодувати ЛХ-кодом восьмирозрядну ($N = 8$) послідовність 10001101. Якщо код орієнтований на виправлення двократних викривлень, то $b = 2$, кількість узагальнених символів $n = N/b = 4$. Як модуль для отримання контрольних символів використаємо величину $s = 4$. Відомо, що в коді Хеммінга при $n = 4$ потрібно три перевірочні символи α_1, α_2, α_4, а інформаційними символами є $\alpha_3 = 10$, $\alpha_5 = 00$, $\alpha_6 = 11$, $\alpha_7 = 01$ Для отримання першого перевірочного символу складемо за модулем чотири α_3, α_5, α_7:

$$\alpha_1 = \{\alpha_3 + \alpha_5 + \alpha_7\}_4 = 11.$$

Аналогічно цьому:

$$\alpha_2 = \{\alpha_3 + \alpha_6 + \alpha_7\}_4 = 10,$$
$$\alpha_4 = \{\alpha_5 + \alpha_6 + \alpha_7\}_4 = 00.$$

Після кодування одержано код

$$11.10.10.00.00.11.01 = \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7,$$

який може бути записаним у запам'ятовуючий пристрій, переданим до каналу зв'язку й т.д.

Нехай зчитаний або прийнятий із каналу зв'язку код має викривлення в п'ятій групі:

$$\alpha_1, \alpha_2, \alpha_3, \alpha_4, \acute{\alpha}_5, \alpha_6, \alpha_7 = 11.10.10.00.01.11.01.$$

Після обчислення нових контрольних символів, одержимо:

$$\alpha_1 = \{\alpha_3 + \acute{\alpha}_5 + \alpha_7\}_4 = 00,$$
$$\alpha_2 = \{\alpha_3 + \alpha_6 + \alpha_7\}_4 = 10,$$
$$\alpha_4 = \{\acute{\alpha}_5 + \alpha_6 + \alpha_7\}_4 = 01.$$

Результати порівняння дадуть код 101, оскільки перший та третій перевірочні символи не співпадають. Це свідчить про виявлення помилки в п'ятому символі, що й було насправді.

Неважко визначити й величину викривлення. Дійсно, будь-який із перевірочних символів, наприклад, α_i, при викривленні деякого інформаційного, наприклад, α_j, що приймає участь у формуванні символу α_i, має величину:

$$\acute{\alpha}_i = \{\alpha_c + \alpha_d + \ldots + \{\alpha_j + \Delta\alpha_j\} + \ldots\}_s = \{\alpha_i + \Delta\alpha_j\}_s, \qquad (1)$$

звідки

$$\Delta\alpha_j = \{\acute{\alpha}_i - \alpha_i\}_s. \qquad (2)$$

Для вищерозглянутого прикладу:

$$\Delta\alpha_5 = \{\acute{\alpha}_1 - \alpha_1\}_4 = \{00 - 11\}_4 = 01,$$

або

$$\Delta\alpha_5 = \{\acute{\alpha}_4 - \alpha_4\}_4 = \{01 - 00\}_4 = 01.$$

Знаючи величину ($\acute{\alpha}_i$) та місце викривлення (i), легко здійснити корекцію, оскільки з (2) витікає:

$$A_i = \{\acute{\alpha}_i - \Delta\alpha_j\}_s.$$

У нашому прикладі

$$\alpha_5 = \{\acute{\alpha}_5 - \Delta\alpha_5\}_4 = \{01 - 01\}_4 = 00,$$

що і є насправді.

Алгоритм декодування ЛХ-коду може бути спрощеним, якщо при кодуванні замість перевірочних символів α_i в записану або передану послідовність записувати величину

$$\Delta\alpha_i = \{s - \Delta\alpha_j\}_s.$$

Тоді для вже розглянутого прикладу (α_1 =11, α_2 =10, α_4 = 00) $\Delta\alpha_1$ = 01, $\Delta\alpha_2$ = = 10, $\Delta\alpha_4$ = 00 записувати (передавати) необхідно код:

$$\Delta\alpha_1, \Delta\alpha_2, \alpha_3, \Delta\alpha_4, \alpha_5, \alpha_6, \alpha_7 = 01.10.10.00.00.11.01.$$

Якщо зчитано або прийнято слово з тим же викривленням, що й раніше, тобто

$$\alpha_1, \alpha_2, \alpha_3, \alpha_4, \acute{\alpha}_5, \alpha_6, \alpha_7, = 01.10.10.00.01.11.01,$$

то після декодування отримаємо:

$$\Delta\alpha_1 = \{\alpha_1 + \alpha_3 + \acute{\alpha}_5 + \alpha_7\}_4 = 01,$$
$$\Delta\alpha_2 = \{\alpha_2 + \alpha_3 + \alpha_6 + \alpha_7\}_4 = 00,$$
$$\Delta\alpha_4 = \{\alpha_4 + \acute{\alpha}_5 + \alpha_6 + \alpha_7\}_4 = 01.$$

При цьому, якщо відмінним від нуля перевірочним символам приписати значення 1, а іншим код 0, то одержимо код i = 101, що визначає місце викривлення, величина якого дорівнює значенню будь-якого ненульового перевірочного символу. Для розглянутого прикладу величина викривлення $\Delta\alpha_i$ = 01, корекція якого нескладна.

<u>У лишково-матричних кодах</u> БКС розбивається на узагальнені символи, які зводяться в прямокутну матрицю розмірності $m \times n$ (m стовпців і n рядків) (рис. 1).

$$\begin{Vmatrix} \alpha_1 & \alpha_2 & . \ . \ . & \alpha_m \\ \alpha_{m+1} & \alpha_{m+2} & . \ . \ . & \alpha_{2m} \\ . & . & . \ . \ . & . \\ \alpha_{m(n-1)+1} & \alpha_{m(n-1)+2} & . \ . \ . & \alpha_{mn} \end{Vmatrix}.$$

Рис. 1. Представлення БКС у вигляді матриці

Ця матриця при кодуванні розширюється на один рядок і один стовпець за рахунок перевірочних символів, кожний з яких є доповненням до *s* суми за модулем *s* елементів відповідного рядка або відповідного стовпця, при цьому одержують нову розширену матрицю (рис. 2), яка записується в ЗП (передається до каналу зв'язку).

$$\left\| \begin{array}{cccc} \alpha_1 & \alpha_2 & \ldots & \alpha_m & s-\sum_{i=1}^{m}\alpha_i (\mathrm{mod} s) \\ \alpha_{m+1} & \alpha_{m+2} & \ldots & \alpha_{2m} & s-\sum_{i=1}^{m}\alpha_{m+i} (\mathrm{mod} s) \\ . & . & \ldots & . & . \\ \alpha_{m(n-1)+1} & \alpha_{m(n-1)+2} & \ldots & \alpha_{nm} & s-\sum_{i=1}^{m}\alpha_{m(n-1)+i} (\mathrm{mod} s) \\ s-\sum_{k=1}^{n}\alpha_{m(k-1)+1} (\mathrm{mod} s) & s-\sum_{k=1}^{n}\alpha_{m(k-1)+2} (\mathrm{mod} s) & \ldots & s-\sum_{k=1}^{n}\alpha_{nm} (\mathrm{mod} s) & \end{array} \right\|$$

Рис. 2. Представлення БКС у вигляді розширеної матриці

При декодуванні викривлених БКС ті перевірочні елементи з додаткових рядка й стовпця, які відповідають рядку або стовпцю, що містить викривлені символи, відрізнятимуться від нуля, що дає можливість визначати місце викривлення. Якщо викривленим є тільки один елемент у рядку й стовпці, то ненульове значення відповідних перевірочних символів визначить величину цієї помилки. У цьому значенні можливості ЛМ-коду по відношенню до узагальнених символів повністю співпадатимуть із можливостями по виявленню й виправленню викривлень двійкового матричного коду по відношенню до двійкових символів.

Приклад. Нехай необхідно закодувати ЛМ-кодом восьмирозрядне БКС 10.00.11.10. Для $b = 2$ і $s = 4$ одержимо матрицю:

$$\left\| \begin{array}{cc} \alpha_1 & \alpha_2 \\ \alpha_3 & \alpha_4 \end{array} \right\| = \left\| \begin{array}{cc} 10 & 00 \\ 11 & 01 \end{array} \right\|.$$

Після кодування розширена матриця матиме вигляд:

$$\left\| \begin{array}{ccc} \alpha_1 & \alpha_2 & s-(\alpha_1+\alpha_2)(\mathrm{mod}\ s) \\ \alpha_3 & \alpha_4 & s-(\alpha_3+\alpha_4)(\mathrm{mod}\ s) \\ s-(\alpha_1+\alpha_3)(\mathrm{mod}\ s) & s-(\alpha_2+\alpha_4)(\mathrm{mod}\ s) & \end{array} \right\| = \left\| \begin{array}{ccc} 10 & 00 & 10 \\ 11 & 01 & 00 \\ 11 & 11 & \end{array} \right\|.$$

Нехай зчитана (прийнята з каналу зв'язку) послідовність, що відповідає наступній матриці (викривлений елемент першого рядка другого стовпчика):

$$\begin{Vmatrix} 10 & 01 & 10 \\ 11 & 01 & 00 \\ 11 & 11 & \end{Vmatrix}.$$

У результаті декодування шляхом додавання за модулем s усіх елементів (включно з додатковими) відповідних рядків та стовпців, одержуємо матрицю

$$\begin{Vmatrix} 10 & 01 & 01 \\ 11 & 01 & 00 \\ 00 & 01 & \end{Vmatrix},$$

з якої виходить, що викривленим є елемент першого рядка й другого стовпця, а величина викривлення дорівнює 01. Після чого корекція b-розрядного викривлення стає тривіальною.

Узагальнений завадостійкий код умовних лишків. Алгоритми кодування–декодування

Ще одним із прикладів узагальнених кодів є [1] код умовних лишків (лишків умовних код, ЛУ-код), який дозволяє знаходити й виправляти b-розрядні пакети викривлень, згруповані в межах будь-якого з n узагальнених символів і потребує при цьому надмірність біля

$$r \approx 2b + 1$$

двійкових розрядів (оскільки $p_k \approx 2p_n\, p_{n+1}$, $r = [\log 2p_k] + 1$).

Оскільки в основі ЛУ-коду лежать властивості системи лишкових класів (СЛК), то в цьому коді принципово можуть бути використані відомі алгоритми кодування–декодування. До таких алгоритмів відносяться алгоритм нулізації і, так званий Z-алгоритм [4].

В основі цих алгоритмів лежить той факт, що будь-яке викривлення в одній із груп розрядів α_i переводить початкове число з робочого діапазону $[0, P = \prod_{i=1}^{k} p_i)$ до діапазону $[P, R = p_k \cdot P)$, тобто призводить (див. рис. 3) до збільшення початкового числа $A' < P$ на деяку величину $l_i \cdot R_i$. Тут l_i і $R_i = R/p_i$ — цілі числа. Дійсно, якщо вихідне число

$$A = \alpha_1, \alpha_2, \ldots, \alpha_i, \ldots, \alpha_n, \alpha_k$$

є викривленим по основі p_i і має вигляд:

$$\widetilde{A} = \alpha_1, \alpha_2, \ldots, \widetilde{\alpha}_i, \ldots, \alpha_n, \alpha_k,$$

де

$$\widetilde{\alpha}_i = \{\alpha_i + \Delta\alpha_i\} \pmod{p_i},$$

то це є еквівалентним наступному перетворенню (при виконанні операцій у лишкових класах):

$$\widetilde{A} = (\alpha_1, \alpha_2, \ldots, \alpha_i, \ldots, \alpha_n, \alpha_k) + (0, 0, \ldots, \Delta\alpha_i, \ldots, 0, 0) =$$
$$= (\alpha_1, \alpha_2, \ldots, \{\alpha_i + \Delta\alpha_i\} \pmod{p_i}, \ldots, \alpha_{n1}, \alpha_k).$$

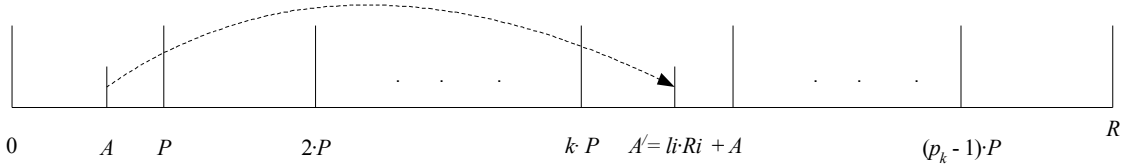

Рис. 3. Вихід викривленого числа за межі робочого діапазону

При цьому величина викривлення перевищує величину робочого діапазону P:

$$\Delta A = (0, 0, \ldots, \Delta\alpha_i, \ldots, 0, 0) > P,$$

оскільки тільки число вигляду

$$\Delta A = l_i \cdot R_i = l_i \cdot R/p_i$$

має всі лишки, окрім лишка по основі p_i, такими, що дорівнюють нулю. Але $\Delta A = l_i \cdot R_i > P = R/p_k$, тобто навіть при $l_i = 1$ величина $R/p_i > R/p_k$ за тієї причини, що $p_k > p_i$.

Відтак, сума $\widetilde{A} = A' + \Delta A > P$, тобто викривлене число, вийшло за межі робочого діапазону P і попало до діапазону $[P, R)$. Отже, цей факт можна використати в алгоритмах кодування–декодування. Один із таких алгоритмів — алгоритм нулізації — розглянуто в [1]. У цій статті розглянемо ще один — Z-алгоритм.

Для виявлення викривлень у Z-алгоритмі використовується відмічений вище факт, що викривлене число виходить за межі робочого діапазону, тобто:

$$\widetilde{A} \geq P. \tag{3}$$

Скористаємось відомим співвідношенням для переводу чисел з СЛК у позиційну систему числення:

$$\widetilde{A} = \sum_{i=1}^{i=n+1} \alpha_i B_i - \left[(1/R) \sum_{i=1}^{i=n+1} \alpha_i B_i \right] \times R, \tag{4}$$

де B_i — константа системи числення, її ортогональний базис, причому

$$B_i = R \cdot m_i / p_i,\ (i = 1, 2, \ldots, n + 1); \tag{5}$$

$(n + 1)$ — число умовних основ, включаючи контрольну; m_i — ціле позитивне число («вага» ортогонального базису B_i), таке, при якому $m_i B_i \pmod{p_i} = 1$.

Підставивши вираз (4) у (3) з урахуванням (5), отримаємо:

$$\sum_{i=1}^{i=n+1} \alpha_i R m_i / p_i - \left[(1/R) \sum_{i=1}^{i=n+1} \alpha_i R m_i / p_i \right] \times R > R / p_k . \tag{6}$$

Скоротивши обидві частини (6) на R, отримаємо, що в разі наявності викривлень,

$$Z > 1/p_к, \tag{7}$$

де

$$Z = \sum_{i=1}^{n+1} \alpha_i m_i / p_i - \left[\sum_{i=1}^{n+1} \alpha_i m_i / p_i \right]. \tag{8}$$

Вирази (7), (8) визначають Z-алгоритм декодування для ЛУ-коду, який лише визначає наявність викривлень. Цей алгоритм включає $(n + 1)$ незалежних (за необхідності одночасних) операцій множення коду i-ї групи ($i = 1,\ldots, n + 1$) на відповідну константу і потім додавання $(n + 1)$ отриманих добутків.

Для побудови алгоритму, здатного не лише визначати наявність, але й виправляти викривлення, скористаємось наступними міркуваннями.

Оскільки викривлення по i-й основі, як показано вище, має величину $\Delta A = l_i \cdot R_i = l_i \cdot R / p_i$, то очевидним є нерівність:

$$\widetilde{A} - l_i \cdot R_i < P, \tag{9}$$

причому величина l_i визначається з виразу:

$$[\widetilde{A} / R_i] = [(A + l_i \cdot R_i) / R_i] = l_i. \tag{10}$$

Тоді з урахуванням (4)–(6), (9) вираз (10) набуде вигляду:

$$Z \cdot p_i - [Z \cdot p_i] < p_i / p_к, \tag{11}$$

Ясно, що вираз (6) і еквівалентний йому вираз (11) справедливі лише для тієї основи p_i, у лишку якої мається викривлення. Відтак, вираз (11) дозволяє визначити місце (номер групи), де виникло викривлення. Неважко впевнитися, що величина цього викривлення:

$$\Delta\alpha_i = \{[\widetilde{A} / R_i] \cdot R_i\}_{p_i} = \{[Zp_i] \cdot R_i\}_{p_i}.$$

Власне виправлення зводиться до операції:

$$\alpha_i = \{\breve{\alpha}_i - \Delta\alpha_i\}_{p_i}. \qquad (12)$$

Таким чином, вирази (8), (11), (12) визначають *Z*-алгоритм декодування для корегувального ЛУ-коду.

Причому, оскільки лишки по будь-яким основам є рівноправними, то все сказане вище відноситься й до контрольної основи. Прийнявши на етапі кодування $\alpha_k = 0$, отримаємо:

$$\alpha_k = (p_k - P \cdot [Z \cdot p_k]) \pmod{p_k}, \qquad (13)$$

і тоді вирази (8), (13) визначають *Z*-алгоритм кодування.

Розглянемо приклади використання *Z*-алгоритму стосовно $p_1 = 4$, $p_2 = 5$, $p_3 = 7$, $p_k = 71$, розрахувавши попередньо константи, які є необхідними для визначення змінних *Z*. Для обраних умов отримаємо: $P = 4 \cdot 5 \cdot 7 = 140$; $R = P \cdot p_k = 9940$.

При цьому $R_1 = 2485$; $R_2 = 1988$; $R_3 = 1420$; $R_4 = P = 140$, $m_1 = 1$; $m_2 = 2$; $m_3 = 6$; $m_4 = 3$. Позначивши значення m_i / p_i як g_i, отримаємо:

$$g_1 = 0{,}25;\ g_2 = 0{,}4;\ g_3 = 0{,}85714;\ g_4 = 0{,}493257.$$

Приклад. Закодувати повідомлення 11.01.10 із використанням *Z*-алгоритму ЛУ-коду. Приймемо на етапі кодування $\alpha_4 = 0$. З виразу (8) отримаємо:

$$Z =]\alpha_1 \cdot g_1 + \alpha_2 \cdot g_2 + \alpha_3 \cdot g_3 + \alpha_4 \cdot g_4[=$$

$$=]3 \cdot 0{,}25 + 1 \cdot 0{,}4 + 2 \cdot 0{,}857142 + 0 \cdot 0{,}493257[=]2{,}86428[= 0{,}86428,$$

де позначка $]x[$ означає обрахування дробової частини від величини *x*.
Тоді, згідно з (13):

$$\alpha_4 = (p_4 - P \cdot [z \cdot p_4]) \pmod{p_4} = (71 - 140 \cdot [0{,}86428 \cdot 71]) \pmod{71} = 51_{(10)} = 110011_{(2)}.$$

Приклад. Знайти й виправити викривлення в повідомленні, що використане вище, де

$$\breve{A} = 11.01.01.110011.$$

Тоді

$$Z =]3 \cdot 0{,}25 + 1 \cdot 0{,}4 + 1 \cdot 0{,}857142 + 51 \cdot 0{,}493257[=]27{,}147949[= 0{,}147949.$$

Оскільки, згідно з виразом (7):

$$Z = 0{,}147949 > 1/p_k,$$

то робимо висновок про наявність викривлення в наданій кодовій комбінації. Для виявлення місця викривлення оцінюємо справедливість нерівностей (11):

$$Z\cdot p_1 - [Z\cdot p_1] = 0{,}91796 < p_1/p_k = 0{,}09859 \text{ — нерівність не є справедливою,}$$

$$Z\cdot p_2 - [Z\cdot p_2] = 0{,}739745 < p_2/p_k = 0{,}070422 \text{ — нерівність не є справедливою,}$$

$$Z\cdot p_3 - [Z\cdot p_3] = 0{,}035643 < p_3/p_k = 0{,}09859 \text{ — нерівність є справедливою.}$$

Звідки витікає висновок про викривлення в третій групі розрядів величиною

$$\Delta\alpha_3 = \{[Zp_3]\cdot R_3\}_{p_3} = \{[1{,}03561{,}22]\cdot 1420\}_7 = \{1420\}_7 = 6,$$

тому

$$\alpha_3 = \{\alpha_3 - \Delta\alpha_3\}_{p_3} = \{1 - 6\}_7 = 2 = 10_{(2)}.$$

Порівнюючи отримане значення α_3 з вихідним (приклад 3), упевнюємося в правильній корекції знайденого викривлення.

Таким чином, застосування запропонованих узагальнених кодів дозволяє забезпечити виявлення та виправлення викривлень в b-розрядних узагальнених символах у кожному з базових кодових слів. З урахуванням перемежування глибиною λ довжина пакетів викривлень в узагальнених кодових словах, які можуть бути виправленими, може дорівнювати $\lambda\cdot b$ двійкових символів. Застосування таких кодів, на погляд авторів, дозволить розв'язати сформульовану проблему щодо надійного забезпечення цілісності інформаційних об'єктів в умовах впливу пакетів викривлень значної тривалості.

1. *Матов О.А., Василенко В.С.* Узагальнені завадостійкі коди в задачах забезпечення цілісності інформаційних об'єктів. Код умовних лишків. // Реєстрація, зберігання і оброб. даних. — 2006. — Т. 8, № 3. — С. 48–66.

2. *Дубровский В.В.* CDMA — взгляд глазами профессионала // mailto:v_dubrovskii@mail.ru.

3. *Акушский И.Я., Юдицкий Д.И.* Машинная арифметика в остаточных классах. — М.: Сов. радио, 1966. — 421 с.

4. *Василенко В.С., Будько М.М., Короленко М.П.* Контроль и відновлення цілісності інформації в автоматизованих системах // Правове, нормативне та метрологічне забезпечення Системи захисту інформації в Україні. — К.: НТУУ «КПІ», 2002. — Вип. 4. — С. 119–128.

Надійшла до редакції 08.12.2006