УДК 681.3

В. С. ВАСИЛЕНКО, О. К. ЮДІН

АЛГОРИТМИ КОДУВАННЯ-ДЕКОДУВАННЯ УЗАГАЛЬНЕНОГО ЗАВАДОСТІЙКОГО КОДУ УМОВНИХ ЛИШКІВ В ЗАДАЧАХ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ

Вступ

Викривлення іформації, тобто порушення її цілісності, можливі на будь-якому етапі її циркуляції у обчислювальних мережах: при зберіганні, передачі або обробці. Для усунення таких викривлень на етапах передачі чи зберігання широко застосовуються різноманітні завадостійкі коди та відповідні алгоритми кодування-декодування. Одним із класів таких кодів є узагальнені коди, при застосуванні яких операції при кодуванні-декодуванні здійснюються над групами двійкових розрядів – узагальненими символами.

Під кодом умовних лишків розуміється представлення інформаційного об'єкту заданої розрядності – базового кодового слова, групи розрядів (пакети) якого, незалежно від системи попереднього кодування, розглядаються як лишки деякого умовного числа А в системі лишкових класів (СЛК). Код кожної i-ї групи (пакету) розглядається як s – значний розряд α_i, який може приймати будь-яке з s значень від 0 до $s-1$, де $s = 2^b$ і умовно вважається лишком згаданого умовного числа А по основі p_i. Для вирішення задач забезпечення виявлення і, можливо, виправлення викривлень в таке представлення вводиться надлишкова інформація у вигляді лишка від ділення числа А на додаткову контрольну основу, яка повинна задовольняти сформульованим в [1] умовам. Тоді на таке представлення розповсюджуються можливості СЛК по виявленню і виправленню викривлень в будь-якій групі розрядів. Відомі алгоритми кодування-декодування [1, 2] як раз і використовують цей факт. Нижче пропонується розширення можливостей одного із відомих алгоритмів – алгоритму нулевізації з метою його використання не лише для контролю цілісності, але і її поновлення.

Використання для кодування-декодування алгоритму нулевізації

Суть алгоритму нулевізації зводиться до того, що як при кодуванні, так і при декодуванні числа

$$\tilde{A} = (\alpha_1, \alpha_2, \ldots, \{\alpha_i + \Delta\alpha_i\}_{p_i}, \ldots, \alpha_n, \alpha_k)$$

по лишкам усіх n основ, що утворюють робочий діапазон α_i ($i = 1, 2, \ldots, n$), послідовно формуються так звані мінімальні числа виду

$$t_1 = (\alpha_1, \alpha_2', \alpha_3', \ldots, \alpha_n', \alpha_k'),$$
$$t_2 = (0, (\alpha_2 - \alpha_2')_{p_2}, \alpha_3^{(2)}, \ldots, \alpha_n^{(2)}, \alpha_k^{(2)}),$$
$$t_3 = (0, 0, (\alpha_3 - \alpha_3' - \alpha_3^{(2)})_{p_3}, \alpha_4^{(3)}, \ldots, \alpha_n^{(3)}, \alpha_k^{(3)}),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$t_n = (0, 0, 0, \ldots, (\alpha_n - \sum_{j=1}^{n-1} \alpha_n^{(j)})_{p_n}, \alpha_k^{(n)}).$$

Підсумок цих чисел $T = \sum_{i=1}^{n} t_i$ має дві властивості [1]. По-перше лишки цієї суми по всіх основах, окрім p_k, завжди дорівнюють лишкам вихідного числа $\tilde{A}$. По-друге, величина цієї суми завжди є меншою ніж величина робочого діапазону $T < P$, тобто величина Т лежить в межах робочого діапазону і для невикривлених чисел $T = A$.

Неважко помітити, що *процес отримання величини $T = A$ є процесом кодування вихідного* числа ЛУ-кодом, тобто значення A залежить лише від цього вихідного числа і не залежить від невідомої при кодуванні величини лишку по контрольній основі p_k. Цей лишок (контрольна ознака, що розшукується) α_k при цьому дорівнює сумі за модулем $p_к$ усіх проміжних величин $\alpha_k^{(i)}$ (i = 1, 2, ..., n) тобто:

$$\alpha_k = (\sum_{i=1}^{n} \alpha_k^{(i)})\ (\mathrm{mod}\ p_k).$$

При декодуванні ж віднімання із числа $\tilde{A}$ величини T приводить до того, що отримана різниця

$$\tilde{A} - T = k \cdot P$$

має по всіх основах, окрім контрольної, лишки, що дорівнюють нулю, а по контрольній

$$\gamma = (\alpha_k - (T\ \mathrm{mod}\ p_k))\ (\mathrm{mod}\ p_k) = (k \cdot P)\ (\mathrm{mod}\ p_k),$$

тобто при запису в лишкових класах має вид

$$\tilde{A} - \mathrm{T} = (0, 0, \ldots, 0, \ldots 0, (k \cdot P)\ (\mathrm{mod}\ p_k)),$$

де k = 0, 1, 2, …, p_k.

Для невикривлених чисел, тобто при k = 0, величина γ = 0, для викривлених $\gamma \neq 0$. *Таким чином установлюється факт наявності чи відсутності викривлень.*

Для ілюстрації можливостей алгоритму розглянемо два приклади.

Приклад. Хай необхідно закодувати з використанням алгоритму нулевізації вихідний код 110110, вважаючи, що можлива довжина пакета викривлень b = 2. Тоді можливе розбиття вихідного коду на три (n = 3) двохрозрядні групи α_1 =11, α_2 =01, α_3 =10, s = 4, а в якості умовних основ можна вибрати p_1 = 4, p_2 = 5, p_3 = 7. При цьому значення контрольної основи ($p_к > 2 \cdot p_n \cdot p_{n-1}$ = 2·5·7 = 70) можна вибрати $p_к$ = 71, що потребує для свого відображення семи розрядів. Внаслідок цього для кодування формується код

$$\mathrm{A} = 011.001.010.0000000.$$

Перше мінімальне число t_1 повинне мати лишок по першій основі, що дорівнює $11_{(2)} = 3_{(10)}$. Таким числом є t_1 = 3 або при представленні в СЛК з вибраними основами

$$t_1 = 11.011.011.0000011.$$

Друге мінімальне число t_2 повинне мати лишок по першій основі, який дорівнює нулю, а по другій

$$(\alpha_2 - \alpha'_2)\ (\mathrm{mod}\ p_2) = (1 - 3)\ (\mathrm{mod}\ 5) = 11_{(2)}.$$

Мінімальним числом, яке має такі лишки по першій і другій основам, є t_2 = 8, тобто

$$t_2 = 000.011.001.0001000.$$

Трете мінімальне число t_3 повинно мати нульові лишки по першим двом основам, а по третій

$$(\alpha_3 - \alpha\ _3 - \alpha^{(2)}{}_3)\ (\mathrm{mod}\ p_3) = 5 = 101_{(2)}.$$

Мінімальним числом, що має такі лишки, є t_3 = 40, тобто

$$t_3 = 000.000.101.0101000.$$

Тоді сума цих чисел $\mathrm{T} = \sum_{i=1}^{3} t_i$ дорівнює 51, тобто

$$T = 11.01.10.0110011.$$

Код T є результатом кодування.

Приклад. Декодувати з використанням алгоритму нулевізації для умов наведеного вище прикладу код $\tilde{A}$ = 11.01.01.0110011, в якому викривлена третя пара розрядів. Як і раніше

$$t_1 = 011.011.011.0000011,$$
$$t_2 = 000.011.001.0001000.$$

Для третього мінімального числа t_3

$$(\alpha_3 - \alpha'_3 - \alpha_3^{(2)})\ (\mathrm{mod}\ p_3) = 4 = 100_{(2)}.$$

Мінімальним числом, що має такі лишки, є t_3 = 60, тобто

$$t_3 = 000.000.100.\ 0111100.$$

При цьому

$$T = \sum_{i=1}^{3} t_i = 71,$$

тобто оскільки $(T) \pmod{71} = 0$, то

$$T = 110110.0000000$$

$$\gamma = (\alpha_k - (T \bmod p_k)) \pmod{p_k} = (0110011 - 0000000) \pmod{71} = 51.$$

Оскільки $\gamma \neq 0$, то робіться висновок про наявність в числі, що декодується, викривлення. Оскільки при цьому

$$\gamma = (k \cdot P) \pmod{p_k} = (k \cdot 140) \pmod{71},$$

то $k = 10$, тому що $1400 \pmod{71} = 51$.

Нескладно упевнитися в тому, що число, що декодується $A = 1471$, може бути отримане тільки внаслідок викривлення вихідного числа $A = 51$ на величину

$$\Delta A = 1420 = 000.000.110.0000000.$$

тобто при викривленні третьої групи розрядів на величину $\Delta\alpha_3 = 110$, після чого корекція результату здійснюється просто:

$$\alpha_3 = (\tilde{\alpha}_3 - \Delta\alpha_3) \pmod 7) = = (1 - 6) \pmod 7) = 2 = 10_{(2)}.$$

Порівнявши отримане значення з вихідним, невикривленим (умови прикладу 1), упевнюємося в тому, що корекція здійснена вірно. Зрозуміло, однак, що коригування викривлень тим шляхом, який розглянуто вище, тобто шляхом підбирання величини викривлення, є цілком неефективним.

Для виявлення можливостей алгоритму щодо коригування викривлень нагадаємо:

1. Відомий факт, що при $p_к > p_n \cdot p_{n-1}$ між величиною викривлення $\Delta\alpha_i$ і величиною γ є взаємно однозначна відповідність, що дає змогу сподіватися, що, отримавши γ, можна якимось чином визначити місце і величину викривлення, тобто здійснити її виправлення.

2. Те, що на числовій осі величина викривлення $l_i \cdot R_i$ відображається точкою в деякому піддіапазоні «контрольного» діапазону $[(P + 1), R)$. Відповідно, процес викривлення початкового числа А відобразиться переміщенням точки A із робочого діапазону $[0, P)$ в деякий інший піддіапазон. Звернемо увагу на те, що в залежності від величини початкового числа викривлене число (A_1 чи A_2) може попасти в один із суміжних діапазонів із номерами k або $(k - 1)$. Зокрема, при

$$A = A_1 \leq k \cdot P - l_i \cdot R_i,$$

це буде (в уже прийнятих позначеннях) діапазон $((k - 1) \cdot P,\ k \cdot P)$, тобто діапазон із номером $(k - 1)$, а при

$$A = A_2 > k \cdot P - l_i \cdot R_i$$

це буде діапазон $(k \cdot P,\ (k + 1) \cdot P)$, тобто діапазон із номером k.

Внаслідок операції нулевізації із числа A', яке контролюється, віднімаються відповідно числа $T = A' - (k - 1) \cdot P < P$, чи $T = A' - k \cdot P < P$. При цьому по контрольній основі $q = p_k$ одержується результат γ, такий, що відповідає лівій межі піддіапазону $[(k - 1) \cdot P,\ k \cdot P)$, тобто величині $(k - 1) \cdot P$, або ж такий, що відповідає лівій межі піддіапазону $[k \cdot P,\ (k + 1) \cdot P)$, тобто величині $k \cdot P$.

Тобто маємо

$$\gamma = \{k \cdot P\}_q, \text{ або } \gamma = \{(k - 1) \cdot P\}_q.$$

Звідси, за правилами СЛК, отримаємо

$$k = \{\gamma / \{P\}_q\}_q, \text{ чи } (k - 1) = \{\gamma / \{P\}_q\}_q. \tag{1}$$

Тобто, використовуючи вирази (1), завжди можна визначити номер того діапазону, в який потрапило викривлене число, та результат нулевізації – число $k \cdot P$. Оскільки величина викривлення $li{\cdot}Ri$ і результат нулевізації $k{\cdot}P$ є близькими, тобто їх різниця є меншою за величину робочого діапазону P, то це надає принципову можливість визначити місце викривлення.

Оскільки подальші міркування певним чином залежать від можливих співвідношень величин $k{\cdot}P$ та $li{\cdot}Ri$, розглянемо два наступні випадки.

В першому випадку, при $k{\cdot}P > l_i{\cdot}R_i$ значення R_1, яке характеризує величину і місце викривлення, можна визначити із очевидної нерівності

$$k{\cdot}P - [k{\cdot}P/ R_i]{\cdot}R_i < P. \tag{2}$$

Підставимо у (2) замість R_1 його значення у вигляді

$$R_i = P{\cdot}q/ p_i.$$

Тоді

$$k{\cdot}P - [k{\cdot}P/ Ri]{\cdot}Ri = k{\cdot}P - [k{\cdot}P{\cdot}p_i / (P{\cdot}q)]{\cdot} P{\cdot}q/ p_i = k{\cdot}P - [k{\cdot}p_i /q]{\cdot}P{\cdot}q/ p_i < P.$$

Розділивши обидві частини правої частини останнього нерівняння на величину P, отримаємо

$$k - [k{\cdot}p_1 /q]{\cdot}q/p_i < 1.$$

Помножимо обидві частини останнього нерівняння на величину p_i, одержимо:

$$k{\cdot}p_i - [k{\cdot}p_i /q] {\cdot}q < p_i, \tag{3}$$

або

$$\{k{\cdot}p_i\}_q < p_i. \tag{4}$$

Звернемо увагу на те, що в (3), (9) вирази в квадратних дужках є не що інше, як величина l_i:

$$[k{\cdot}P/ R_1] = [k{\cdot}p_i /q] = l_i. \tag{5}$$

Вирази (2) та еквівалентні їм вирази (3), (4) утворюють системи нерівнянь по n (i = 1, 2, ... n) нерівнянь в кожній, в яких справедливим є лише одне нерівняння для того номера і та значення основи p_1, по якій має місце викривлення.

Таким чином, внаслідок розв'язання будь-якої із систем нерівнянь (2)– (4) щодо змінної p_1 місце викривлення стає виявленим.

Для визначення ж його величини проаналізуємо величини $T = A' - k{\cdot}P$, чи $T = A' - (k - 1){\cdot}P$, які формуються по усіх лишках, окрім лишку по контрольній основі в ході операції нулевізації числа, яке контролюється.

Неважко зрозуміти, що вирази (2) – (4) є справедливими в разі, коли величина викривлення $l_i{\cdot}R_i < k{\cdot}P$. В цьому випадку величина сформованого в ході нулевізації числа T є меншою вихідного числа A_2 на величину $(k{\cdot}P - l_i{\cdot}R_i)$, тобто

$$T = A' - k{\cdot}P = A2 - (k{\cdot}P - l_i{\cdot}R_i) < A2, \tag{6}$$

та

$$\Delta \tilde{A} = (k{\cdot}P - li{\cdot}R_i),$$

а величина скоригованого числа повинна визначатися як:

$$A_2 = T + (k{\cdot}P - li{\cdot}R_i).$$

Тобто величина скоригованого значення лишку:

$$\alpha_i = \{\tilde{\alpha}_i + \Delta\tilde{\alpha}_i) = \{T - (k{\cdot}P - l_i{\cdot}\mathrm{R}_i)\}\mathrm{mod}\, p_i = \{\tilde{\alpha}_i - \{l_i{\cdot}\mathrm{R}_i\}\mathrm{mod}\, p_i\}\mathrm{mod}\, p_i,$$

або із урахуванням (5):

$$\alpha_i = \{\tilde{\alpha}_i - \{[k{\cdot}p_i /q]{\cdot}\mathrm{R}_i\}\mathrm{mod}\, p_i\}\mathrm{mod}\, p_i. \tag{7}$$

Приклад. Нехай в СЛК із основами 2, 3, 5, 17 вихідне число 18_{10} = 0, 0, 3, 1 внаслідок викривлення перетворилося на 0, 0, 0, 1 = 120_{10}.

Результат нулевізації дає

$$\Gamma = 0, 0, 0, 1, \gamma = 1.$$

Звідси

$$k = \{\gamma/\{P\}q\}q = \{1/13\}_{17} = 4.$$

Пошук місця викривлення із

$$\{k{\cdot}p_i\}q < p_i$$

для $k = 4$ дає

$$\{4{\cdot}2\}_{17} < 2 \text{ – невірно,}$$
$$\{4{\cdot}3\}_{17} < 3 \text{ – невірно,}$$
$$\{4{\cdot}5\}_{17} < 5 \text{ – вірно,}$$

тобто виявлене викривлення по основі $p_3 = 5$.

Розрахунок скоригованого лишку по основі p_3:

$$\alpha_3 = \{0 - \{[20/17]{\cdot}42\}\bmod 5\}\bmod 5 = 3.$$

Видно, що корекцію викривлення здійснено правильно.

В другому випадку, коли результат нулевізації – число $(k - 1){\cdot}P$ є меншим за величину викривлення $l_i{\cdot}R_i$, обчислення місця і величини викривлення за виразами (6),(7) призведе до невірних результатів. Тоді, з урахуванням властивостей операцій в лишкових класах, для визначення місця та величини викривлення слід скористатися виразом

$$q - \{(k-1){\cdot}p_i\}q < p_i.$$

В разі вірності цієї нерівності по одній із основ p_i правомочним є висновок про те, що

$$\gamma = \{(k-1){\cdot}P\}_q,$$

а отже

$$k = \{\gamma/\{P\}_q\}_q + 1. \tag{8}$$

Зрозуміло, що в цьому разі величина викривлення $l_i{\cdot}R_i > (k - 1){\cdot}P$. Тоді величина сформованого в ході нулевізації числа T є більшою вихідного числа $A2$ на величину $[l_i{\cdot}R_i - (k-1){\cdot}P]$, тобто

$$T = A' - (k-1){\cdot}P = A_1 + [l_i{\cdot}R_i - (k-1){\cdot}P] < A1. \tag{9}$$

Останній вираз може бути представленим у вигляді

$$T = A' - k{\cdot}P = A1 - [(k-1){\cdot}P - l_i{\cdot}R_i].$$

Неважко помітити, що вирази (6) та (9) є тотожними, якщо вважати, що номер діапазону в обох випадках має значення – k. l, хоча значення викривлення при цьому

$$\Delta\bar{A} = -(k{\cdot}P - l_i{\cdot}R_i),$$

величина скоригованого числа повинна визначатися, як і раніше, із виразу

$$A1 = T + ((k-1){\cdot}P - l_i{\cdot}R_i).$$

Тобто величина скоригованого значення лишку:

$$\alpha_i = \{\bar{\alpha}_i + \Delta\alpha_i\} = \{T + ((k-1){\cdot}P - l_i{\cdot}R_i)\}\bmod p_i = = \{\bar{\alpha}_i - \{l_i{\cdot}R_i\}\bmod p_i\}\bmod p_i,$$

або із урахуванням (7) отримаємо, як і раніше:

$$\alpha_i = \{\bar{\alpha}_i - \{[k{\cdot}p_i/q]{\cdot}R_i\}\bmod p_i\}\bmod p_i.$$

Приклад. Нехай в СЛК із основами 2, 3, 5, 17 вихідне число 0_{10} = 0, 0, 0, 0 внаслідок викривлення перетворилося на число 0, 0, 2, 0 = 102_{10}.

Результат нулевізації дає

$$\Gamma = 0, 0, 0, 5, \gamma = 5.$$

Звідси, за правилами виконання операцій в СЛК,

$$k = \{\gamma/\{P\}_q\}_q = \{5/13\}_{17} = (5 + 2{\cdot}17)/13 = 3.$$

Пошук місця викривлення із

$$\{k{\cdot}p_i\}q < p_i$$

для $k = 3$ дає:

$$\{3{\cdot}5\}_{17} = 15 < 5 \text{ – невірно,}$$

а

$$q - \{k{\cdot}p_i\}q < p_i$$

для $(k-1) = 3$

$$17 - 5 = 2 < 5 \text{ – вірно,}$$

тобто, як і в попередньому прикладі, виявлене викривлення по основі p_3, але з урахуванням (8) при $(k-1) = 3$, тобто при $k = 4$.

Розрахунок скоригованого лишку по основі p_3:

$$\alpha_3 = \{2 - \{[20/17]\cdot 42\} \bmod 5\} \bmod 5 = 2 - 2 = 0.$$

Видно, що корекція викривлення здійснена правильно.

Використання для кодування-декодування z-алгоритму.

Для виявлення викривлень в z-алгоритмі використовується відмічений вище факт, що викривлене число виходить за межі робочого діапазону, тобто

$$\tilde{A} \geq P. \quad (10)$$

Скористаємось співвідношенням для переводу чисел із СЛК в позиційну систему числення

$$\tilde{A} = \sum_{i=1}^{i=n+1} \alpha_i B_i - [(1/R)\sum_{i=1}^{i=n-1} \alpha_i B_i] \times R, \quad (11)$$

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

$$B_i = R\cdot m_i/p_i, \ (i = 1, 2, \dots, n+1); \quad (12)$$

– $(n + 1)$ – число умовних основ, включаючи контрольну;

– m_i – ціле позитивне число, «вага» ортогонального базису B_i, таке, при якому

$$m_i B_i \ (\mathrm{mod}\ p_i) = 1.$$

Підставивши вираз (11) в (10) з врахуванням (12), отримаємо

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

Скоротивши в останньому виразі обидві частини на R, отримаємо, що в разі наявності викривлень

$$z > 1/p_к. \quad (13)$$

де

$$Z = \sum_{i=1}^{n-1} \alpha_i m_i / p_i - [\sum_{i=1}^{n+1} \alpha_i m_i / p_i]. \quad (14)$$

Вирази (13), (14) визначають z-алгоритм декодування для ЛУ-коду, який лише визначає наявність викривлень. Цей алгоритм включає $(n + 1)$ незалежних (при необхідності одночасних) операцій множення коду i-ї групи ($i = 1, \dots, n+1$) 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

$$\tilde{A} - l_i\cdot R_i < P. \quad (15)$$

причому величина $l_i\cdot$ визначається з виразу

$$[\tilde{A} / R_i] = [(A - l_i\cdot R_i) / R_i] = l_i \quad (16)$$

Тоді з врахуванням (11), (12), (13), (15) вираз (16) прийме вид

$$z\cdot p_i - [z\cdot p_i] < p_i/p_к, \quad (17)$$

Ясно, що вираз (19) і еквівалентний йому вираз (17) справедливі лише для тієї основи p_i, в лишку якої є викривлення. Відтак, вираз (17) дозволяє визначити місце (номер групп), де виникло викривлення. Неважко упевнитися, що величина цього викривлення

$$\Delta\alpha_i = \{[\tilde{A} / R_i]\cdot R_i\}_{p_i} = \{[zp_i]\cdot R_i\}_{p_i},$$

Власне виправлення зводиться до операції

$$\alpha_i = \{\tilde{\alpha}_i - \Delta\alpha_i\}_{p_i} \quad (18)$$

Таким чином, вирази (14), (17), (18) визначають z-алгоритм декодування для коригуючого ЛУ-коду.

Причому, оскільки лишки по будь-яких основах є рівноправними, то сказане вище стосується і контрольної основи. Прийнявши на етапі кодування $\alpha_k = 0$, отримаємо

$$\alpha_k = (p_k - P\cdot[z\cdot p_k]) \ (\mathrm{mod}\ p_k) \quad (19)$$

і тоді вирази (14), (19) 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 необхідні 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 з використанням z-алгоритму ЛУ-коду. Приймемо на етапі кодування $\alpha_4 = 0$. Із виразу (14) отримаємо

$$Z =]\alpha_1{\cdot}g_1 + \alpha_2{\cdot}g_2 + \alpha_3\, g_3 + \alpha_4{\cdot}\, g_4[\ =]3{\cdot}0.25 + +1{\cdot}0{,}4 + 2{\cdot}0{,}857142 + 0{\cdot}0.493257[\ = 0{,}86428,$$

де позначка]х[означає обчислення астини від величини х.

Тоді згідно з (19)

$$\alpha_4 = (p_4 - P\cdot[z\, p_4])\ (\mathrm{mod}\ p_4) = 51_{(10)} = 110011_{(2)}.$$

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

$$\tilde{A} = 11.01.01.\ 110011.$$

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 (13),

$$z = 0{,}147949 > 1/p_\kappa,$$

то робимо висновок про наявність викривлення в наданій кодовій комбінації.

Для виявлення місця викривлення оцінюємо справедливість нерівнянь (17):

$$z\cdot p_1 - [z\cdot p_1] = 0{,}91796 < p_1/p_\kappa = 0{,}09859,$$

нерівність не є справедливою:

$$z\cdot p_2 - [z\cdot p_2] = 0{,}739745 < p_2/p_\kappa = 0{,}070422,$$

нерівність не є справедливою;

$$z\cdot p_3 - [z\cdot p_3] = 0.035643 < p_3/p_\kappa = 0{,}09859,$$

нерівність є справедливою.

Звідси витікає висновок про викривлення в третій групі розрядів величиною

$$\Delta\alpha_3 = \{[zp_3]\ R_3\}_{p_3} = =\{[1{,}03561.22]\cdot 1420\}_7 = 6,$$

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.

Висновки

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.

Окрім того, слід відмітити, що застосування запропонованих алгоритмів кодування-декодування узагальнених ЛУ-кодів дозволяє забезпечити виявлення та виправлення викривлень в b-розрядних узагальнених символах в кожному із базових кодових слів.

Список літератури 1. *Акушский И.Я., Юдицкий Д.И.* Машинная арифметика в остаточных классах. // М.: Сов. радио, 1966. 421 с. 2. *Василенко В.С., Будько М.М. Короленко М.П.* Управління контролем та оперативним поновленням цілісності інформації в корпоративних мережах. // Управляющие системы и машины. 2000. № 5/6. С. 128 – 134

Харківський національний
університет радіоелектроніки

Надійшла до редколегії 04.03.2007