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
вул. Космонавта Комарова, 1, 03058 Київ, Україна

Процедура нулізації при контролі та поновленні цілісності інформаційних об'єктів у коді умовних лишків

Запропоновано швидкодіючі процедури контролю цілісності та корегування спотворень інформаційних об'єктів телекомунікаційних мереж на основі алгоритму нулізації в умовах застосування коду умовних лишків.

Ключові слова: *завадостійке кодування, код умовних лишків, контроль цілісності, контрольна основа, основа коду, поновлення цілісності, спотворення.*

Вступ

Разом із задачею забезпечення цілісності інформаційних об'єктів у сучасних телекомунікаціях не менш важливою є задача забезпечення доступності цих об'єктів. З цією метою прагнуть підвищувати швидкість інформаційного обміну при збереженні можливостей щодо цілісності. Однією із можливостей цього є застосування багаторівневих (багатопозиційних) символів. Однак при цьому спотворення одного із символів призводить до появи групового (наприклад, у декількох бітах) спотворення (спотворення узагальненого символу). Для виявлення таких спотворень доцільно застосовувати спеціальні коди для виявлення і (можливого) виправлення спотворень в узагальнених символах. Одним із таких кодів є код умовних лишків (ЛУ-код) [1, 2, 4]. У таких кодах відповідний інформаційний об'єкт розглядається як деяке число, яке за певними правилами розподіляється на декілька, наприклад на n груп, двійкових розрядів. Ці групи, у свою чергу, розглядаються як залишки a_i від ділення деякого умовного числа в позиційній системі числення A на набір умовних основ p_i (i = 1, 2, …, n):

$$A = a_1, a_2, ..., a_n .$$

Для забезпечення функцій контролю, а, можливо, контролю та поновлення цілісності до складу основ додають додаткові (одну чи, в загальному випадку, декілька) контрольні, надлишкові основи системи числення, наприклад p_q, та обраховують (на етапі кодування) лишок по контрольній основі (якщо контрольна основа одна) a_q.

Відомі алгоритми кодування-декодування в таких кодах. Одним із таких алгоритмів є, так званий, *z*-алгоритм. Його перевагою є відносна простота суто алгебраїчних процедур, але суттєвим недоліком — застосування у цих процедурах операції обчислення цілої частини від нескінчених дробових чисел, що може стати причиною неправильного кодування-декодування. Іншим є алгоритм нулізації, який не має операцій над нескінченими дробовими числами, але у відомих описах і реалізаціях цей алгоритм використовується лише для виявлення факту наявності спотворень [3], або ж для реалізації потребує великої кількості операцій, а відтак, і значних часових витрат [4].

Метою цієї роботи є розроблення процедури застосування алгоритму нулізації не лише в режимі виявлення, а й у режимі швидкодійного корегування спотворень.

Використання алгоритму нулізації для виявлення та корегування спотворень

Як відомо [3], внаслідок декодування із застосуванням процедури нулізації отримується величина, яка має лишки по всім основам, окрім контрольної, що дорівнюють нулю, а по контрольній — лишок, величина якого

$$\gamma = (kP) \bmod p_q,$$

де $k = 0, 1, 2, \ldots, p_q - 1$. Для неспотворених чисел, тобто при $\gamma = 0$, величина $k = 0$, для спотворених $\gamma \neq 0$. Отже, *визначений алгоритм надає змогу виявлення факту наявності спотворень.*

Звернемо увагу, що з останнього виразу нескладно визначити номер піддіапазону *k*, до якого попадає спотворене число *A*:

$$k = (\gamma/P) \bmod p_q.$$

Проілюструємо сказане на прикладах кодування-декодування із застосуванням у ЛУ-коді процедур нулізації, що буде корисним і при подальших міркуваннях.

Приклад 1. Нехай необхідно закодувати з використанням алгоритму нулізації вихідний код 110110, вважаючи, що довжина узагальненого символу, а отже і можлива довжина пакету спотворень $b = 2$. Тоді можливе розбиття вихідного коду на три ($n = 3$) дворозрядні групи $\alpha_1 = 11_2$, $\alpha_2 = 01_2$, $\alpha_3 = 10_2$, $s = 4$, а як умовні основи можна вибрати $p_1 = 4$, $p_2 = 5$, $p_3 = 7$. При цьому як значення контрольної основи можна вибрати $p_q = 71$ (нагадаємо, що контрольна основа повинна задовольняти умові $p_q > 2 \cdot p_n \cdot p_{n-1} = 2 \cdot 5 \cdot 7 = 70$), що потребує для свого відображення семи розрядів. Унаслідок цього для кодування формується код

$$A = 11.01.10.0000000.$$

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

$$t_1 = 11.11.011.0000011.$$

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

$$((\alpha_2 - \alpha_2^1) \pmod{p_2}) = (1 - 3) \pmod 5 = 11_{(2)}.$$

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

$$t_2 = 00.11.001.0001000.$$

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

$$((\alpha_3 - \alpha_3^1 - \alpha_3^2) \pmod{p_3}) = (2 - 3 - 1) \pmod 7 = 5 = 101_{(2)}.$$

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

$$t_3 = 00.00.101.0101000.$$

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

$$T = 11.01.10.0110011.$$

Код $T = A$ є результатом кодування.

Приклад 2. Необхідно декодувати з використанням алгоритму нулізації базове кодове слово $\widetilde{A}$ = 11.01.01.0110011, в якому спотворена третя пара розрядів при спотворенні первинного значення коду третьої групи 10 на величину 110 так, що (10 – 110) mod 7 = 01. Як і раніше (приклад 1):

$$t_1 = 11.11.011.0000011,$$
$$t_2 = 00.11.001.0001000.$$

Для третього мінімального числа t_3

$$((\alpha_3 - \alpha_3^1 - \alpha_3^2) \pmod{p_3}) = (1 - 3 - 1) \pmod 7 = 4 = 100_{(2)}.$$

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

$$t_3 = 00.00.100.\ 0111100.$$

При цьому

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

але оскільки $T(\text{mod } 71) = 71(\text{mod } 71) = 0$, то $T = 11.01.01.0000000$

і $\gamma = (\alpha_q - (\text{T mod } p_q))\ (\text{mod } p_q) = (0110011 - 0000000)\ (\text{mod } 71) = 51.$

Оскільки $\gamma \neq 0$, то можна зробити *висновок про наявність спотворення в числі, що декодується*.

Для корегування спотворень за результатами нулізації слід визначити не лише факт наявності спотворень, але і їхнє місце та величину. Одним із можливих кроків на цьому шляху є визначення, до якого з інтервалів (піддіапазонів) величиною P потрапляє спотворене число.

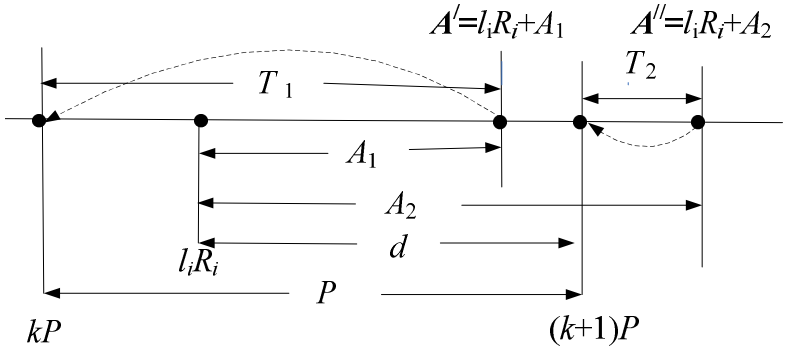
Нагадаємо, що введення контрольної основи величиною p_q призводить до розширення діапазону представлення P в p_q разів, іншими словами утворює p_q піддіапазонів величиною P кожен. Нагадаємо також [3], що спотворене число може бути представленим як сума початкового (не спотвореного) числа A та вектора спотворень E: $\widetilde{A} = A + E$, де $A = a_1, a_2, ..., a_i, ...a_q$ — вихідне (неспотворене) число, а вектор спотворення E в СЛК має лишки, що дорівнюють нулю по усім основам, окрім тієї, де є спотворення. Тоді вектор спотворення є числом виду $E = 0,0,..., \Delta a_i, 0,0,..., 0 \ = l_i \cdot R_i$.

Тобто $E = 0,0,..., (l_i \cdot R_i) \text{mod} p_i, 0,0,..., 0$, оскільки тільки числа, які діляться націло на $R_i = R / p_i$ мають у своєму представленні в системі лишкових класів (СЛК) такий набір лишків. У останніх виразах величина $R = \prod_{i=1}^{k=n+1} p_i$ — контрольний (повний) діапазон представлення чисел у СЛК, а лишок від спотворення ΔA_i у СЛК має вигляд $\Delta a_i = E \bmod p_i = (l_i \cdot R_i) \bmod p_i$. Тобто спотворене число $\widetilde{A} = A + E$, а спотворений лишок по основі p_i має значення:

$$\widetilde{a}_i = \widetilde{A} \bmod p_i = (A + E) \bmod p_i = (a_i + \Delta a_i) \bmod p_i . \qquad (1)$$

На числовій осі (див. рисунок) величина спотворення $l_i \cdot R_i$ відображається точкою в одному з піддіапазонів «контрольного» діапазону $[(P + 1), R)$. Відповідно, процес спотворення початкового числа A відобразиться переміщенням точки A із робочого діапазону $[0, P)$ до деякого піддіапазону з номером k, тобто до піддіапазону $[k \cdot P, (k \cdot P + 1))$. Звернемо увагу на те, що, залежно від величини початкового чис-

ла A спотворене число ($A' = l_i \cdot R_i + A_1$ чи $A'' = l_i \cdot R_i + A_2$), може попасти до діапазону з номером k при $A_1 < d = (k + 1) \cdot P - l_i \cdot R_i$, або до діапазону з номером $(k + 1)$ при $A_2 \geq d$. Звернемо увагу на несуттєву залежність номеру піддіапазону від величини початкового (неспотвореного) числа та на суттєву його залежність від місця та величини спотворення. Іншими словами, спотворення певної величини в певному умовному лишку призводить до переміщення будь-якого вихідного числа лише до одного із двох суміжних піддіапазонів з номерами k або $(k + 1)$.



Ілюстрація процесу нулізації

Звідси робимо висновок, що визначення у будь-який спосіб величини $l_i \cdot R_i$, забезпечує визначення місця спотворення (i), його величини $\Delta a_i = (l_i \cdot R_i) \bmod p_i$. Із рисунка зрозуміло також, що номер піддіапазону k нескладно визначити із очевидного співвідношення

$$k = [l_i \cdot R_i / P],$$

де позначка $[X]$ означає обчислення цілої частини від X.

Як видно із рисунку, відстань між величиною $l_i \cdot R_i$ та найближчими до неї величинами $k \cdot P$ та $(k \cdot P + 1)$ завжди є меншою ніж величина робочого діапазону P. Цей факт можна використати для визначення величини $l_i \cdot R_i$ шляхом розв'язання систем нерівнянь:

$$l_i \cdot R_i - k \cdot P < P, \qquad (2,a)$$

$$(k+1) \cdot P - l_i \cdot R_i < P. \qquad (2,б)$$

Тобто, після операції нулізації та визначення k і встановлення факту наявності спотворення ($\gamma \neq 0$), рішення цих систем — знаходження вірної нерівності шляхом перебору i, та, відповідно R_i, і дозволяє визначити всі шукані змінні, необхідні для корегування цього спотворення: i — номер спотвореної групи розрядів (спотвореного лишку), місце спотворення та $\Delta a_i = (l_i \cdot R_i) \bmod p_i$ — величина спотворення:

$$a_i = (\tilde{a}_i - \Delta a_i) \bmod p_i. \qquad (3)$$

Таким чином, **алгоритм виявлення факту наявності та корегування спотворень складається з наступних етапів**.

1. Виявлення факту наявності спотворень шляхом аналізу результату нулізації величини γ: при $\gamma \neq 0$ робиться *висновок про наявність спотворення*.

2. Визначення номеру піддіапазонів k чи $(k+1)$, до якого, залежно від початкового значення вихідного числа A, попало спотворене число $\widetilde{A}$.

3. Визначення місця спотворення: i — номеру спотвореної групи розрядів, а отже, спотвореного лишку $\widetilde{a}_i$, та величини спотворення $\Delta a_i = (l_i \cdot R_i) \bmod p_i$.

4. Корегування спотворень.

Послідовність операцій (процедур) *першого етапу* є відомою і додатково розглядалася вище. Найбільш зрозумілим шляхом визначення номеру піддіапазонів k чи $(k+1)$ на другому етапі є реалізація операцій (процедур) з розв'язання систем нерівнянь (2,*а*) та (2,*б*). Розглянемо послідовність цих операцій.

Визначення номерів піддіапазонів k чи $(k+1)$ *на другому етапі* розглянемо як продовження **прикладу 2**. Для цього скористаємося наведеним раніше співвідношенням $\gamma = (kP) \bmod p_q$. Із цього виразу номер піддіапазону $k = \{\gamma / \{P\}_{p_q}\}_{p_q}$ і для умов прикладу 2: $k = \{51/\{140\}_{71}\}_{71} = \{51/69\}_{71} = 10$ і, відповідно, $(k+1) = 11$.

Завдання *третього етапу* розглянемо шляхом розв'язання систем нерівнянь (2,*а*) та (2,*б*) щодо спотвореного числа $\widetilde{A}$ = 11.01.01.0110011, коли вже виконані операції етапів 1 та 2 внаслідок чого одержано: $\gamma \neq 0$, зроблено висновок про наявність спотворення в числі, що декодується, та можливі номери піддіапазонів розташування спотворення $k = 10$ і $(k+1) = 11$.

Нагадаємо, що в цій роботі розглядаються приклади для системи числення з константами: величина робочого діапазону $P = 4 \cdot 5 \cdot 7 = 140$, величина повного діапазону $R = P \cdot p_q = 4 \cdot 5 \cdot 7 \cdot 71 = 9940$, $R_1 = R/p_1 = 2485$, $R_2 = R/p_2 = 1988$, $R_3 = R/p_3 = 1420$. Тоді, окрім того, $k \cdot P = 1400$, та $(k+1) \cdot P = 1540$.

Для розв'язання систем нерівнянь (2,*а*), (2,*б*) необхідними є додаткові константи системи числення, якими є величини можливих спотворень у цій системі числення $l_i \cdot R_i$ для всіх номерів умовних основ i та усіх значень номерів відповідних піддіапазонів l_i. Ці константи розраховуються в процесі розв'язання систем нерівнянь (2,*а*) та (2,*б*).

Розглянемо послідовність операцій при розв'язання систем нерівнянь (2,*а*) та (2,*б*).

1. Для аналізу можливого спотворення в першій групи (умовний лишок по основі $p_1 = 4$ (6 операцій порівняння)), необхідно в міру зміни значення l_1 розрахувати:

— при $l_1 = 1$: $\Delta A = l_1 \cdot R_1 = 2485$; при $l_1 = 2$: $\Delta A = l_1 \cdot R_1 = 4970$; при $l_1 = 3$: $\Delta A = l_1 \cdot R_1 = 7455$;

— при перевірці правильності нерівнянь (21,*а*) та (2,*б*), оскільки $k \cdot P = 1400$ і $(k+1) \cdot P = 1540$ є меншими ніж найменше з $l_1 \cdot R_1 = 2485$, вочевидь, робимо висновок про відсутність рішень зазначених нерівностей.

2. Для аналізу можливого спотворення в другій групі (умовний лишок по основі $p_2 = 5$ (8 операцій порівняння), необхідно в міру зміни значення l_2 розрахувати:

— при l_2 =1: $\Delta A = l_2 \cdot R_2 = 1988$; при l_2 =2: $\Delta A = l_2 \cdot R_2 = 3976$; при $l_2 = 3$: $\Delta A = l_2 \cdot R_2 = 5964$; при l_2 =4: $\Delta A = (l_2 \cdot R_2) = 7952$;

— при перевірці правильності нерівнянь (2,*а*) та (2,*б*), оскільки $k \cdot P = 1400$ і $(k+1) \cdot P = 1540$ є меншими ніж найменше з $l_2 \cdot R_2 = 1988$ також робимо висновок про відсутність рішень зазначених нерівностей.

3. Для аналізу можливого спотворення в третій групі (умовний лишок по основі $p_3 = 7$ (до 12 операцій порівняння), необхідно в міру зміни значення l_3 розрахувати:

— при $l_3 = 1$: $\Delta A = l_3 \cdot R_3 = 1420$; при $l_3 = 2$: $\Delta A = l_3 \cdot R_3 = 2840$; при $l_3 = 3$: $\Delta a_3 = = (l_3 \cdot R_3) = 4260$; при $l_3 = 4$: $\Delta A = l_3 \cdot R_3 = 5680$; при $l_3 = 5$: $\Delta A = l_3 \cdot R_3 = 7100$; при $l_3 = 6$: $\Delta A = l_3 \cdot R) = 8520$;

— при перевірці правильності нерівнянь (2,*а*) та (2,*б*), виявляється випадок задовольняння нерівності для $k \cdot P = 1400$ при $l_3 \cdot R_3 = 1420$ ($l_3 \cdot R_3 - k \cdot P = = 1420 - 1400 = 20 < 140$), звідки витікає рішення про наявність спотворення третьої групи розрядів вихідного числа зазначених нерівностей.

Величина спотворення — $\Delta a_3 = (l_3 \cdot R_3) \bmod p_3 = 1420 \bmod 7 = 6$, а операція корегування спотворення $a_3 = (\widetilde{a}_3 - \Delta a_3) \bmod p_3 = (1-6) \bmod 7 = 2 = 10_2$, що відповідає значенню цієї групи у неспотвореному числі.

Оскільки максимальна кількість операцій при розв'язанні систем нерівнянь (2,*а*) та (2,*б*) дорівнює $(p_i - 1)$ для кожної із *n* груп, то максимальна кількість операцій при розв'язанні систем нерівнянь по усім *n* групам складе: $(\sum_{i=1}^{n} p_i - n)$. Отже, при великій кількості умовних основ p_i та їхніх значних величинах тривалість третьої процедури алгоритму виявлення факту наявності та корегування спотворень може бути суттєвою. Із цього витікає висновок щодо необхідності виявлення можливостей щодо її прискорення.

Табличне корегування спотворень за результатами нулізації

Прискорення цієї процедури є можливим у разі використання однозначної функціональної пов'язаності між результатами виконання операції нулізації γ, можливими номерами суміжних піддіапазонів величиною P — $k = \{\gamma / \{P\}_{p_q}\}_{p_q}$ (чи, можливо (k +1), що залежить від величини неспотвореного числа, яке контролюється), та величиною спотворення вихідного числа $E = (l_i \cdot R_i)$, а отже, величиною спотворення Δa_i та номером *i* спотвореної групи у числі, яке контролюється.

З викладеного робимо висновок, що при застосуванні нулізації для встановлення факту наявності спотворень ($\gamma \neq 0$) для будь-якого спотворення $\Delta A_i = l_i \cdot R_i$ та прискорення процедури із визначення місця та величини спотворень доцільно заздалегідь визначити та створити таблицю відповідності між результатом нулізації γ (чи парою суміжних номерів піддіапазонів k, (k + 1)) та Δa_i, l_i. Зрозуміло, що така таблиця формується для умов застосування певної системи умовних лишків, тобто певного набору основ такої системи. Звернемо увагу на те, що для кожного

із можливих спотворень Δa_i взаємно пов'язані величини γ, k, та, відповідно (k + + 1), можуть бути визначеними із уже застосованих чи зрозумілих співвідношень:

$$\Delta a_i = (l_i \cdot R_i) \bmod p_i,\ k = [l_i \cdot R_i / P],\ \gamma = \{k \cdot P\}_{p_q}.$$

Формування такої таблиці розглянемо на прикладі вже розглянутої у попередніх прикладах системи умовних лишків, що дозволяє виявляти та виправляти спотворення в дворозрядних групах із $p_1 = 4$, $p_2 = 5$, $p_3 = 7$ та $p_q = 71$ та її основними константами: величина робочого діапазону $P = 4 \cdot 5 \cdot 7 = 140$, величина повного діапазону $R = 9940$, $R_1 = R/p_1 = 2485$, $R_2 = R/p_2 = 1988$, $R_3 = R/p_3 = 1420$.

Знайдемо співвідношення між величинами можливих спотворень і номерами піддіапазонів, до яких може бути «переміщеним» унаслідок цих спотворень вихідний інформаційний об'єкт у такій системі числення:

— для $l_1 = 1$: $\Delta a_1 = (l_1 \cdot R_1) \bmod 4 = 2485 \bmod 4 = 1$; $k = [2485/140] = 17$, $\gamma = \{17 \cdot 140\}_{71} = \{2380\}_{71} = 37$; $(k+1) = 18$; $\gamma = \{18 \cdot 140\}_{71} = \{2520\}_{71} = 35$; для $l_1 = 2$: $\Delta a_1 = (l_1 \cdot R_1) \bmod 4 = 4970 \bmod 4 = 2$, $k = [4970/140] = 35$, $\gamma = \{35 \cdot 140\}_{71} = \{4900\}_{71} = 1$; $(k+1) = 36$, $\gamma = \{36 \cdot 140\}_{71} = \{5040\}_{71} = 70$; для $l_1 = 3$: $\Delta a_1 = (l_1 \cdot R_1) \bmod 4 = 7455 \bmod 4 = 3$, $k = [7455/140] = 53$, $\gamma = \{53 \cdot 140\}_{71} = \{7420\}_{71} = 36$; $(k+1) = 54$, $\gamma = \{54 \cdot 140\}_{71} = \{7560\}_{71} = 34$;

— для $l_2 = 1$: $\Delta a_2 = (l_2 \cdot R_2) \bmod 5 = 1988 \bmod 5 = 3$, $k = [1988/140] = 14$, $\gamma = \{14 \cdot 140\}_{71} = \{1960\}_{71} = 43$; $(k+1) = 15$, $\gamma = \{15 \cdot 140\}_{71} = \{2100\}_{71} = 41$; для $l_2 = 2$: $\Delta a_2 = (l_2 \cdot R_2) \bmod 5 = 3976 \bmod 5 = 1$, $k = [3976/140] = 28$, $\gamma = \{28 \cdot 140\}_{71} = \{3920\}_{71} = 15$; $(k+1) = 29$, $\gamma = \{29 \cdot 140\}_{71} = \{4060\}_{71} = 13$; для $l_2 = 3$: $\Delta a_2 = (l_2 \cdot R_2) \bmod 5 = 5964 \bmod 5 = 4$, $k = [5964/140] = 42$, $\gamma = \{42 \cdot 140\}_{71} = \{5880\}_{71} = 58$; $(k+1) = 43$, $\gamma = \{43 \cdot 140\}_{71} = \{6020\}_{71} = 56$; для $l_2 = 4$: $\Delta a_2 = (l_2 \cdot R_2) \bmod 5 = 7952 \bmod 5 = 2$, $k = [7952/140] = 56$, $\gamma = \{56 \cdot 140\}_{71} = \{7840\}_{71} = 30$; $(k+1) = 57$, $\gamma = \{57 \cdot 140\}_{71} = \{7980\}_{71} = 28$;

— для $l_3 = 1$: $\Delta a_3 = (l_3 \cdot R_3) \bmod 7 = 1420 \bmod 7 = 6$, $k = [1420/140] = 10$, $\gamma = \{10 \cdot 140\}_{71} = \{1400\}_{71} = 51$; $(k+1) = 11$, $\gamma = \{11 \cdot 140\}_{71} = \{1540\}_{71} = 49$; для $l_3 = 2$: $\Delta a_3 = (l_3 \cdot R_3) \bmod 7 = 2840 \bmod 7 = 5$, $k = [2840/140] = 20$, $\gamma = \{20 \cdot 140\}_{71} = \{2800\}_{71} = 31$; $(k+1) = 21$, $\gamma = \{21 \cdot 140\}_{71} = \{2940\}_{71} = 29$; для $l_3 = 3$: $\Delta a_3 = (l_3 \cdot R_3) \bmod 7 = 4260 \bmod 7 = 4$, $k = [4260/140] = 30$, $\gamma = \{30 \cdot 140\}_{71} = \{4200\}_{71} = 11$; $(k+1) = 31$, $\gamma = \{31 \cdot 140\}_{71} = \{4340\}_{71} = 9$; для $l_3 = 4$: $\Delta a_3 = (l_3 \cdot R_3) \bmod 7 = 5680 \bmod 7 = 3$, $k = [5680/140] = 40$, $\gamma = \{40 \cdot 140\}_{71} = \{5600\}_{71} = 62$; $(k+1) = 41$, $\gamma = \{41 \cdot 140\}_{71} = \{5740\}_{71} = 60$; для $l_3 = 5$: $\Delta a_3 = (l_3 \cdot R_3) \bmod 7 = 7100 \bmod 7 = 2$, $k = [7100/140] = 50$, $\gamma = \{50 \cdot 140\}_{71} = \{7000\}_{71} = 42$; $(k+1) = 51$, $\gamma = \{51 \cdot 140\}_{71} = \{7140\}_{71} = 40$; для $l_3 = 6$: $\Delta a_3 = (l_3 \cdot R_3) \bmod 7 = 8520 \bmod 7 = 1$, $k = [8520/140] = 60$, $\gamma = \{60 \cdot 140\}_{71} = \{8400\}_{71} = 22$; $(k+1) = 61$, $\gamma = \{61 \cdot 140\}_{71} = \{8540\}_{71} = 20$.

Звернемо увагу, що такі розрахунки дійсно можуть бути зробленими заздалегідь, оскільки їхні результати не є залежними від можливих величин чисел, цілісність яких слід перевірити та, в разі потреби, відновити. Тому їх можна представити таблицею наведеного нижче вмісту.

У таблиці у першому рядку (вхід у таблицю) наводиться результат нулізації γ, у другому — номер групи спотворених розрядів *i*, у третьому — величина спотворення Δa_i. Тоді при контролі та поновленні цілісності, одержавши внаслідок операції нулізації лишок по контрольній основі γ, можна зчитати з таблиці номер спотвореної групи *i* та величину спотворення Δa_i. *Таким чином, задачі третього етапу вирішуються, по суті, за одну операцію звернення до таблиці.*

Для **прикладу 1** із таблиці визначаємо, що при $\gamma = 51$ виявлено наявність спотворення у третій групі величиною $\Delta a_3 = 6_{10} = 110_2$, що дійсно мало місце. Отже задачі третього етапу — визначення місця спотворення: номеру *i* спотвореної групи розрядів, а отже, спотвореного лишку $\widetilde{a}_i$, та величина його спотворення $\Delta a_i = (l_i \cdot R_i) \bmod p_i$ є розв'язаними.

Тоді, одержавши місце виникнення *i* та величину спотворення Δa_i, *на четвертому етапі можна також за одну модульну операцію здійснити корегування спотворення* (див. вираз (1)):

$$a_i = (\widetilde{a}_i - \Delta a_i) \bmod p_i .$$

Для попередніх прикладів:

γ	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
i		1								3		3		2
Δa_i		2								4		4		1
γ	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**
i		2					3		3					
Δa_i		1					1		1					
γ	**28**	**29**	**30**	**31**	**32**	**33**	**34**	**35**	**36**	**37**	**38**	**39**	**40**	**41**
i	2	3	2	3			1	1	1	1			3	2
Δa_i	2	5	2	5			3	1	3	1			2	3
γ	**42**	**43**	**44**	**45**	**46**	**47**	**48**	**49**	**50**	**51**	**52**	**53**	**54**	**55**
i	3	1						3		3				
Δa_i	2	3						6		6				
γ	**56**	**57**	**58**	**59**	**60**	**61**	**62**	**63**	**64**	**65**	**66**	**67**	**68**	**69**
i	2		2		3		3							
Δa_i	4		4		3		3							
γ	**70**													
i	1													
Δa_i	2													

$$a_i = (\tilde{a}_3 - \Delta a_3) \bmod p_3 = (001 - 110) \bmod 7 = 10_2 .$$

Неважко упевнитися в правильності виконаного корегування.

Висновок

Запропоновано швидкодіючий алгоритм декодування для коду умовних лишків, який дозволяє на основі процедури нулізації за одну табличну операцію визначити як місце, так і величину спотворення і здійснити, за одну модульну операцію корекцію виявлених спотворень.

1. *Василенко В.С.* Целостность и доступность информационных объектов (монография) / В.С. Василенко, О.Я. Матов. — Saarbrucken, Deutschland: LAMBERT Academic Publishing, 2013. — 95 с. — ISBN 978-3-659-47333-3.

2. *Василенко В.С.* Код условных вычетов (монография) / В.С. Василенко. — Saarbrucken, Deutschland: LAMBERT Academic Publishing, 2013. — 129 с. — ISBN 978-3-659-48203-8.

3. *Матов О.Я.* Теорія інформації та кодування (монографія) / О.Я. Матов, В.С. Василенко // Х.: Експрес-книга, 2014. — 440 с. — ISBN 978-966-02-7096-1.

4. *Матов О.Я.* Контроль та поновлення цілісності на основі алгоритму нулізації в коді умовних лишків / О.Я. Матов, В.С. Василенко, М.Ю. Василенко // Реєстрація, зберігання і оброб. даних. — 2011. — Т. 13, № 3. — С. 72–81.

Надійшла до редакції 09.09.2015