УДК 656.7.085:657.71(045)

КОНТРОЛЬ ТА ПОНОВЛЕННЯ ЦІЛІСНОСТІ ІНФОРМАЦІЙНИХ ОБ'ЄКТІВ ІЗ ЗАСТОСУВАННЯМ КОДУ УМОВНИХ ЛИШКІВ

В. С. Василенко, канд. техн. наук, доц.

Національний авіаційний університет

kszi@ukr.net

Розглянуто умови забезпечення правильного функціонування механізмів контролю та поновлення цілісності інформаційних об'єктів у телекомунікаційних мережах. Зокрема, визначені та обґрунтовані вимоги щодо величин контрольних основ застосованого коду.

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

The conditions to ensure the proper functioning of control mechanisms and update the integrity of information objects in telecommunication networks have been considered. In particular, determined and reasonable requirements for the control variables applied code bases.

Keywords: FEC, code conditional deductions, integrity monitoring, control base, the base code, restoring the integrity of the, distortion.

Постановка проблеми

Теоретичною основою коду умовних лишків (УЛ-коду) є система лишкових класів (СЛК).

У цих системах кодова комбінація (базове кодове слово) розглядається як деяке (реальне в СЛК чи умовне в УЛ-коді) число.

У цих кодах для завадостійкого кодування, як і в інших кодах, вводиться надлишковість у вигляді реального чи умовного лишку від розподілу вихідного числа A на контрольну основу p_k.

Її введення призводить до розширення діапазону представлення до величини

$$R = P \cdot p_k = P \cdot q,$$

де $P = \prod_{i=1}^{n} p_i$ -діапазон представлення неспотворених чисел (робочий діапазон), а p_i (i = 1, 2, …, n) — основи системи числення, обрані для даної системи представлення.

В зазначених умовах неспотвореними числами (цілісність яких ніяким чином не порушена) вважаються такі, величина яких не перевищує визначеного наперед діапазону представлення неспотворених чисел (робочого діапазону).

Спотворені числа $\tilde{A}$ (цілісність яких тим чи іншим чином є порушеною), на відміну від неспотворених, зосереджені за межами робочого діапазону, тобто $\tilde{A} > P$.

Але виявлення як факту наявності спотворення, так і його місця та величини, є можливим лише за умови правильного визначення параметрів застосованого завадостійкого коду, зокрема величин усіх основ системи числення, включаючи і контрольну.

Аналіз досліджень і публікацій

У працях [1–2] досить детально проаналізовано можливості та основні способи (механізми) застосування узагальненого коду умовних лишків (УЛ-коду) в задачах захисту цілісності інформаційних об'єктів телекомунікаційних мереж, а також деякі вимоги щодо величин основ, що утворюють так званий робочий діапазон, та деякі з вимог щодо величин контрольних основ.

Зокрема, що стосується вибору основ, які створюють робочий діапазон, то в праці [1] вимога до них сформульована одна — ці основи повинні бути взаємно простими числами.

Там само показано, що в задачах контролю цілісності інформаційних об'єктів для однозначного визначення наявності викривлень величина контрольної основа має бути більшою ніж величина найбільшої з робочих основ.

Один з варіантів вимог до контрольної основи наведено в праці [2]. Але цей підхід потребує, на погляд автора, більшої деталізації, яка здатна зробити його більш повним та обґрунтованим.

Ціль

Під час використання в завадостійкому кодуванні СЛК у класичному вигляді чи у вигляді коду умовних лишків (УЛ-коді) [1] постає традиційна для задач цього класу проблема розрізнення неспотворених (правильних) кодових комбінацій (чисел, базових кодових слів) від спотворених (неправильних). Виявлення факту наявності чи відсутності порушень цілісності в числі (інформаційному об'єкті), а також визначення місця та величини спотворень — завдання відповідних алгоритмів контролю та поновлення цілісності інформаційних об'єктів. Як уже зазначалося, однією з умов можливості побудови таких

алгоритмів є коректність (правильність) вибору його констант, якими в цьому випадку є надлишкові (контрольні) основи системи числення. Ці основи повинні відповідати певним вимогам.

Мета статті — більш повна та обґрунтована деталізація вимог щодо надлишкових (контрольних) основ у задачах контролю та поновлення цілісності інформаційних об'єктів.

Код умовних лишків у задачах контролю та поновлення цілісності

Що стосується вибору основ, які створюють робочий діапазон, то вимога до них одна — ці основи повинні бути взаємно простими числами. Вимоги ж щодо надлишковості, яка визначається величиною контрольної основи q, витікають із таких міркувань.

При виборі величин контрольної основи в задачах контролю та поновлення цілісності будемо враховувати одержані в працях [1; 2] підходи та результати.

Отже, для виявлення наявності спотворень досить визначити, в якому із діапазонів (робочому чи контрольному) знаходиться число, правильність якого перевіряється.

Покажемо, що при правильному виборі контрольної основи цього достатньо і для визначення місця і величини такого спотворення.

Спотворене число може бути представленим як сума початкового (не спотвореного) числа A та вектора спотворень E: $\tilde{A} = A + E$, де вектор спотворення E в СЛК має лишки, що дорівнюють нулю, за усіма основами, окрім тієї, де є спотворення. Надалі нагадаємо, що вектор спотворення є числом виду $E = 0,0,...,\Delta A,0,0,...,0 = l_i R_i$, чи $E = 0,0,...,(l_i R_i) \bmod p_i,0,0,...,0,$ оскільки тільки числа, які діляться націло на $R_i = R / p_i$, мають у своєму представленні в СЛК такий набір лишків.

В останніх виразах величина $R = \prod_{i=1}^{k=n+1} p_i$ — контрольний (повний) діапазон представлення чисел у СЛК.

На числовій осі величина спотворення $E = l_i R_i$ відображається точкою в деякому піддіапазоні «контрольного» діапазону [(P + 1), R).

Таким чином, процес спотворення початкового числа A відобразиться переміщенням точки A із робочого діапазону [0, P) у деякий піддіапазон із номером k.

Звернемо увагу на те, що в піддіапазон із цим номером k спотворене число ($A' = l_i \cdot R_i + A_1$ чи $A' = l_i \cdot R_i + A_2$) може потрапити (рис. 1) залежно від величини початкового числа (A_1 чи A_2) та взаємного розташування лівих границь піддіапазонів — точок kP та $l_i R_i$ відповідно.

На рис. 1, *а* зображено ситуацію, коли величина початкового числа A_1 перевищує різницю між значеннями $l_i R_i$ та kP, тобто коли $A_1 > (kP - l_i R_i)$.

Ситуація, зображена на рис. 1, *б*, відповідає варіанту, коли величина початкового числа A_2 є меншою ніж різниця між значеннями $l_i R_i$ та $(k+1)P$.

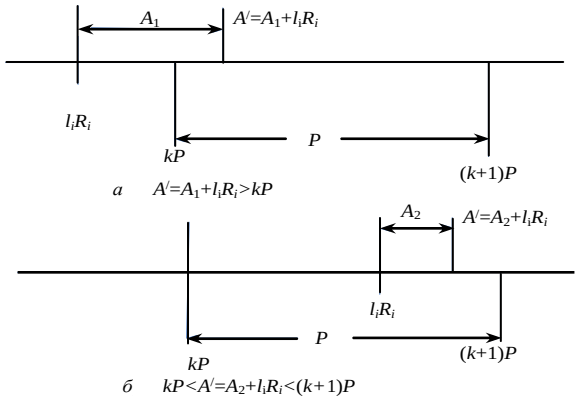

Рис. 1. Ілюстрація розташування спотворених чисел

В обох випадках величина спотворення (чи довжина вектора спотворення) E відповідає умові:

$$(k - 1) \cdot P < E = l_i R_i < (k + 1)P. \qquad (1)$$

Звернемо увагу на те, що такий самий результат може бути одержаний залежно від величини початкового (неспотвореного) числа A при попаданні вектора спотворення E в межі діапазону, ширину якого можна визначити з виразу (1), якщо від правої частини цього рівняння відняти ліву:

$$\Delta E = (k+1) \cdot P - (k - 1)P = 2P.$$

Отже, правильний результат при декодуванні можна одержати лише у випадку, коли можливі спотворення (чи кінці вектора спотворень) є рознесеними на величину, яка є не меншою ніж $\Delta E = 2P$.

Оскільки кількість піддіапазонів P у межах контрольного діапазону $R = Pp_k$ визначається величиною контрольної основи (точніше, дорівнює) p_k, то і відстань між кінцями вектора спотворень залежить від величини p_k.

Цей висновок має бути врахованим при визначенні величини контрольної основи p_k.

Із наведеного витікає, що механізми визначення наявності, місця виникнення та величини спотворення повинні ґрунтуватися на виявленні тим чи іншим шляхом хоча б однієї із таких взаємно пов'язаних величин як i, p_i, та $\Delta\alpha_i$, l_i, R_i, ΔA відповідно.

Таким чином, для ідентифікації спотвореного числа (чи величини спотворення) із номером ос-

нови i слід забезпечити попадання спотворених по різних основах чисел у різні діапазони, що, у свою чергу, є можливим за умови, що відстань між двома довільними діапазонами, в які можуть потрапити спотворені числа, перевищувала б подвійне максимальне значення не спотвореного числа ($2P$). Наприклад, при $l_iR_i > l_jR_j$:

$$l_iR_i > l_jR_j + P, \text{ чи } l_iR_i - l_jR_j > 2P. \qquad (2)$$

Звідси:

$$l_iPp_k / p_i - l_jPp_k / p_j > 2P;$$

$$l_iPp_k / p_i - l_jPp_k / p_j > 2;$$

$$p_k(l_i / p_i - l_j / p_j) > 2;$$

$$p_k > 2/(l_i / p_i - l_j / p_j) = 2p_ip_j /(l_ip_j - l_jp_i).$$

Оскільки шукане значення контрольної основи (мінімально можливе (граничне) значення) повинно перевищувати величину, яка визначається дробовим числом, то для пошуку максимального значення цієї дробової величини слід визначити максимальне значення чисельника та мінімальне значення знаменника.

Максимальне значення чисельника в цьому виразі дорівнює подвійному добутку двох найбільших з основ системи числення $2p_np_{n-1}$, а мінімальне значення знаменника (це цілочисельна величина!):

$$l_ip_j - l_jp_i = 1,$$

оскільки дорівнювати нулю знаменник може лише тоді, коли

$$l_ip_j = l_jp_i,$$

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

Отже, в разі визначення величини та місця спотворення за фактом попадання спотвореного числа до інтервалу з номером l_i чи l_j, вимога до мінімально можливого (граничного) значення величини контрольної основи може бути записаною у вигляді:

$$p_k > 2p_np_{n-1}. \qquad (3)$$

При зворотному співвідношенні між величинами векторів спотворення, тобто при $l_iR_i < l_jR_j$, їх різниця є від'ємною величиною, тобто

$$l_iPq / p_i - l_jPq / p_j < 0,$$

тоді за правилами виконання модульних операцій (у цьому випадку за модулем R) умова (2) набуде вигляду:

$$l_iR_i < l_jR_j + P, \text{ чи } R + l_iR_i - l_jR_j > 2P.$$

Звідси:

$$R + l_iPp_k / p_i - l_jPp_k / p_j > 2P;$$

$$p_k + l_ip_k / p_i - l_jp_k / p_j > 2;$$

$$p_k(1 + l_i / p_i - l_j / p_j) > 2;$$

$$p_k > 2/(1 + l_i / p_i - l_j / p_j) = 2p_ip_j /(p_ip_j + l_ip_j - l_jp_i).$$

$$p_ip_j + l_ip_j - l_jp_i = 1$$

може бути досягнутим при мінімальному значенні другого (позитивного) доданку l_ip_j та максимальному значенні третього (відмінного) — l_jp_i.

Не важко побачити, що $\min(l_ip_j = p_j)$ (при $l_i = 1$), а $\max(l_jp_i) = (p_j - 1)p_i = p_ip_j - p_i$ (при $l_j = p_j - 1$). Тоді $\min\ (p_ip_j + l_ip_j - l_jp_i) = p_i + p_j$, а вираз для визначення шуканого максимального значення p_k набуває вигляду:

$$p_k > 2/(1 + l_i / p_i - l_j / p_j) = 2p_ip_j /(p_i + p_j)$$

і є меншим, ніж у виразі (3).

Отже, оскільки правильний результат декодування потрібен у будь-якій ситуації, мінімально можливі (граничні) значення величини контрольної основи слід розраховувати, виходячи із виразу (3).

Висновок

Таким чином, у статті розглянуто питання изначення величин основ коду умовних лишків для випадків його використання для контролю та поновлення цілісності та запропоновано вирази для розрахунку мінімально можливих (граничних) значень величин контрольної основи.

ЛІТЕРАТУРА

1. *Василенко В. С.* Код умовних лишків у задачах контролю цілісності / В. С. Василенко // Матеріали VI міжнародної науково-практичної конференції "Aknualne problemy nowoczenych nauk — 2010" 07—15 червня 2010. Nowoczesne informacyjne technologie. Fizyka. — Перемишль: "Nauka i studia" 2010. — Т. 28. — С. 34–36.

2. *Василенко В. С.* Вибір величини контрольної основи для коду умовних лишків / В. С. Василенко, О. Я. Матов // Реєстрація, зберігання і обробка даних. — К., 2010. — Т. 12, № 1. — С. 73–78.

Стаття надійшла до редакції 01.07.2011.