УДК 004.057.4(045)

КОД УМОВНИХ ЛИШКІВ В ЗАДАЧАХ КОНТРОЛЮ ЦІЛІСНОСТІ ІНФОРМАЦІЙНИХ ОБ'ЄКТІВ

В. С. Василенко, канд. техн. наук, доц., ***О. В. Дубчак***
Національний авіаційний університет
edubchak@yandex.ru

Розглянуто код умовних лишків як засіб контролю цілісності інформаційних об'єктів, що має високу ймовірність виявлення та виправлення викривлень; запропоновано механізм контролю наявності викривлень в інформаційних об'єктах з використанням процедури нулізації

Ключові слова: цілісність інформації, завадостійке кодування, лишкові класи, процедура нулізації, контрольна ознака.

The code of the conditional rests as the control means of integrity of information objects with high probability of detection and correction of curvatures is considered; the mechanism of the control of distortions presence in information objects with zeroing procedure is offered

Keywords: Integrity of information, noiceproof coding, residual classes, zeroing procedure, control sign.

Постановка проблеми

Наявність завад в інформаційних системах і мережах призводить до великої кількості неправильно виконуваних обчислень, неправильного читання командних і керуючих посилань, зниження ефективності мережі. Труднощі боротьби з завадами полягають у їх безладності, нерегулярності й у структурній подібності з інформаційними сигналами. Тому захист інформації від помилок і шкідливого впливу завад має велике практичне значення і є однією з найважливіших сучасних проблем.

Високі вимоги до цілісності передачі, обробки та зберігання ресурсів інформаційних систем і мереж диктують необхідність застосування відповідних засобів захисту. Цілісність інформаційних даних, як відомо з загальноприйнятої термінології [1], — це властивість, яка полягає в неможливості будь-якої їх модифікації неавторизованим користувачем або процесом. Інакше кажучи, під цілісністю інформації розуміють відсутність у ній будь-яких викривлень — змін, модифікацій, що не були санкціоновані її власником, незалежно від причин або джерел виникнення таких викривлень. Забезпечення цілісності інформаційних об'єктів може включати не тільки виявлення викривлень, а також і відновлення ушкодженої інформації.

Серед методів захисту від помилок найбільше поширення одержало завадостійке кодування, що дає змогу отримати достатньо високі якісні показники роботи інформаційних систем. Його основне призначення — вживання всіх можливих заходів для того, щоб імовірність викривлень інформації була досить малою, незважаючи на наявність завад або збоїв у роботі мережі. Завадостійке кодування припускає розробку коригувальних (завадостійких) кодів, що виявляють і виправляють певного роду помилки, а також побудову й реалізацію пристроїв, що кодують і декодують інформаційні дані.

Фахівцями доведено, що при використанні завадостійкого кодування ймовірність неправильної передачі багаторазово знижується.

Під час аналізу процесу контролю цілісності інформаційні об'єкти та їх окремі елементи — символи розглядаються як числа в деяких системах числення, що використовуються в завадостійкому кодуванні. У завадостійких кодах, крім інформаційних елементів, завжди міститься один або декілька додаткових елементів, що є перевірними й слугують для досягнення більш високої якості передачі даних. Отже, до складу даних, які потребують захисту, уводиться особлива надлишкова інформація — ознака цілісності або контрольна ознака — залежно від термінології, обраної в задачах контролю цілісності або завадостійкого кодування. Цей надлишок — спосіб відображення корисної інформації, процедура формування якого відома і який з дуже високою ймовірністю відповідає інформації, що захищається. Наявність у кодах надлишкової інформації дає можливість виявляти й виправляти (або тільки виявляти) помилки.

При цьому між інформацією, що контролюється, і ознаками цілісності встановлюється функціональний (регулярний) односторонній зв'язок. Його особливість полягає в тому, що процедури розрахунку контрольної ознаки за початковою інформацією, яка захищається, відомі, а процедура зворотного розрахунку початкової інформації за контрольними ознаками найчастіше не існує. Перевірка наявності чи відсутності викривлень зводиться в такому разі до процедур визначення існування вказаного функціонального одностороннього зв'язку між ознаками

цілісності та інформацією, взятою з каналу зв'язку або зчитаною із запам'ятовуючого пристрою (ЗП).

Як відомо, викривлення інформації може носити природний або штучний, навмисний чи випадковий, характер. Особливістю штучних навмисних викривлень є те, що несанкціонований користувач — зловмисник прагне забезпечити, зімітувати наявність функціонального зв'язку між модифікованою їм початковою інформацією й ознаками цілісності. У такому випадку порушнику необхідні знання правил формування ознаки цілісності, щоб визначити відповідну ознаку після проведеної, необхідної для здійснення його мети, модифікації початкової інформації перед наступним етапом її використання — передачею одержувачу або перед записом у ЗП. При успішному формуванні вказаних ознак розкриття наявності модифікації унеможливлюється. Для запобігання невиправних наслідків модифікації інформації її авторизованому власнику необхідно використовувати:

- невідомі потенційним порушникам, тобто *закриті процедури* формування контрольних ознак, що дуже складно забезпечити;
- уведення в загальновідомі процедури формування контрольних ознак *закриті параметри* — ключі перетворення.

В останньому разі, не знаючи закритих параметрів — ключів перетворення, порушник не зуміє зімітувати наявність регулярного зв'язку між модифікованою їм початковою інформацією, взятою або зчитаною із ЗП, і ознаками цілісності.

Мета

Формування контрольних ознак у процедурах з використанням завадостійких кодів — найбільш відомий та відпрацьований з механізмів контролю цілісності. Однак, як правило, ці коди мають загальновідомі алгоритми, їх параметри, наприклад, набори утворюючих поліномів чи матриць кодування, зазвичай, мають вкрай незначну кількість варіантів. Це — суттєвий недолік подібних кодів при їх використанні в задачах контролю цілісності в умовах навмисних впливів.

У статті запропоновано один з підходів, пов'язаний з використанням у задачах контролю цілісності інформаційних об'єктів алгоритмів кодування — декодування завадостійкого коду умовних лишків (ЛУ-коду), які є вільними від зазначеного недоліку.

Етапи контролю наявності викривлень інформаційних об'єктів

Задачі контролю цілісності, тобто наявності викривлень в інформаційних об'єктах унаслідок природних чи штучних впливів, розв'язуються в декілька етапів. Перший з них полягає у формуванні ознак цілісності відповідних інформаційних об'єктів, достовірність яких передбачається контролювати. Залежно від обраної термінології цей процес може визначатися як формування контрольних ознак, виконання операції кодування тощо.

На другому етапі здійснюється власне контроль цілісності. Цей процес може відбуватися декількома шляхами: перевіркою відповідності ознаки цілісності, яка сформована після приймання або зчитування із ЗП, тій, що була сформована до передачі або запису в ЗП; використанням алгоритмів виявлення наявності викривлень — контролю правильності інформаційного об'єкта; декодуванням інформаційних об'єктів на базі теорії завадостійкого кодування.

Як відомо з праці [2], ЛУ-код належить до узагальнених кодів, в яких усі операції із кодування-декодування здійснюються не над окремими двійковими розрядами, а над їх групами — узагальненими символами. В основу ЛУ-коду покладено властивості системи лишкових класів (СЛК), тому в ньому принципово можуть бути використані відомі [3] алгоритми кодування-декодування. Ці алгоритми базуються на тому факті, що будь-яке викривлення в одній з груп розрядів α_i переводить початкове число з робочого діапазону $\left[0, P=\prod_{i=1}^{n} p_i\right)$ у діапазон $[P, R=qP)$, тобто приводить до збільшення початкового числа $A'<P$ на деяку величину $l_i R_i$, де q — контрольна, надлишкова основа значення якої перевищує значення будь-якої з основ, які утворюють робочий діапазон P, тобто $q>p_i,\ \ i=1,2,...,n$ [3]; l_i та R_i — цілі числа $\left(R_i=\frac{R}{p_i}\right)$; R_i — основні константи обраної системи числення.

Якщо припустити, що вихідне число

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

є викривленим по основі p_i і набуває вигляду

$$A'=\alpha_1,\alpha_2,...,\tilde{\alpha}_i,...,\alpha_n,\alpha_\pi,$$

де $\tilde{\alpha}_i=\{\alpha_i+\Delta\alpha_i\}\,(\mathrm{mod}\ p_i)$, то в системі числення в лишкових класах це є еквівалентним такому перетворенню:

$$A=(\alpha_1,\alpha_2,...,\{\alpha_i+\Delta\alpha_i\}\,(\mathrm{mod}\ p_i),...,\alpha_n,\alpha_k)=$$
$$=(\alpha_1,\alpha_2,...,\alpha_i,...,\alpha_n,\alpha_k)+(0,0,...,\Delta\alpha_i,...,0,0).$$

При цьому величина викривлення

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

тобто перевищує величину робочого діапазону P.

Це пов'язано з тим, що тільки число

$$\Delta A = l_i R_i = l_i \frac{R}{p_i}$$

має всі лишки, окрім лишка по основі p_i, такими, що дорівнюють нулю. Але величина $\frac{R}{p_i} > \frac{R}{q}$, якщо $q > p_i$, тоді, навіть при $l_i = 1$, величина викривлення $\Delta A = l_i R_i > P = \frac{R}{q}$.

Отже, сума $A = A' + \Delta A > P$ тобто викривлене число виходить за межі робочого діапазону P і попадає у діапазон $[P, R)$, що може бути певним чином виявленим (рис. 1).

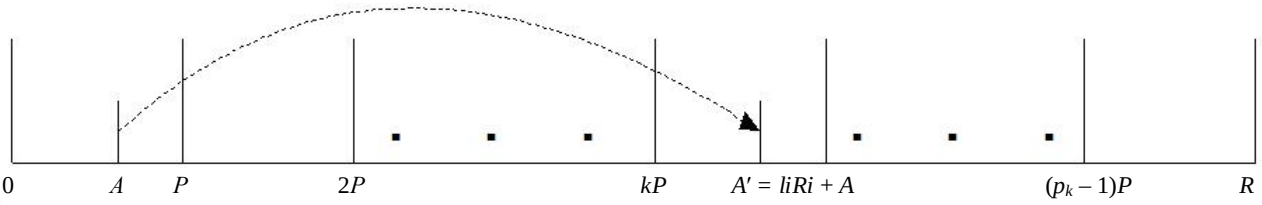

Рис. 1. Вихід викривленого числа A' за межі робочого діапазону $\left[0, P = \prod_{i=1}^{n} p_i\right)$

Таким чином, для виявлення наявності порушень цілісності досить установити факт виходу прийнятого або зчитаного числа за межі робочого діапазону. Запропоновані нижче алгоритми контролю цілісності (кодування-декодування) також використовують цей факт.

Процедура нулізації в задачі контролю цілісності інформаційних об'єктів

Алгоритми з використанням процедури нулізації є одним з механізмів контролю наявності викривлень в інформаційних об'єктах унаслідок природних чи штучних впливів, що використовують властивості завадостійкого кодування, які має СЛК. Тому ці алгоритми передбачають наявність процедури кодування-декодування, яка складається з двох етапів.

На першому етапі, при формуванні ознаки цілісності, контрольної ознаки чи кодуванні, операції алгоритму з використанням процедури нулізації зводяться до того, що за першими n лишками α_i $(i = 1, 2, ..., n)$ числа

$$A = (\alpha_1, \alpha_2, ..., \{\alpha_i + \Delta\alpha_i\} \pmod{p_i}, ..., \alpha_n, \alpha_k)$$

послідовно формуються, так звані *мінімальні* числа вигляду:

$$t_1 = (\alpha_1, \alpha_2^{(1)}, \alpha_3^{(1)}, ..., \alpha_n^{(1)}, \alpha_k^{(1)});$$

$$t_2 = (0, (\alpha_2 - \alpha_2^{(1)}) \pmod{p_2}, \alpha_3^{(2)}, ..., \alpha_n^{(2)}, \alpha_k^{(2)});$$

$$t_3 = (0, 0, (\alpha_3 - \alpha_3^{(1)} - \alpha_3^{(2)}) \times$$

$$\times \pmod{p_3}, \alpha_4^{(3)}, ..., \alpha_n^{(3)}, \alpha_k^{(3)});$$

.....;

$$t_n = (0, 0, , 0, ..., (\alpha_n - \sum_{j=1}^{n-1} \alpha_n^{(j)}) \pmod{p_n}, \alpha_k^{(n)}).$$

Зауважимо, що кожне з таких мінімальних чисел може бути подано у вигляді

$$t_i = v_i \prod_{j=1}^{i-1} p_i.$$

З урахуванням того, що в СЛК

$$t_i \pmod{p_i} = \alpha_i^{i-1} = \{\alpha_i - \sum_{j=i}^{i-1} \alpha_i^{(j)}\} \pmod{p_i} =$$

$$= v_i \prod_{j=1}^{i-1} p_i \pmod{p_i},$$

величину v_i можна визначити як

$$v_i = \left\{\frac{\alpha_i^{i-1}}{\prod_{j=1}^{i-1} p_i}\right\} \pmod{p_i} = \left\{\alpha_i - \frac{\sum_{j=i}^{i-1} \alpha_i^{(j)}}{\prod_{j=1}^{i-1} p_i}\right\} \pmod{p_i}$$

для усіх лишків α_i з номерами $i > 1$, а для першого з лишків α_1 значення $v_1 = 1$.

Підсумок цих чисел $T = \sum_{i=1}^{n} t_i$ має такі дві властивості [2]:

1) лишки цієї суми за всіма основами, окрім p_k, завжди дорівнюють лишкам вихідного числа A;

2) величина цієї суми завжди є меншою, ніж величина робочого діапазону, $T < P$, тобто величина T лежить у межах робочого діапазону і для невикривлених чисел $T = A'$.

Таким чином, процес отримання величини $T = A'$ є *процесом кодування* вихідного числа ЛУ-кодом, при цьому значення A' залежить лише від цього вихідного числа й не залежить від невідомої при кодуванні величини лишку за контрольною основою p_k.

Цей лишок α_k (контрольна ознака, ознака цілісності, що розшукується) дорівнює сумі за мо-

дулем p_k проміжних величин $\alpha_k^{(i)}$ (äå $i = 1, 2, ..., n$), тобто

$$\alpha_k = T(\text{mod } \text{p}_\text{k}) = \left(\sum_{i=1}^{\text{n}} \alpha_k^{(\text{i})} \right) (\text{mod } p_k).$$

На другому етапі здійснюється контроль цілісності або декодування шляхом віднімання від числа A' величини T. Ця дія приводить до того, що отримана різниця

$$\Gamma = A' - T = kP$$

має за всіма основами, окрім контрольної, лишки, які дорівнюють нулю, а за контрольною основою — лишок, величина якого

$$\gamma = (\alpha_k - T \text{ (mod } p_k)) \text{ (mod } p_k) = (kP) \text{ (mod } p_k).$$

Величина Γ при запису в лишкових класах має вид

$$\Gamma = (A' - T) \text{ (mod } p_k) = (0, 0, ...0, ...0, kP \text{ (mod } p_k)),$$

де $k = 0, 1, 2, ..., p_k - 1$.

Звернемо увагу та те, що для невикривлених чисел величина $k = 0$, а отже, $\gamma = 0$, для викривлених — $k \neq 0$ і $\gamma \neq 0$.

Висновок

Отже, в умовах навмисних впливів для контролю цілісності інформаційних об'єктів доцільно використовувати алгоритми кодування-декодування коду умовних лишків; аналіз величини γ, отриманої внаслідок нулізації інформаційного об'єкта, дає змогу з високою ймовірністю встановити факт наявності чи відсутності порушень його цілісності.

ЛІТЕРАТУРА

1. *Нормативний* документ Системи технічного захисту інформації «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу» (НД ТЗІ 1.1-002-99);

2. *Василенко В. С.* Механізми контролю цілісності інформації та її поновлення / В. С. Василенко, М. М. Будько, М. П. Короленко. — К. : НТУ «КПІ» // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 2000. — С. 130—139.

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

Стаття надійшла до редакції 10.03.2011.