УДК 681.3

В.С. Василенко

МОДЕЛІ ПРОЦЕСІВ ЗАХИСТУ ЦІЛІСНОСТІ ІНФОРМАЦІЙНИХ ОБ'ЄКТІВ З ВИКОРИСТАННЯМ КОДУ УМОВНИХ ЛИШКІВ. АЛГОРИТМ НУЛІЗАЦІЇ

Summary The models of processes of defense of integrity of information's holding object with application of code of conditional tailings which provide high probabilities of exposure of violations of integrity and correction of the exposed curvatures are examined.

Вступ

У статті розглядаються моделі процесів захисту цілісності інформаційних об'єктів із застосуванням коду умовних лишків, які забезпечують високі ймовірності виявлення порушень цілісності та виправлення виявлених викривлень. Визначення множини та характеристик можливих атак розглядається як основа їх моделювання з метою оцінки можливих ризиків для власників відповідних інформаційних потоків чи розподілених мереж.

Моделі процесів захисту цілісності інформаційних об'єктів

Відповідно до загальноприйнятої термінології [1] під цілісністю інформації розуміється її властивість, яка полягає у тому, що інформація не може бути модифікована неавторизованим користувачем або процесом. Іншими словами, під цілісністю інформації розуміється відсутність в ній будь-яких викривлень (модифікацій), які не були санкціоновані її власником, не залежно від причин або джерел виникнення таких викривлень.

Для забезпечення контролю цілісності інформаційних об'єктів, включаючи і відновлення зруйнованої інформації застосовується певна множина відповідних моделей, в кожній із яких ці об'єкти та їх окремі символи розглядаються як числа в деяких системах числення, а до складу інформації, яка захищається, найчастіше включають надлишкову 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 з дуже високою ймовірністю відповідає інформації, що захищається.

В таких моделях 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 зворотного розрахунку початкової інформації по контрольних ознаках найчастіше не існує). Контроль цілісності (перевірка наявності чи відсутності викривлень) зводиться при цьому до тих або інших процедур (деякі із них

приведені нижче) перевірки наявності вказаного регулярного (функціонального) одностороннього зв'язку між ознаками цілісності і прийнятою з каналу зв'язку (або зчитаною із ЗП) інформацією.

Характерною особливістю навмисних викривлень є те, що зловмисник прагне забезпечити, зімітувати наявність регулярного (функціонального) зв'язку між модифікованою їм початковою інформацією і ознаками цілісності. З цією метою порушник, використовуючи знання процедур формування контрольних ознак, після необхідної для його цілей модифікації початкової інформації перед передачею одержувачу (перед записом в ЗП) забезпечує формування відповідних ознак. При успішному формуванні вказаних ознак, розкрити наявність модифікації неможливо. Для боротьби з цим власнику (або авторизованому користувачу) необхідно використовувати або закриті (невідомі потенційним порушникам) моделі формування контрольних ознак (що дуже складно забезпечити), або вводити в загальновідомі процедури формування контрольних ознак закриті параметри (ключі перетворення). Не знаючи цих закритих параметрів (ключів перетворення), порушник не зуміє забезпечити, зімітувати наявність регулярного (функціонального) зв'язку між модифікованою їм початковою інформацією, прийнятою (або зчитаної із ЗП), і ознаками цілісності.

Найбільш відомими й відпрацьованими моделями забезпечення цілісності є формування контрольних ознак з використанням завадостійких кодів. Однак коди в таких моделях, як правило мають загальновідомі алгоритми, а їх параметри (це можуть бути, наприклад, набори утворюючих поліномів чи кодуючих матриць) мають вкрай незначну кількість варіантів, що є суттєвим недоліком таких моделей контролю цілісності в умовах навмисних впливів.

В статті пропонується один із підходів, пов'язаний із використанням в моделі контролю цілісності інформаційних об'єктів алгоритмів кодування – декодування завадостійкого коду умовних лишків (ЛУ-коду), які є вільними від зазначеного недоліку.

Код умовних лишків в моделі контролю цілісності. Алгоритм нулізації

Задачі контролю цілісності (наявності викривлень в інформаційних об'єктах внаслідок природних чи штучних впливів) вирішуються принаймні у два етапи. Перший етап полягає в формуванні ознак цілісності (в залежності від прийнятої термінології це може бути формування контрольних ознак, виконання операції кодування,) відповідних інформаційних об'єктів, цілісність яких передбачається контролювати. На другому етапі здійснюється власне контроль цілісності. Цей контроль чи то шляхом перевірки співпадання ознаки цілісності, яка сформована після приймання (зчитування із запам'ятовуючого пристрою) з тією, що була сформована до передачі (запису в запам'ятовуючий пристрій), чи то шляхом використання алгоритмів виявлення наявності викривлень – контролю вірності інформаційного об'єкту, декодування інформаційних об'єктів на базі теорії завадостійкого кодування.

Нагадаємо [2], що ЛУ-код відноситься до узагальнених кодів, в яких усі операції із кодування – декодування здійснюються не над окремими двійковими розрядами, а над їх групами – узагальненими символами. В основі ЛУ-коду лежать властивості системи лишкових класів (СЛК), тому в ньому принципово можуть бути використані відомі [3] алгоритми кодування–декодування. В основі цих алгоритмів лежить той факт, що будь-яке викривлення в одній з груп розрядів α_i переводить початкове число з робочого діапазону [0, P = $\prod_{i=1}^{n} p_i$) в діапазон [P, R = $q \cdot$P), тобто приводить до збільшенню початкового числа $A' < P$ на деяку величину $l_i \cdot R_i$. Тут q – контрольна, надлишкова основа така, що її значення перевищує значення будь-якої із основ, що утворюють робочий діапазон P, тобто $q > p_i$, i = 1, 2, …, n [3]; а l_i і R_i – цілі числа ($R_i = R/p_i$); R_i – основні константи такої системи числення. 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 вид

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

де

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

то це в системі числення в лишкових класах є еквівалентним наступному перетворенню

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

При цьому величина ΔA викривлення

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

перевищує величину робочого діапазону P. Це пов'язано із тим, що тільки число виду

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

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

Відтак, сума $A^{/} = A' + \Delta A > P$, тобто викривлене число (див. рис. 1) вийшло за межі робочого діапазону P і попало в діапазон [P, R), що може бути певним чином виявленим.

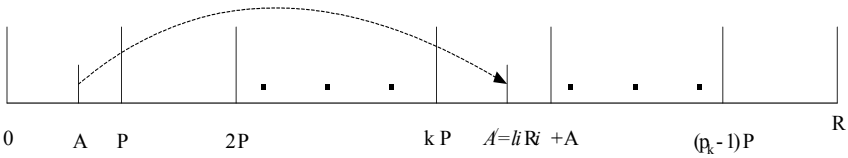

Рис. 1. До виходу викривленого числа за межі робочого діапазону

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

Алгоритми нулізації є одним із механізмів контролю цілісності (наявності викривлень в інформаційних об'єктах внаслідок природних чи штучних впливів), що використовують властивості завадостійкого кодування, які має система лишкових класів. Тому ці алгоритми передбачають наявність процедури кодування – декодування, яка складається із двох етапів.

На першому етапі (при формуванні ознаки цілісності, контрольної ознаки чи кодуванні) операції алгоритму з використанням процедури нулізації зводяться до того, що по першим n лишкам α_i (i = 1, 2, …, n) числа

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

послідовно формуються, так звані мінімальні числа виду:

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

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

$t_3 = (0, 0, (\alpha_3 - \alpha_3^1 - \alpha_3^2) \pmod{p_3}, \alpha_4^{(3)}, \ldots, \alpha_n^{(3)}, \alpha_k^{(3)})$,

……..

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

Звернемо увагу на те, що кожне із таких мінімальних чисел може бути представленим у вигляді

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

З урахуванням того, що в системі лишкових класів

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

величину v_i можна визначити як

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

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

Підсумок цих чисел $T = \sum_{i=1}^{n} t_i$ має наступні дві властивості [2]. По-перше, лишки цієї суми по всім основам, окрім p_k, завжди дорівнюють лишкам

вихідного числа А. По-друге, величина цієї суми завжди є меншою ніж величина робочого діапазону: Т < Р, тобто величина Т лежить в межах робочого діапазону і для не викривлених чисел Т = *А'*.

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

$$\alpha_k = T \pmod{p_k} = \left(\sum_{i=1}^{n} \alpha_k^{(i)}\right) \pmod{p_k}.$$

На другому етапі здійснюється контроль цілісності (чи декодування) шляхом віднімання із числа A' величини Т, що призводить до того, що отримана різниця

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

має по всім основам, окрім контрольної, лишки, що дорівнюють нулю, а по контрольній – лишок, величина якого

$$\gamma = (\alpha_k - (T \bmod p_k)) \pmod{p_k} = (kP) \pmod{p_k}.$$

Величина Γ при запису в лишкових класах має вид

$$\gamma = (A' - T) \pmod{p_k}) = (0, 0, \ldots, 0, \ldots 0, k \cdot P \pmod{p_k}),$$

де k = 0, 1, 2, …, $p_k - 1$.

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

Таким чином, аналіз величини γ, отриманої внаслідок нулізації інформаційного об'єкту, дозволяє установити факт наявності чи відсутності порушень цілісності.

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., Будько М.М., Короленко М.П.* Механізми контролю цілісності інформації та її поновлення. К.: НТУ "КПІ" // Правове, нормативне та метрологічне забезпечення Системи захисту інформації в Україні. 2000, С. 130 – 139;
3. *Акушский И.Я., Юдицкий Д.И.* Машинная арифметика в остаточных классах. // М.: Сов. радио, 1966. – 421 с.

Поступила 15.02.2010р.