**Вячеслав Василенко, Фархад Мікель Огли Гасімов**

**(Київ, Україна)**

**ЗАВАДОСТІЙКИЙ КОД УМОВНИХ ЛИШКІВВ ЗАДАЧАХ  
КОНТРОЛЮ ЦІЛІСНОСТІ**

На сьогоднішній день завдання контролю та поновлення цілісності інформації в сучасних інформаційно-комунікаційних системах та мережах є важливим як ніколи [1-2]. Майже вся інформація в нашому житті перетекла в мережу, і без сумніву є ті, хто хоче цим скористатися вкравши або змінивши потрібну нам інформацію. На сьогоднішній день одним з найвідоміших механізмів поновлення інформації вважають формування хеш-функції на етапі запису чи передачі інформації. Під хеш-функцією розуміється відображення інформації,яка контролюється,в образ фіксованої невеликої довжини за правилами того чи іншого перетворення. Найчастіше використовують механізми блочного контролю цілісності інформації, коли контрольована інформація розподіляється на блоки – базові та узагальнені кодові слова.

Метою статті є використання завадостійкого коду, що має механізм формування контрольних ознак та є стійким щодо несанкціонованої зміни даних, або їх псування.

Задля досягнення такої мети, автори пропонують завадостійкий код, у якому для формування контрольних ознак можна використовувати певну множину невідомих зловмисникам (секретних) констант і щоб цей код міг забезпечити необхідну цілісність інформації від її несанкціонованої зміни(модифікації) або спотворення.

Для цього пропонуються використати можливості теорії лишкових класів по відношенню до інформації, наданої у вигляді кодів, незалежно від систем числення, а також застосування основ системи числення, які можуть бути використані як секретні елементи і забезпечувати за рахунок цього формування на базі теорії лишкових класів контрольних ознак, які є стійкими до розкриття.

За рахунок цього очікується забезпечення цілісності отриманої інформації шляхом виявлення та виправлення спотворень, зменшення ймовірності виникнення завад в результаті впливів природних та штучних завад, а також стійкості цієї інформації до навмисної зміни або спотворення.

Спотворення інформації, тобто її несанкціонована зміна, можливе на будь-якому етапі її перебування у обчислювальних мережах: при зберіганні, передачі або обробці. Наразі в сучасних інформаційних системах розповсюдженим є забезпечення цілісності інформації із застосуванням завадостійких коригуючих кодів. Цей метод знайшов широке застосування в протоколах передачі даних. При цьому при одночасному застосуванні перемежування потрібної глибини забезпечується можливість збільшення довжини інформаційних об’єктів, цілісність яких контролюється. Але більшість завадостійких кодів не мають можливості використовувати закриті (таємні) алгоритми чи їх константи, і тому не виключають можливостей із будь-якої модифікації інформаційних об’єктів. Як код, що має можливість використання секретних параметрів пропонуються узагальнений завадостійкий коригуючий код на базі теорії лишкових класів, так званий код умовних лишків (ЛУ ‒ код).

В системі лишкових класів будь-яке число представляють у вигляді набору лишків від розподілу цього числа на набір взаємно простих чисел, які мають назву основ системи числення – *pi*, де *і =* 1, 2, …, *n, n* – кількість таких основ. Вибір величини *n* здійснюють з умови, яка викладена нижче. Тоді

А = α1, α2, …, αn, (1)

де α = А – [А/*pi*]·*pi*, а позначка [А/*pi*] означає операцію розрахунку цілої частини від дробового числа А/*pi*. При цьому між числом А і його уявленням () існує взаємна однозначна відповідність при умові, що



де *Р* – діапазон представлення або робочий діапазон інформаційних об’єктів (чисел), α*і*– значення *і* ‒ тої групи двійкових розрядів, яка не перевищує величини відповідної основи *pi*.

Основною властивістю системи лишкових класів (СЛК) є те, що вона дозволяє нам ефективніше виявляти і виправляти спотворення в групах двійкових розрядів, тобто в узагальнених символах. Якщо ми введемо ще одну, надлишкову, основу *рк,* то уявлення *А* в розширеному діапазоні *R = P·рк*, у вигляді

А = α1, α2, …, α*n*, α*k*, (2)

де α*ĸ* – лишок по основі *рк*, утворює завадостійкий код. При побудові таких завадостійких кодів слід забезпечити наступні умови: при *pk>pn* будь-яке спотворення в одному з лишків (узагальненому символі) α*і* може бути виявленим, а при *pк*> 2·*pn·pn*­1, де *pn*, *pn*­1 – найбільші із основ, може бути і виправленим.

У такого коду є свої недоліки. По-перше можливі спотворення знаходяться і виправляються (спотворений символ поновлюється) тільки в тому випадку, якщо спотворено лише один з символів α*і*, тобто спотворення повинні бути фіксованими в межах однієї із груп розрядів. Цей недолік є притаманним будь-якому коду і тому усувається всім відомими способами, наприклад, застосуванням декореляції, глибина якої повинна бути не менше ніж 2. По-друге, є також недолік, пов'язаний з необхідністю роботи з числами в системі числення в залишкових класах. Цей недолік достатньо просто усунути в ЛУ–коді, який вводиться таким чином.

Код деякого числа *А* – базове кодове слово (БКС), представляють в будь-якій системі числення, зокрема позиційній, наприклад двійковій. Розбивають цю послідовності певним (у загальному випадку довільним) чином на *n* узагальнених символів, як і для решти узагальнених кодів.

Код кожного *i*−го узагальненого символу розглянемо як *s*− значний розряд б*i*, який може приймати будь-яке з *s* значень від 0 до (*s*− 1), де *s* = 2*b*. Код цього символу вважається лишком деякого *умовного числаА* по основі *pi.* Оскільки величина б*i*, як елемент початкового числа

0 ≤ б*i* ≤ *s*− 1,

а як лишок від ділення *А* на *pi*

0 ≤ б*i* ≤ *pi*,

то для представлення коду будь-якої групи у вигляді лишку по основі *pi* необхідно, щоб виконувалася наступна умова

*pi*>*s* – 1,

інакше в групу із *b* розрядів може бути записаним код α*і* ≥ *pi*, що в лишкових класах не допустимо.

При такому підході будь-які комбінації початкового коду числа *А* ми “вписуємо” в систему числення з основами *pi* (*і* = 1, 2, ...). Якщо ми розширимо систему основ на надлишкову основу *pk*і для одержаного набору умовних лишків б*i*(*і* = 1, 2,...) розрахуємо надлишковий умовний лишок б*k*,то на одержане нами умовне число

А’ = б1, б2, …, бn,б*ĸ* (3)

розповсюджується усі можливості СЛК по виявленню і виправленню спотворень, тобто одержаний код (3) має всі властивості коду (2), але останній код може бути застосованим для будь-якої двійкової послідовності, а не тільки по відношенню до чисел в лишкових класах. Таким чином ми можемо усунути другий недолік коду (2).

ЛУ-код дозволяє нам знаходити і виправляти *b* − розрядні пакети спотворень, згруповані в межах будь-якого з *n* узагальнених символів і потребує при цьому надмірність біля *r* ≈ 2*b* + 1 двійкових розрядів, оскільки

*рk* ≈ 2*рnрn*+1, *r* = [log2*рk*] + 1.

В конкретних випадках ця надмірність може відхилятися в ту або іншу сторону, що залежить також від алгоритмів кодування-декодування.

Оскільки в основі ЛУ-коду лежать властивості СЛК, то в цьому коді ми можемо використати і відомі алгоритми кодування-декодування [3].

Це стає можливим завдяки тому, що спотворення в одній з груп розрядів б*і* переводить початкове число з робочого діапазону [0, P = ) в діапазон [P, R = *pk*·Р), що призводить до збільшенню початкового числа   
*А’ < Р* на деяку величину *li·Ri*. Де *li* і *Ri = R/ pi* – цілі числа. А якщо вихідне число

А = б1, б2, …, б*i*,…,бn, бk

є спотвореним по основі *pi* і прийме вид

 = б1, б2, …, ,… ,бn,бĸ

де

 = {б*i* + Дб*i* } (mod*pi*),

то це буде еквівалентним наступному перетворенню

= (б1, б2, …, б*i*,…,бn, бk) + (0, 0, …, Дб*i*, …,0, 0) =

= (б1, б2, …, {б*i* + Дб*i* } (mod*pi*),…,бn1, бk).



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

При цьому величина спотворення перевищує величину робочого діапазону Р:

ΔА = (0, 0, …, Δα*i*, …,0, 0) > Р,

оскільки тільки число виду

ΔА = *li*·R*i* = *li*·R/*pi*

має всі лишки, окрім лишка по основі *pi*, такими, що дорівнюють нулю. Але   
ΔА = *li*·R*i*> P = R/*pk* тобто, навіть при *li* = 1 величина R/*pi*> R/*pk* по тій причині, що *pk>pi*.

Відтак, якщо сума *= А’ +* ДА > Р, а спотворене число вийшло за межі робочого діапазону Р, попало в діапазон [P, R). Коли ж спотворення відсутні (ДА = 0) прийняте число < Р, знаходиться в робочому діапазоні. Завдяки цьому факту ми можемо здійснювати кодування(формування надлишкових символів) та декодування(виявлення наявності викривлень та можливого їх корегування). Це дає можливість унеможливити несанкціоновану модифікацію інформації, що циркулює в телекомунікаційних мережах.

***Таким чином***, запропоновано завадостійкий код умовних лишків, що дав можливість зробити несанкціоновану модифікацію інформації неможливою. Це призвело до підвищення рівня захисту інформації, що циркулює в телекомунікаційних та інформаційно-комунікаційних системах і мережах.

**Література:**

1. Василенко В.С., Дубчак О.В. Частотна дискретизація як метод підвищення перепускної спроможності каналів передачі даних. Матеріали V міжнародної Науково – практичної конференції “Naukowaprzestrzen Europa – 2009” 07–15 квітня 2009 roku. Informacy jnetechnologie. – Перемишль: “Nauka і studia” 2009. – Т. 17, С. 84–87
2. Ігнатов В.А. Теорія інформації та передачі сигналів. – М.:Сов.радио, 1979. – 280 с.
3. Руднєв Ю.П. Підвищення надійності цифрових пристроїв методом через мірного кодування. – М.: “Енергія”, 1974. – 290 с.