УДК 004.056.2

О. Я. Матов[1], В. С. Василенко[2], М. Ю. 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

Захист цілісності інформації при застосуванні коду «зважених груп»

Для задач забезпечення контролю цілісності інформаційних об'єктів на прикладі коду «зважених груп» розглянуто загальні підходи щодо побудови завадостійких кодів.

Ключові слова: *вагові коефіцієнти, завадостійкість, контроль за модулем, надлишковість.*

Вступ

Система технічного захисту інформації забезпечує цілісність інформації, якщо вона зберігається, передається або обробляється, достовірною, повною і захищеною від ненавмисних і навмисних спотворень. Одним із основних способів забезпечення цілісності інформації в автоматизованих системах є застосування засобів контролю цілісності програмних засобів та оброблюваної інформації, включаючи в деяких випадках і її відновлення. Найчастіше для захисту від природних впливів такі засоби контролю цілісності будуються на основі застосування тих чи інших завадостійких кодів. До найбільш уживаних найчастіше відносять [1, 2] коди з контролем на парність (непарність), Хеммінга, циклічні, Ріда-Соломона та ін.

Нагадаємо, що більшість широко вживаних кодів, призначено для виявлення спотворень *в одному чи декількох символах* або виявлення і виправлення спотворень *в одному із символів* кожного з базових кодових слів, які утворюють відповідний інформаційний об'єкт. Нагадаємо також, що основними з характеристик будь-якого завадостійкого коду є надлишковість, яка потрібна для забезпечення його функцій, та ймовірність виявлення (чи пропуску) спотворень. Надлишковість визначається довжиною контрольної частини, яка не повинна бути занадто великою, оскільки вона впливає на загальний обсяг інформації та, відповідно, на швидкість її передачі. В той же час, надлишковість, залежно від потреб, має бути достатньою для виявлення, чи виявлення та виправлення заданого класу спотворень та для забезпечення також потрібної імовірності виявлення (чи пропуску) спотво-

рень. Отже, застосована надлишковість повинна дозволяти будувати та застосовувати ефективні алгоритми виявлення та корегування спотворень.

У статті, як завадостійкий, розглядається код, названий у роботах [3, 4] кодом «зважених груп», визначено його можливості щодо виявлення чи виявлення та усунення класів спотворень, прийнятих при побудові найпоширеніших кодів. У статті розглядається потрібна для цього надлишковість, показується також, що такий код є основою (генератором) для побудови як що не всіх, то, принаймні, більшості із відомих завадостійких кодів.

Код «зважених груп» у задачах виявлення спотворень

Цей код, як і багато інших, є *n*-символьною послідовністю, яка складається із *m* суто інформаційних та k надлишкових символів, тобто $n = m + k$. Код дозволяє виявляти чи виявляти та усувати спотворення в цих *n*-символьних блоках інформаційних об'єктів [3, 4]. Для спрощення, в межах цих міркувань, будемо вважати, що при формуванні ознак цілісності відповідні контрольні символи набувають номери від 1 до k. Тоді інформаційні символи можуть бути записаними як:

$$A = a_{k+1}, a_{k+2}, ..., a_{k+i}, ..., a_n .$$

Величина ознаки цілісності таких кодів *R* (*k* контрольних символів) визначає потрібну надлишковість і, в загальному випадку, може розраховуватися як

$$R = \sum_{i=k+1}^{n} a_i \cdot c_i . \qquad (1)$$

У виразі (1): a_i — значення *i*-го, у загальному випадку багаторозрядного, узагальненого символу (УС) інформаційного об'єкта; c_i — їхні вагові коефіцієнти.

Цей *k*-символьний код приформовується до початкової послідовності і передається разом із нею, утворюючи *n*-символьний ($n = m + k$) код повідомлення (базового кодового слова).

Нехай розрядність УС є однаковою і дорівнює, наприклад, *b* двійковим символам. Тоді максимальне чисельне значення символів дорівнює $2^b - 1 = p - 1$. Величину $p = 2^b$ іноді зручно вважати основою деякої системи числення.

Оскільки при усіх операціях щодо контролю чи контролю та поновлення цілісності інформаційних об'єктів для формування контрольних ознак використовуються вагові коефіцієнти певних груп символів, то такий код, природно, одержав назву [3, 4] коду «зважених груп». Покажемо можливості цих кодів щодо виявлення та виправлення спотворень.

Загальний алгоритм виявлення спотворень включає наступні кроки. *На першому кроці* при контролі цілісності *n*-символьного об'єкта, котрий контролюється, за виразом (1) розраховують нову контрольну ознаку

$$\tilde{R} = \sum_{i=k+1}^{n} a_i' \cdot c_i \,, \tag{2}$$

де $\tilde{R}$ — значення контрольної ознаки, інформаційного об'єкта, котрий контролюється, a_i' — значення його *i*-го, можливо спотвореного, символу. Оскільки спотворення, за визначенням, є можливим лише в одному із символів (нехай це буде символ із номером *j*), то всі прийняті символи a_i', окрім того, що є спотвореним $(\tilde{a}_j)$, дорівнюють переданим $a_i' = a_i$ для всіх $i \neq j$. Тоді вираз (2), можна записати у вигляді:

$$\tilde{R} = \sum_{i=k+1=}^{j-1} a_i + \tilde{a}_j \cdot c_j + \sum_{i\ \ j+1}^{n} a_i \cdot c_i \,.$$

Другим кроком є порівняння початкового (*R*) та знов обчисленого значень контрольної ознаки ($\tilde{R}$), наприклад, шляхом знаходження різниці цих величин:

$$\Delta R = \tilde{R} - R = \sum_{i=k+1=}^{j-1} a_i + \tilde{a}_j \cdot c_j + \sum_{i\ \ j+1=}^{n} a_i \cdot c_i - \sum_{i\ \ k+1}^{n} a_i \cdot c_i =$$
$$= (\tilde{a}_j - a_j) \cdot c_j = \Delta a_j \cdot c_j,$$

звідки

$$\Delta R = \Delta a_j \cdot c_j. \tag{3}$$

Третім кроком є аналіз величини ΔR. Зрозуміло, що в разі відсутності спотворень величина $\Delta a_j = 0$ і, відповідно, $\Delta R = 0$. Інакше, при $\Delta R \neq 0$ та, відповідно, $\Delta a_j \neq 0$ слід *констатувати факт наявності спотворень*. Тобто, величина ΔR є індикатором спотворень.

Отже, з аналізу виразу (3) витікає, що при застосуванні коду «зважених груп» є можливість виявляти наявність спотворень. Причому можна стверджувати, що ця можливість не залежить від величин вагових коефіцієнтів c_j, тобто існує навіть при однакових вагових коефіцієнтах, наприклад, при $c_j = 1$.

Код «зважених груп» у задачах корегування спотворень. Визначення вагових коефіцієнтів

Зрозуміло, що процедуру корегування слід здійснювати лише після установлення факту наявності спотворень, тобто коли індикатор спотворення — величина ΔR є відмінною від нуля $\Delta R \neq 0$.

Для корегування спотворень необхідно знати як місце спотворення (номер спотвореного символу), так і його величину.

Отже, *четвертим кроком* процедури виявлення та корегування спотворень є визначення місця спотворення. Це, принципово, можна зробити із виразу (3), коли спотворення — несанкціонована зміна величини УС визначається як

$$\Delta a_j = \Delta R / c_j. \tag{4}$$

Зрозуміло, що одержану з (4) величину Δa_j можна вважати величиною спотворення лише в разі, коли ця величина є цілою та не перевищує максимально можливого значення символу, тобто не перевищує величини 2^b. Тоді для визначення місця спотворень процедуру (4) необхідно застосовувати по відношенню до усіх інформаційних символів коду, тобто для всіх можливих значень $j = k, k+1,..., n-1$, принаймні доти, поки з виразу (4) не буде одержаним ціле значення величини Δa_j, таке, що $\Delta a_j < p = 2^b$. У разі, коли при деякому значенні c_j одержана величина Δa_j задовольняє цим умовам, є підстави стверджувати, що *місцем спотворення є узагальнений символ* $\tilde{a}_j$ *із номером* j та величиною спотворення — Δa_j. У разі ж, коли при жодному значенні c_j ($j = k, k+1,..., n-1$) ціле значення Δa_j не одержано, слід зробити висновок про відсутність спотворень інформаційних символів (наявність спотворень у надлишкових символах, як правило, ігнорується).

Останнє твердження є справедливим тільки тоді, коли існує можливість розрізняти величину Δa_j від значень інших можливих спотворень, визначених із (4), для будь-яких вагових коефіцієнтів інформаційних символів із номерами ($i = k, k+1,..., n-1$) для усіх $i \neq j$.

При цьому слід врахувати, що спотворення може призвести до неоднозначної зміни початкового значення узагальненого символу — як у бік збільшення, так і у бік зменшення чисельного значення УС, тобто

$$\tilde{a}_j = a_j \pm \Delta a_j,$$

де a_j — чисельне значення вихідного (неспотвореного) УС; $\tilde{a}_j$ — чисельне значення спотвореного УС; Δa_j — величина спотворення. Не знаючи напрямку зміни спотвореного УС, неможливо здійснити корегування, навіть при відомих місці та величині спотворення.

Для уникнення цієї неоднозначності, а отже і для спрощення подальших операцій з виявлення та корегування спотворень, доцільним є представлення процесу спотворення у вигляді додавання величини спотворення до неспотвореного значення УС за деяким модулем. Оскільки результат такої операції повинен знаходитись у межах від нуля до $(2^b - 1)$, то як значення модуля слід використовувати

лише величину $p = 2^b$. Тоді спотворене значення відповідного символу можна представити як

$$\tilde{a}_j = (a_j + \Delta a_j) \bmod 2^b,$$

та, відповідно:

$$a_j = (\tilde{a}_j - \Delta a_j) \bmod 2^b. \quad (5)$$

Із виразів (2)–(5) зрозуміло, що для однозначного виявлення місця спотворення на величину вагових коефіцієнтів інформаційних символів c_i і, відповідно, на розрядність контрольної ознаки, слід наложити певні обмеження.

Розглянемо спочатку обмеження на величину вагових коефіцієнтів інформаційних символів. *Перше з обмежень* витікає із уже сформульованої, необхідної для корегування вимоги розрізняння спотворень у різних символах, тобто забезпечення умови $\Delta a_j \cdot c_j \neq \Delta a_i \cdot c_j$. Неважко зрозуміти, що для цього за умови, що величини спотворення Δa_i чи Δa_j не перевищують максимального значення символів $2^b - 1$, значення вагових коефіцієнтів інформаційних символів повинні бути, *по-перше*, більшими, ніж основа *p*, тобто

$$c_i > 2^b. \quad (6)$$

Отже, вагові коефіцієнти повинні бути не менше ніж двохсимвольними для всіх $i = k+1, k+2, ..., n$. *По-друге*, оскільки значення спотворень у різних символах можуть бути однаковими, тобто $\Delta a_j = \Delta a_i$, то для їхнього розрізняння слід забезпечити умову $c_j \neq c_i$.

У найпростішому випадку бінарних символів ($b = 1$), коли можливі спотворення у будь-яких символах можуть приймати лише одне значення $\Delta a_i = 1$, вираз (6) залишається єдиним обмеженням. Дійсно, у цьому разі величина синдрому спотворення (3) стає такою, що дорівнює величині вагового коефіцієнта спотвореного символу: $\Delta R = \Delta a_j \cdot c_j = c_j$, а отже при різних значеннях c_j місце спотворення визначається однозначно.

У разі ж застосування коду щодо узагальнених символів із розрядністю, що перевищує одиницю ($b > 1$), останню нерівність слід розглядати як необхідну, але недостатню умову розрізняння спотворень. Останнє твердження можна проілюструвати наступним прикладом.

Нехай контролюється інформаційний об'єкт, що складається із двох розрядних ($b = 2$) символів, а серед множини вагових коефіцієнтів є $c_j = 6$ та $c_i = 9$, які задовольняють умові (6). Нехай також унаслідок контролю одержано значення

$\Delta R = 18 \neq 0$. Тоді спроба виявлення величини спотворення, виходячи із виразу (6) дасть $\Delta a_j = 18 / 6 = 3$, та $\Delta a_i = 18/9 = 2$. Оскільки кожне із них не перевищує значення $p = 2^b = 4$, ці обидва значення спотворень є допустимими.

Неважко дійти висновку, що для уникнення наведеної в прикладі ситуації, як необхідну і достатню умову слід розглядати вимогу, щоби **вагові коефіцієнти були взаємно простими числами, такими що задовольняють нерівності (6), тобто перевищують максимальне чисельне значення символів** 2^b. *Це є другим обмеженням щодо величин вагових коефіцієнтів.*

Звернемо увагу на те, що, для виконання своїх функцій і контрольні ознаки, і синдроми спотворень повинні бути числами у деякій позиційній системі числення. Оскільки розрядність символів контрольної ознаки, за визначенням, дорівнює b, то основою такої системи числення є величина $p = 2^b$. При цьому кожен символ цієї системи числення має свій ваговий коефіцієнт, величина яких, як відомо, має значення p^j ($j = 0, 1, 2, \ldots, k-1$).

Оскільки розрізняти спотворення слід у всіх символах інформаційного об'єкта, включаючи надлишкові, то, зрозуміло, вагові коефіцієнти інформаційних символів не повинні дорівнювати ваговим коефіцієнтам надлишкових символів, тобто величинам p^i:

$$c_i \neq p^j \ (j = 0, 1, 2, \ldots, k-1;\ i = k, k+1, \ldots, n-1). \qquad (7)$$

Це є третім обмеженням щодо величин вагових коефіцієнтів.

Тільки при вагових коефіцієнтах інформаційних і надлишкових символів, які задовольняють наведеним обмеженням, лише для одного із узагальнених символів величина Δa_j буде і цілим числом, і не перевищить величину $p = 2^b$. Відносно до цього символу і слід робити висновок щодо виявлення місця і величини спотворення.

Відмітимо, що при такому виборі вагових коефіцієнтів інформаційних символів значення величини ΔR є не тільки *індикатором спотворень* (при $\Delta R = 0$ спотворень немає, та при $\Delta R \neq 0$ спотворення є), але й *синдромом спотворень*, оскільки є покажчиком символу, де є спотворення.

Отже, за рахунок вибору вагових коефіцієнтів, слід добитися таких результатів, коли при виконанні операції (4) у разі ділення не на c_j, а на будь-який інший ваговий коефіцієнт $c_i \neq c_j$ ($i = k, k+1, \ldots, n-1$) результат розподілу стає дробовим числом. У цьому разі, оскільки дійсне значення синдрому спотворення дорівнює $\Delta R = a_j \cdot c_j$, то після ділення на $c_i \neq c_j$ вираз (4) набуде невірного значення (що нижче умовно показано знаком тильди над шуканою величиною Δa_i):

$$\Delta \tilde{a}_i = \Delta R / c_i = \Delta a_j \cdot c_j / c_i,$$

яке у силу того, що вагові коефіцієнти інформаційних символів є простими числами, буде дробовим, що не припустимо щодо величин можливих спотворень.

Зрозуміло, що значення результату розподілу (у сенсі — дробове чи ціле) залежить лише від співвідношення всіх можливих пар вагових коефіцієнтів і може бути гарантовано дробовим, як уже зазначалося, лише тоді, коли ***вагові коефіцієнти інформаційних символів є взаємно простими числами***.

Отже, наявність дробового значення результату ділення свідчить про відсутність спотворення в цій групі і необхідність продовження пошуку.

Наявність же за виразом (4) *цілого значення результату ділення* синдрому спотворень ΔR на ваговий коефіцієнт c_j, яке не перевищує величину $p = 2^b$, свідчить про *виявлення місця спотворення*, тобто номеру спотвореного символу $\tilde{a}_j$, а також — *про правильне визначення величини спотворення* Δa_j.

Тоді *п'ятим кроком* процедури є власне корегування спотворень шляхом виконання операції (див. вираз (5)):

$$a_j = (\tilde{a}_j - \Delta a_j) \bmod 2^b .$$

Таким чином, правильний вибір вагових коефіцієнтів інформаційних символів дозволяє здійснити як виявлення можливих спотворень, так і їхнього корегування.

Визначення значності та надлишковості коду «зважених груп»

Нагадаємо, що під значністю завадостійкого коду розуміють загальну кількість символів коду *n*, яка дорівнює сумі кількості інформаційних *m* та надлишкових *k* символів:

$$n = m + k.$$

Отже надлишковість складається із визначеної, чи припустимої довжини інформаційної частини повідомлення *m* та потрібної, при цьому, надлишковості *k*. Слід враховувати, що в останньому виразі доданки *m* та *k* найчастіше мають той чи інший функціональний зв'язок. Найпростіший із таких зв'язків полягає у тому, що збільшення кількості інформаційних *m* призводить до збільшення кількості надлишкових символів *k*.

Тому для початку будемо вважати, що *первинними параметрами коду*, заданими для оцінок значності та надлишковості коду «зважених груп» якимось обставинами, є кількість інформаційних символів *m* із розрядністю *b* двійкових символів кожен.

Це одразу визначає кількість взаємно простих вагових коефіцієнтів інформаційних символів c_i (i = 1, 2, …, m), величина яких вибирається з умов (вирази (6) та (7)) $c_i > 2^b$, $c_i \neq p^j$ (j = 0, 1, 2, …, $k-1$; $i = k, k+1, ..., n-1$), а також розрядність цих вагових коефіцієнтів. Зрозуміло, що при визначенні величин вагових коефіцієнтів їхня розрядність повинна бути обраною не меншою ніж ($b+1$).

Ці первинні параметри дозволяють здійснити визначення потрібної надлишковості, яку необхідно ввести для забезпечення виявлення чи виявлення та усунення усієї множини можливих спотворень. Як зрозуміло, ця надлишковість забезпечується кількістю та величиною символів для відображення контрольної ознаки R (вираз (1)) та синдрому спотворень ΔR (вираз (3)). Виходячи з викладеного, для вибору потрібних значності та надлишковості коду «зважених груп» необхідно наступне.

1. Виходячи з наявної кількості інформаційних символів *m*, слід здійснити вибір такої ж кількості їхніх вагових коефіцієнтів, визначити їхні величини та розрядність. Позначимо максимальну розрядність вибраних вагових коефіцієнтів інформаційних символів через b_k. Наприклад, якщо кількість інформаційних символів m дозволяє обмежитися кількістю вагових коефіцієнтів із діапазону $2^b \le c_i < 2^{2b}$, то максимальне значення добутку $a_i \cdot c_i$ стає трисимвольним. У разі потреби слід іти на збільшення кількості вагових коефіцієнтів до потрібної, а отже, на збільшення розрядності як вибраних вагових коефіцієнтів, так і потрібної розрядності добутку $a_i \cdot c_i$.

2. Після вибору кількості та, відповідно, розрядності вагових коефіцієнтів b_k можна визначитись із кількістю символів контрольної ознаки, тобто з величиною *k*. Наприклад, у разі, вірності попереднього припущення, коли максимальне значення $a_i \cdot c_i$ є трисимвольним, контрольна ознака R у виразі (1), як сума трисимвольних доданків, має бути, як мінімум, чотирисимвольною, тобто *k* =4.

3. Визначити значність коду $n = m + k$.

Зрозуміло, що використання як вагових коефіцієнтів лише простих чисел зменшує їхню можливу кількість, особливо при малій розрядності груп b, але це зменшення при значних розрядностях груп не є суттєвим обмеженням. Наприклад, при використанні символів байтової довжини *b* = 8 (1 байт) кількість простих чисел, які можна використати як вагові коефіцієнти, навіть у суттєво обмеженому діапазоні ($8 < b < 6000$), взятому з довідника [5], налічує більше ніж 700. Тоді, наприклад, для протоколів IP та TCP, можна забезпечити передачу дейтаграм із максимальним розміром 65536 байтів із виявленням і виправленням спотворень при глибині декореляції (перемежування) менше ніж 93. Можна очікувати, що вибір простих чисел із ширшого діапазону ($8 < b < 65536$) дозволить суттєво зменшити цю глибину перемежування (приблизно до 9–10).

Загальні можливості та шляхи зменшення надлишковості коду «зважених груп»

У вже згаданих роботах [2, 3] розглядалася найбільш спрощена задача забезпечення цілісності інформаційних об'єктів при мінімальній розрядності символів a_i: *b* = 1 (бінарні символи). На відміну від цих підходів, будемо розглядати символи a_i як узагальнені з розрядністю, яка є відмінною від одиниці, тобто при $b \ne 1$. Не важко усвідомити, що кількість таких символів дорівнює величині m/b. Окрім того, будемо відрізняти вимоги щодо надлишковості при контролі цілісності (виявлення лише факту наявності спотворень) та вимоги щодо надлишковості

при корегуванні уже виявлених спотворень (виявлення місця та величини спотворень).

Отже поставимо задачу мінімізації чи зменшення потрібної надлишковості та уточнення вимог до вагових коефіцієнтів.

Першим шляхом зменшення потрібної надлишковості, який є найбільш зрозумілим, є застосування вагових коефіцієнтів, які задовольняють умові (6) та одночасно є найменшими. Цій умові задовольняють, наприклад, вагові коефіцієнти, які вибираються з умови

$$2^b < c_i \le 2^{2b},$$

тобто є такими, що потребують для свого відображення не більше двох узагальнених символів.

Це є можливим, коли кількість таких чисел є не меншою ніж кількість символів інформаційної частини повідомлення, що є не завжди можливим. Одразу відмітимо можливість іноді полегшити таке обмеження за рахунок вибору, при потребі, потрібної глибини перемежування (декореляції) λ такої, що $M \le \lambda \cdot 2^b$, де M — загальна довжина інформаційного блоку, який підлягає кодуванню кодом «зважених груп».

Аналіз особливостей побудови деяких інших завадостійких кодів підказує наявність *другого шляху зменшення потрібної надлишковості*, який застосовано при побудові таких кодів. Цим шляхом при обчисленні контрольної ознаки є *застосування* операцій *за певним модулем*. При цьому вираз (1) для розрахунку контрольної ознаки набуває вигляду:

$$R = \sum_{i=1}^{m/b} a_i \cdot c_i \pmod{P}, \tag{8}$$

де P — значення обраного модуля.

Із аналізу виразу (8), витікає, що спроби подальшого зменшення надлишковості можна очікувати за рахунок зменшення модуля P, зміни величин вагових коефіцієнтів c_i, розрядності груп (b) та, як показує досвід застосування інших кодів, — способу додавання (арифметичне, порозрядне по модулю 2 т.п.).

Отже, як розвиток *другого шляху* розглянемо можливість зменшення потрібної надлишковості за рахунок застосування такого мінімально можливого модуля, при якому одержані результати є ще правильними у сенсі вимог щодо застосованого коду. Зрозуміло, що обмеженням такого зменшення є таке значення модуля P, а отже і надлишковості, яке дозволяє, залежно від призначення коду, забезпечити безпомилкове визначення чи наявності, чи, також, місця та величини можливого спотворення в інформаційному об’єкті.

При аналізі цього шляху врахуємо, що при декодуванні здійснюється обрахування різниці знов і попередньо обрахованих контрольних ознак із застосуванням операцій за mod P:

$$\Delta R = \left[\sum_{i=1}^{m/b} a_i' \cdot c_i - \sum_{i=1}^{m/b} a_i \cdot c_i \right] (\mathrm{mod}\, P),$$

унаслідок чого одержується синдром спотворення:

$$\Delta R = \Delta a_j \cdot c_j \,(\mathrm{mod}\, P). \qquad (9)$$

Звідси, при відмінному від нуля індикаторі спотворень $\Delta R \neq 0$ робиться висновок щодо наявності спотворень, що уже *є достатнім в операціях з можливістю визначення лише факту наявності спотворення.* Також, як і при аналізі виразу (3) робимо висновок, що ця можливість не залежить від величин вагових коефіцієнтів c_j, тобто існує й при однакових вагових коефіцієнтах, наприклад, при $c_j = 1$, оскільки при цьому маємо $\Delta R = \Delta a_j \,(\mathrm{mod}\, P)$.

Після наведених шляхів зменшення можливої надлишковості та одержаних загальних для кодування та декодування виразів (7), (9) можна деталізувати вимоги щодо надлишковості при контролі цілісності (виявленні лише факту наявності спотворень) та вимоги щодо надлишковості при корегуванні вже виявлених спотворень (виявленні місця та величини спотворень).

Спочатку розглянемо вимоги щодо надлишковості, ***потрібної лише для виявлення факту наявності спотворень***. Нагадаємо, що раніше при аналізі виразу (3) уже зроблено наголос на можливість коду «зважених груп» виявляти наявність спотворень, яка не залежить від величин вагових коефіцієнтів c_j. Тобто така можливість існує навіть при однакових вагових коефіцієнтах, наприклад, при $c_j = 1$. Тоді з виразу (9) для $c_j = 1$ маємо, що синдром спотворень дорівнює величині спотворень

$$\Delta R = \Delta a_j \,(\mathrm{mod}\, P).$$

Подальші кроки щодо вибору величини контрольного модуля P при контролі цілісності — в операціях з можливістю визначення лише факту наявності спотворення залежать від деяких додаткових обставин.

Першою з таких обставин є потрібна кратність спотворень Δa_j, наявність яких потрібно виявляти при застосуванні цього коду. Принципово на такий код можна покласти завдання виявлення спотворень у певній кількості розташованих поспіль узагальнених символах (без визначення місця спотворення) із загальною довжиною пакету спотворень $b \cdot l$ $(l = 1,2,...)$ біт, де b, як і раніше, розрядність одного узагальненого символу, l — кількість розташованих поспіль узагальнених символів. Із цією метою необхідно обирати відповідну величину контрольного модуля. Вочевидь ця величина повинна бути такою, що $P \geq 2^{b \cdot l}$, тобто не меншою ніж максимальне число, яке може бути записаним у цих l узагальнених символах.

За необхідності виявлення спотворень кратності меншої ніж один узагальнений символ величину контрольного модуля можна вибирати такою, що не пере-

вищує основи уже згаданої системи числення ($P = 2^b$). Це пов'язано з тим, що чисельне значення індикатора спотворень (без урахування обчислень за модулем P) дорівнює величині спотворень, яка, у свою чергу, є завжди меншою ніж величина 2^b, тобто $\Delta a_j \le 2^b$. Звідси витікає, що при контролі цілісності величину контрольного модуля можна зменшувати від $P = 2^b$ аж до $P = 2$ (у останньому випадку маємо варіант відомого коду з контролем на парність).

Остання можливість обмежується *другою з обставиною*, якою є потрібні ймовірність невиявлення чи ймовірність виявлення спотворень. Як відомо, перша ймовірність визначається із відомого співвідношення $P_{нв} = 1/2^{bk} \approx 1/P$, а друга — зі співвідношення $P_в \approx 1 - P_{нв} = 1 - 1/P$. Зрозуміло, що у цьому випадку мінімально допустима надлишковість повинна бути не меншою ніж $b \cdot k = -\log_2 P_{нв}$ двійкових символів чи k символів розрядністю b.

Отже, залежно від допустимих чи потрібних значень імовірностей пропуску чи виявлення спотворень, які є функціями від застосованої надлишковості, у разі необхідності виявлення спотворень у одному із символів, величину контрольного модуля слід вибирати такою, що не перевищує основи $P \le p = 2^b$.

За наявності спотворень **в операціях з визначенням їхнього місця та величини** з урахуванням особливостей виконання операції ділення по модулю величина можливого спотворення:

$$\Delta a_j = \Delta R / c_j (\mathrm{mod}\, P) = (\Delta R + d \cdot P) / c_j . \qquad (10)$$

У цьому виразі значення d слід збільшувати від $d = 0$ доти, поки не буде одержаним ціле значення шуканої величини Δa_j. Звернемо увагу на те, що найпростіше вираз (10) реалізується при $d = 0$, тобто коли

$$\Delta a_j = \Delta R / c_j ,$$

чи коли операція стає не модульною. Останнє є можливим у разі, коли величина модуля P є не меншою ніж значення ΔR, що, як витікає із (3), є можливим при значенні модуля, яке є не меншим добутку $\Delta a_j \cdot c_j$:

$$P \ge \Delta a_j \cdot c_j . \qquad (11)$$

Отже при визначених максимальних значеннях величин можливих спотворень $(2^b - 1)$ та вагових коефіцієнтів визначення значення модуля P є тривіальною задачею. ***Наприклад***, для забезпечення визначення правильного значення величини Δa_j при односимвольних a_j та двосимвольних c_j потрібним є трисимвольне значення величини ΔR. Отже, **як мінімальне значення модуля *P* можна використати величину $P = 2^{3b}$**, і тоді значення добутку, обчислене за модулем, і значення чисто арифметичного добутку співпадають:

$$\Delta R = \Delta a_j \cdot c_j \pmod{P} = \Delta a_j \cdot c_j ,$$

тобто операція визначення величини та місця спотворення стає не модульною, що значно спрощує її реалізацію.

Висновки

Одержані результати дозволяють стверджувати, що розглянутий у статті код «зважених груп» забезпечує вирішення задач як контролю, так і контролю та поновлення цілісності інформаційних об'єктів. Мінімальне значення потрібної надлишковості є близьким до оптимальної надлишковості кращих з відомих кодів.

1. *Чипига А.Ф.* Информационная безопасность автоматизированных систем: учеб. пособ. для студентов вузов / А.Ф. Чипига. — М.: Гелиос АРВ. — 2010. — 336 с.

2. *Матов О.Я.* Основы теории передачи дискретной информации: учеб. пособ. для курсантов и слушателей КВИРТУ ПВО / О.Я. Матов. — К.: КВИРТУ. — 1977. — 242 с.

3. *Василенко В.С.* Визначення потрібної надлишковості в коді «Зважених груп». Оптимальна надлишковість / М.Ю. Василенко, А.В. Чунарьов // Матеріали 6-ї Міжнар. наук.-практ. конф. «Aktuálni vymoženosti vědy – 2010», DÍl 14, 27.06.2010 – 05.07.2010. — С. 22–24.

4. *Василенко В.С.* Визначення реальної надлишковості для коду «зважених груп» / М.Ю. Василенко, А.В. Чунарьов // Матеріали VI Міжнар. наук.-практ. конф. «Nauka: teoria i praktika – 2010» 07–15 серпня 2010. Nowoczesne informacyjne technologie. Fizyka. — Перемишль: «Nauka I studia». — 2010. — Т. 7. — С. 74–76.

5. *Выгодский М.Я.* Справочник по элементарной математике / М.Я. Выгодский. — М.: Физматгиз, 1962. — 420 с.

Надійшла до редакції 11.07.2013