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

Циклічність операцій контролю за довільним модулем

Для задач забезпечення контролю цілісності інформаційних об'єктів розглянуто підходи щодо виявлення та оцінки циклічності операцій контролю за довільним модулем.

Ключові слова: *завадостійкість, контроль за модулем, циклічність.*

Однією із найважливіших задач технічного захисту інформації є задача забезпечення цілісності інформаційних об'єктів, яка вирішується шляхом контролю наявності чи контролю та корегування спотворень у цих інформаційних об'єктах.

Аналіз процедур контролю цілісності з використанням модульних операцій

Для аналізу контрольованості інформаційні об'єкти найчастіше розбивають на певні частини (блоки) загальної довжини m інформаційних символів, відносно до яких можна застосувати той чи інший завадостійкий код, наприклад, контроль за деяким модулем [1, 2]. Якщо вважати такий блок інформаційного об'єкта деяким числом у позиційній системі числення з основою x, а отже уявити його у вигляді поліному $G(x)$, то при контролі за модулем слід розділити число (поліном) $G(x)$ на обраний модуль. У свою чергу, модуль може бути представленим аналогічним числом (поліномом) $P(x)$ степені k. Після такого ділення одержують лишок довжиною k символів. Цей k-символьний лишок тим чи іншим чином дописують до початкового інформаційного об'єкта. Внаслідок цього утворюється так зване базове кодове слово (БКС) довжиною $n = m + k$ символів, яке в подальшому циркулює (зберігається, передається, обробляється) в телекомунікаційних мережах.

Контрольним модулем $P(x)$ може бути або деяке число (наприклад, число 2 при контролі на парність чи непарність), або більш складна конструкція, наприклад, утворюючий поліном (як у циклічних кодах). У першому випадку здійснюється обчислення k-значного лишку від розподілу m-розрядного початкового інформаційного об'єкта $G(x)$ на відповідний k-значний модуль $P(x)$, передавання

одержаного n-значного БКС каналами передачі, повторне, вже на приймальному боці, обчислення лишку від розподілу інформаційної частини прийнятого БКС і порівняння прийнятого та знов обчисленого лишків. При їхньому збіганні робиться висновок щодо відсутності спотворень, інакше — про їхню наявність та, за певних умов, здійснюється їхнє корегування.

У другому випадку (наприклад, у циклічних кодах) здійснюється обчислення лишку від розподілу зсунутого на k розрядів (чи помноженого на x^k (у відомих циклічних кодах $x = 2$)) початкового інформаційного об'єкта $G(x)$ на утворюючий k-значний поліном $P(x)$. Одержаний k-значний лишок

$$R(x) = [G(x) \cdot x^k] \bmod P(x) \tag{1}$$

додається до зсунутого початкового інформаційного об'єкта, за рахунок чого одержують n-значне БКС виду $F(x) = G(x) \cdot x^k + R(x)$. У виразі (1) операція $\bmod P(x)$ означає обчислення лишку від розподілу попереднього операнда на $P(x)$. На приймальному боці здійснюється обчислення лишку від розподілу одержаного БКС на утворюючий поліном. Цей лишок

$$\begin{aligned} R_{\Sigma}(x) &= [G^{/}(x) \cdot x^k + R(x)] \bmod P(X) = \\ &= G^{/}(x) \cdot x^k \bmod P(X) \oplus R(x) \bmod P(X) = \\ &= [R^{/}(x) \oplus R(x)] \bmod P(X), \end{aligned} \tag{2}$$

в якому $[G^{/}(x) \cdot x^k + R(x)]$ — значення прийнятого БКС з можливою наявністю спотворень в інформаційній частині БКС. У разі відсутності спотворень, тобто при $G^{/}(x) = G(x)$, маємо $R^{/}(x) = R(x)$. Тоді у відомих циклічних кодах результат контролю дорівнює нулю $R_{\Sigma}(x) = [R^{/}(x) \oplus R(x)] \bmod P(x) = 0$, оскільки всі операції додавання здійснюються за модулем 2($\bmod 2$), що позначено вище як $\oplus$, коли $f(x) \oplus f(x) = 0$. Внаслідок цього при $R^{/}(x) = R(x)$ маємо $[R^{/}(x) \oplus R(x)] \bmod 2 = 0$, що свідчить про відсутність спотворень. В іншому випадку, тобто за наявності спотворень, результат контролю є відмінним від нуля. Неважко упевнитися в тому, що за наявності спотворень не в інформаційній частині БКС, а у надлишкових символах, тобто у разі $G^{/}(x) = G(x)$ та $R^{/}(x) \neq R(x)$, одержимо такий же результат: $R_{\Sigma}(x) \neq 0$.

Постановка задачі щодо циклічності операцій контролю за довільним модулем

Відомо, що свою назву цей код одержав за ту властивість, що при контролі циклічно зсунутих БКС одержують ті ж результати, як і без зсуву. Отже циклічність кодів дозволяє здійснювати контроль інформаційних об'єктів без визначення початку інформаційних об'єктів, тобто без їхньої синхронізації, а отже, робить

задачу контролю більш простою. Поставимо задачу забезпечення циклічності операцій контролю за довільним модулем.

Величина $R(x)$ — остача від ділення $G(x)\cdot x^k$ на $P(x)$ показує, що, з іншого боку, для одержання цілочисельного результату ділення, а, отже, нульової остачі, досить збільшити ділене $G(x)\cdot x^k$ на величину

$$R^{/}(x) = P(x) - R(x). \tag{3}$$

Таким чином, за рахунок запропонованої зміни порядку обчислення надлишкових символів, можна очікувати на деяке спрощення процедури контролю і за довільним модулем.

Тобто пропонується наступна процедура кодування та подальшого виявлення наявності спотворень у вихідному інформаційному слові при використанні запропонованого підходу.

При кодуванні:

1) обчислення остачі за виразом (1):

$R(x) = G(x)\cdot x^k \{\mathrm{mod}\, P(x)\}$;

2) доповнення цієї остачі згідно (3) до $P(x)$:

$R^{/}(x) = P(x) - R(x)$;

3) формування результату завадостійкого кодування у вигляді n-значного БКС вигляду:

$$F^{/}(x) = G(x)\cdot x^k + R^{/}(x). \tag{4}$$

При декодуванні:

4) здійснення контролю цілісності прийнятого БКС $F^{/}(x)$ шляхом ділення його на утворюючий поліном $P(x)$ та аналізу відповідної остачі.

У разі відсутності спотворень результат ділення величини $F^{/}(x)$ на $P(x)$ дасть значення, яке дорівнює нулю:

$$\begin{aligned} R_{\Sigma}(x) &= [G(x)\cdot x^k + P(x) - R(x)]\{\mathrm{mod}\, P(X)\} = \\ &= G(x)\cdot x^k \{\mathrm{mod}\, P(X)\} + [P(x) - R(x)]\{\mathrm{mod}\, P(X)\} = \\ &= [R(x) + P(x) - R(x)]\{\mathrm{mod}\, P(X)\} = P(x)\{\mathrm{mod}\, P(X)\} = 0. \end{aligned} \tag{5}$$

І, навпаки, при $R_{\Sigma}(x) \neq 0$, звідки слід робити висновок про наявність спотворень.

Таким чином, процедура (5) надає такий же результат, що і процедура (2), але із (5) циклічність цього коду не є очевидною.

Для здійснення контролю з довільним модулем, представленим, наприклад у вигляді деякого простого числа $P(x) = p_k$, авторами пропонується застосування процедур і обрахування БКС, і контролю його цілісності, які є близькими до процедур кодування звичайним циклічним кодом. При цьому слід врахувати, що, на

відміну від цих суто двійкових кодів, виникає дещо інша ситуація, що пов'язана з відмінностями в типі як відповідних змінних, так і застосованих операцій.

Зрозуміло, що функції утворюючого поліному $P(x)$ повинен перебрати на себе цей контрольний модуль p_k. Тоді доповнення остачі до контрольного модуля набуде вигляду $R^{/}(x) = p_k - R(x)$. Наслідки такої операції при застосуванні цього коду покажемо на наступному прикладі.

***Приклад* 1**. Нехай потрібно здійснити кодування деякого інформаційного об'єкта, наприклад у вигляді десяткового числа 19 (x = 10), за модулем $p_k = 13$. Оскільки лишок від ділення на такий модуль потребує двох розрядів, то і БКС повинно мати [1, 2] два контрольних розряди (k = 2) і відповідно до (4) набуде значення:

$$F(x) = G(x) \cdot x^k + p_k - R(x) = 19 \cdot 10^2 + 13 - 1900 \bmod 13 = 1913 - 2 = 1911.$$

За відсутності спотворень результат контролю на приймальному боці дасть:

$$R^{/}(x) = 1911 \bmod 13 = 0,$$

що свідчить про відсутність спотворень. Неважко упевнитися, що за наявності спотворення в одному із символів БКС величина $R(x)$ є відмінною від нуля. Наприклад, при $F^{/}(x) = 1610$, одержимо $R(x) = 1610 \bmod 13 = 8 \neq 0$, при $F^{/}(x) = 1912$ одержимо $R(x) = 1912 \bmod 13 = 1 \neq 0$ і т.п.

Тоді *застосування процедури* (5) *може дати певний виграш* унаслідок відсутності у цьому випадку необхідності здійснення операції порівняння контрольної ознаки, одержаної разом із БКС, з контрольною ознакою, що обрахована для прийнятого із каналу повідомлення.

Циклічність операцій контролю за довільним модулем

На цьому ж прикладі звернемо увагу на ***можливості щодо циклічності розглянутих операцій контролю за довільним модулем***. Ці можливості полягають у вже згаданій властивості, що при контролі циклічно зсунутих БКС одержують ті ж результати, як і без зсуву.

Для з'ясування можливостей використання цієї ж властивості для операцій контролю за довільним модулем розглянемо можливі результати контролю уже розглянутого об'єкта після циклічного зсуву, наприклад, у бік старших розрядів ($F(x) = 1911 \rightarrow F^{/}(x) = 9111$).

Неважко зрозуміти, що циклічний зсув є еквівалентним множенню усього початкового об'єкта на основу системи числення x (у нашому прикладі — $x = 10$) із одночасним переносом старшого символу на місце молодшого розряду, тобто на місце, яке звільнилося після зсуву молодшого символу. Внаслідок цього $F(x)$ перетвориться в $F^{/}(x) = F(x) \cdot x - a_{n-1} \cdot x^n + a_{n-1}$, а з урахуванням того, що зна-

чення a_{n-1} після переносу стає значенням молодшого розряду $a_{n-1} = a_1$, слід записати $F^{/}(x) = F(x) \cdot x - a_1 \cdot x^n + a_1$.

Для прикладу 1, число 1911 перетвориться на число

$$F^{/}(x) = 1911 \cdot 10 - 1 \cdot 10000 + 1) = 19110 - 10000 + 1 = 9111).$$

Тоді є справедливими перетворення:

$$F^{/}(x) = F(x) \cdot x - a_1 \cdot x^n + a_n = [G(x) \cdot x^k + p_k - R(x)] \cdot x - a_n \cdot (x^n - a_n).$$

При контролі такого циклічно зсунутого інформаційного об'єкта одержимо наступне значення контрольної ознаки:

$$\begin{aligned} R^{/}(x) &= \{[G(x) \cdot x^k + p_k - R(x)] \cdot x - a_1 \cdot (x^n - 1)\} \bmod p_k = \\ &\{\{[G(x) \cdot x^k + p_k - R(x)] \cdot x\} \bmod p_k + \{p_k - a_1 \cdot (x^n - 1)\} \bmod p_k\} \bmod p_k. \end{aligned} \quad (6)$$

При одержанні цього результату використано правила виконання модульних операцій, коли результат будь-яких операцій над складним математичним виразом є результатом тих же операцій над лишками відповідних операндів за цим же модулем. При цьому операція віднімання замінюється на операцію додавання з доповненням від'ємного операнда до відповідного модуля. Для одержання результатів наступних перетворень застосуємо ці ж правила до першого доданку виразу (6):

$$\{[G(x) \cdot x^k + p_k - R(x)] \cdot x\} \bmod p_k.$$

Звернемо увагу на те, що перший операнд операції множення є вже відомим виразом (5) і за модулем p_k дорівнює нулю:

$$[G(x) \cdot x^k + p_k - R(x)] \bmod p_k = 0,$$

а, отже, вираз (6) набуде значення:

$$R^{/}(x) = \{p_k - a_1 \cdot (x^n - 1)\} \bmod p_k. \quad (7)$$

Із останнього виразу не важко побачити, що оскільки величини p_k та n є константами системи контролю, то константою коду є і величина $c = (x^n - 1) \bmod p_k$. Отже результат контролю циклічно зсунутого неспотвореного об'єкта є функцією лише значення молодшого розряду a_1, циклічно зсунутого об'єкта (старшого розряду у незсунутому об'єкті):

$$R^{/}(x) = (p_k - a_1 \cdot c) \bmod p_k. \qquad (8)$$

***Приклад* 2**. Нехай потрібно здійснити декодування інформаційного об'єкта за прикладом 1 ($F(x) = 1911$), одержаним у вигляді 9111, при підозрі, що це БКС може бути циклічно зсунутим.

Контроль цього об'єкта дасть $R(x) = 9111 \bmod 13 = 11 \neq 0$. Отже, прийнято спотворене або циклічно зсунуте БКС. Для перевірки щодо останнього припущення визначимо константу коду — $c = (x^n - 1) \bmod p_k$. Для цього прикладу

$$c = (x^n - 1) \bmod p_k = (10^4 - 1) \bmod 13 = 9999 \bmod 13 = 2.$$

З урахуванням того, що у прийнятому БКС значення молодшого розряду $a_1 = 1$, на підставі виразу (8) маємо $R^{/}(x) = \{13 - 1 \cdot 2\} \bmod 13 = 11$.

Оскільки $R(x) = R^{/}(x) = 11 \neq 0$, робимо висновок, що ***одержаний об'єкт є неспотвореним циклічно зсунутим БКС***.

Іншими словами, у разі одержання при контролі відмінного від нуля лишка за наявності впевненості, що контролювалося БКС без зсувів, слід зробити висновок, що має місце спотворення.

При підозрі, що здійснювався контроль циклічно зсунутого БКС слід:

1) згідно із вищевизначеним виразом (8) обрахувати нове значення контрольної ознаки: $R^{/}(x) = (p_k - a_1 \cdot c) \bmod p_k$ та здійснити повторний контроль цілісності;

2) у разі одержання лишку, що дорівнює попередньому, зробити висновок про відсутність спотворень БКС, яке є циклічно зсунутим. У іншому випадку — висновок, що має місце спотворення.

***Приклад* 3**. Покажемо можливості коду з виявлення спотворення, наявного в інформаційному об'єкті. Нехай потрібно здійснити декодування інформаційного об'єкта за прикладом 1, одержаним у вигляді 1011, з перевіркою підозри, що це БКС може бути циклічно зсунутим.

Первинний контроль цього об'єкта дасть $R(x) = 1011 \bmod 13 = 10 \neq 0$. Для перевірки припущення щодо циклічного зсуву з урахуванням того, що константа коду $c = 2$, а значення молодшого розряду у прийнятому БКС $a_1 = 1$, на підставі виразу (8) маємо $R^{/}(x) = \{13 - 1 \cdot 2\} \bmod 13 = 11$.

Оскільки контрольні ознаки первинного контролю та контролю з підозрою на наявність циклічного зсуву не співпадають ($R(x) = 10 \neq R^{/}(x) = 11$), робимо висновок, що ***одержаний об'єкт є спотвореним БКС***.

Зрозуміло, що циклічний зсув на кількість позицій, яка дорівнює *i*, є еквівалентним послідовному *i*-разовому множенню усього початкового об'єкта на x з одночасним переносом старших символів на місця, які звільнилися після зсуву молодших символів. Тут, як і раніше, x — основа системи числення (у нашому прикладі — $x = 10$). При першому зсуві $F(x)$ перетвориться на $F_1(x) = F(x) \cdot x - a_{n-1} \cdot x^n + a_{n-1} = F(x) \cdot x - a_{n-1} \cdot (x^n - 1)$, а з урахуванням того, що значення a_{n-1}

після переносу стає значенням молодшого розряду $a_{n-1} \to a_1$, для умов апаратурної чи програмної реалізації можна записати: $F_1(x) = F(x) \cdot x - a_1 \cdot x^n + a_1$.

Неважко впевнитися, що при другому зсуві $F_1(x)$ набуде вигляду:

$$F_2(x) = F(x) \cdot x \cdot x - a_{n-1} \cdot (x^n - 1) \cdot x - a_{n-2} \cdot (x^n - 1) = F(x) \cdot x^2 - (x^n - 1) \cdot (a_{n-1} \cdot x + a_{n-2}).$$

Для спрощення подальших міркувань звернемо увагу на те, що лишок за контрольним модулем ($\mathrm{mod}\, p_k$) від першого доданку, як і в попередньому випадку, дорівнює нулю не залежно від величини другого множника. Отже значення лишку:

$$F_2(x) \,\mathrm{mod} p_k = F(x) \cdot x^2 - (x^n - 1) \cdot (a_{n-1} \cdot x + a_{n-2}) = [p_k - (x^n - 1) \cdot (a_{n-1} \cdot x + a_{n-2})] \,\mathrm{mod} p_k.$$

Розповсюджуючи результати, що одержані після прикладів щодо першого та другого зсувів, на циклічний зсув на довільну кількість позицій, яка дорівнює i, можна записати:

$$F_i(x) \,\mathrm{mod} p_k = [p_k - (x^n - 1) \cdot \sum_{j=1}^{i} a_{n-j} \cdot x^{i-j}] \,\mathrm{mod} p_k = [p_k - c \cdot \sum_{j=1}^{i} a_{n-j} \cdot x^{i-j}] \,\mathrm{mod} p_k. \quad (9)$$

Наприклад, при кількості зсувів $i = 3$:

$$\sum_{j=1}^{3} a_{n-j} \cdot x^{i-j} = a_{n-1} \cdot x^{3-1} + a_{n-2} \cdot x^{3-2} + a_{n-3} \cdot x^{3-3} \quad a_{n-1} \cdot x^2 + a_{n-2} \cdot x + a_{n-3}.$$

***Приклад* 4**. Нехай при передаванні повідомлення за прикладом 1 здійснено циклічний зсув на 3 символи так, що має місце перехід вигляду $F(x) = 1911 \to F_3(x) = 1191$. Контроль такого повідомлення дасть результат:

$$F_3(x) \;\mathrm{mod} 13 = \; 1191 \,\mathrm{mod} 13 = 8. \quad (10)$$

Оскільки значення лишку є відмінним від нуля, робимо висновок щодо наявності спотворень, або циклічного зсуву.

Перевіримо наявність циклічного зсуву з урахуванням раніше визначеного значення константи коду $c = 2$. Розрахунки за виразом (9) у припущенні наявності зсуву на один символ дадуть:

$$F_1(x) \,\mathrm{mod} p_k = [p_k - c \cdot \sum_{j=1}^{1} a_{n-j} \cdot x^{i-j}] \,\mathrm{mod} p_k = [p_k - c \cdot a_{n-1}] \,\mathrm{mod} p_k = 13 - 2 \cdot 1 = 11 \neq 0.$$

Отже, припущення щодо наявності зсуву на один символ є невірним.

Розрахунки в припущенні наявності зсуву на два символи дадуть:

1. $\sum_{j=1}^{2} a_{n-j} \cdot x^{i-j} = 1 \cdot x + 9 = 19$;
2. $19 \bmod 13 = 6$;
3. $F_3(x) \bmod p_k = [p_k - c \cdot \sum_{j=1}^{i} a_{n-j} \cdot x^{i-j}] \bmod p_k = [13 - 2 \cdot 6] \bmod 13 = 1 \neq 0.$

Отже, і припущення щодо наявності зсуву на два символи є невірним.

Розрахунки в припущенні наявності зсуву на три символи дадуть:

1. $\sum_{j=1}^{3} a_{n-j} \cdot x^{i-j} = 1 \cdot x^2 + 9 \cdot x + 1 = 191$;
2. $191 \bmod 13 = 9$;
3. $F_3(x) \bmod p_k = [p_k - c \cdot \sum_{j=1}^{i} a_{n-j} \cdot x^{i-j}] \bmod p_k = [13 - 2 \cdot 9] \bmod 13 = 8.$

Оскільки результати цього та першого розрахунків за виразом (10) збігаються, то слід зробити висновок, що прийнято неспотворений інформаційний об'єкт, циклічно зсунутий на 3 символи. Зрозуміло, що у загальному випадку ці перевірки можна здійснювати аж до $n-1$ зсувів, і лише після цього можна зробити остаточний висновок щодо цілісності відповідного об'єкта.

Така властивість щодо виявлення будь-яких циклічних зсувів інформаційних об'єктів надає можливість не лише відкинути як необґрунтовану підозру в наявності спотворень та підтвердити цілісність цих об'єктів, але й визначити кількість зсувів. Це може бути корисним для синхронізації процесів передавання та приймання в інформаційно-телекомунікаційних мережах.

Таким чином, запропонований підхід свідчить про наявність циклічних властивостей кодів із контролем за довільним модулем та про можливості їхнього використання.

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

2 *Матов О.Я.* Основы теории передачи дискретной информации / О.Я. Матов: учеб. пособ. для курсантов и слушателей КВИРТУ ПВО. — 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 міжнародної науково-практичної конференції «Aktuálnivymoženostivědy–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 міжнародної Науково-практичної конференції «Nauka: teoria i praktika – 2010» 07–15 серпня 2010. Nowoczesne informacyjne technologie. Fizyka. — Перемишль: «Nauka I studia», 2010. — Т. 7. — С. 74–76.

Надійшла до редакції 09.04.2013