УДК 004.056.2

О. Я. Матов[1], В. С. Василенко[2]
[1]Інститут проблем реєстрації інформації НАН України
вул. М. Шпака, 2, 03113 Київ, Україна
[2]Національний авіаційний університет
вул. Космонавта Комарова, 1, 03056 Київ, Україна

Захист інформаційних об'єктів від навмисних колізій контрольних ознак у завадостійких кодах

Для завадостійких кодів уведено поняття колізій ознак цілісності та показано, що їхня наявність призводить для одержувача повідомлень до невиявлення, найчастіше навмисних модифікацій, а отже може мати тяжкі наслідки. Показано шляхи мінімізації кількості колізій ознак цілісності.

Ключові слова: *завадостійкі коди, захист інформації, інформаційні об'єкти, колізії ознак цілісності, цілісність.*

Вступ

Як відомо [1], однією з функціональних властивостей захищеності інформаційних об'єктів є цілісність. Порушення цілісності можливе внаслідок природних (шуми) та штучних (завади, модифікація, ненавмисні дії персоналу тощо) впливів. Виявлення цих порушень досягається застосуванням процедур контролю чи контролю та поновлення цілісності. Завданням процедур контролю цілісності є виявлення факту наявності спотворень у відповідному інформаційному об'єкті, а процедур виявлення та поновлення цілісності, окрім цього ще й виявлення місця та величини цих спотворень.

Для вирішення завдань виявлення (в кодах, що виявляють тільки факт наявності спотворень) та розрізняння спотворень (у корегувальних кодах) окрім суто інформаційних використовуються надлишкові символи. Кількість надлишкових символів повідомлення та їхнього значення визначаються вимогами щодо допустимої (чи потрібної) цілісності (допустима ймовірність пропуску спотворень) та обраховуються за процедурами відповідного коду.

Із цією метою обчислюється ознака цілісності (залежно від прийнятої термінології — контрольна ознака, хеш-функція тощо) згідно різних варіацій реалізації виразу [1–6]:

$$R(x) = \sum_{s=1}^{l} a_i c_i \bmod P(x), \qquad (1)$$

де, залежно від коду, $R(x)$ — шукане значення надлишкової k-розрядної частини коду; $P(x)$ — значення так званого контрольного модуля (і тоді $P(x) = P$ — деяке, найчастіше, просте число), або значення так званого утворюючого k-розрядного поліному — поліному, що не розкладається на множники (поліноміальний запис деякого еквіваленту k-розрядного простого числа); a_i — значення символів інформаційної частини повідомлення, а іноді й усього повідомлення (i = 1, 2, …, $l = m$, чи i = 1, 2, …, $l = n = m + k$); m — кількість символів інформаційної частини повідомлення; $n = (m + k)$ — загальна кількість символів повідомлення; c_i — значення вагових коефіцієнтів символів повідомлення (числа); позначка $\sum_{s=1}^{l} a_i$ означає додавання (звичайне арифметичне, чи якесь інше, зокрема, по-символьне (розрядне) додавання по деякому модулю, наприклад по mod2).

Таке повідомлення найчастіше розглядається як числа $A(x)$ в деякій системі числення з основою q. Як символи повідомлення можуть розглядатися: по-перше, окремі розряди, і тоді при q = 2 маємо *двійковий код*; по-друге, сукупність, група розрядів (*узагальнені символи*), і тоді маємо *узагальнені* коди. Довжина узагальненого символу може складати від декількох розрядів до декількох байтів.

Неважко упевнитися в тому, що виразом (1) можуть бути описані якщо не всі, то більшість із відомих кодів. Наприклад, при $l = m$, основі q, коли a_i приймає значення 0, 1,…, (q − 1), $c_i = q^i$ (i = 0, 1, 2, …, m − 1) і $P(x) \ge q^n$, маємо звичний безнадлишковий позиційний, поліноміальний запис числа A в системі числення з основою q, тобто:

$$R(x) = \sum_{s=1}^{l} a_i c_i \bmod P(x) = \sum_{s=1}^{m} a_i q^i \bmod q^n = \sum_{s=1}^{m} a_i q^i = A(x).$$

Аналогічно, при q = 2 (двійкові коди, коли a_i приймає значення 0 чи 1) $c_i = 2^i$ (i = 0, 1, 2, …, m − 1) і $P(x) \ge 2^n$, маємо звичний запис числа $A(x)$ у двійковій системі числення; при $l = n$, основі q = 2, $c_i = i + 1$ (i = 0, 1, 2, …, n − 1) і $P(x) \ge 2^k$, коли на позиціях із номерами 2^i (i = 0, 1, 2, …, k − 1) розташовуються надлишкові, а на решті позицій інформаційні символи, маємо код Хеммінга; при $l = n$, основі q = 2, $P(x)$ — утворюючий поліном коду і $c_i = 2^i \bmod P(x)$, коли на позиціях з номерами i = 0, 1, 2, …, (k − 1) розташовуються надлишкові, а на решті позицій інформаційні символи, маємо одну з модифікацій циклічного коду і т.д.

Обчислення ознак цілісності при контролі цілісності здійснюється за однаковими процедурами при первинному кодуванні, наприклад $R(x)$ перед передаванням інформаційного об’єкта, та після приймання інформаційного об’єкта, наприклад $R'(x)$ при перевірці факту наявності спотворень. В останньому випадку

здійснюється порівняння значень $R(x)$ та $R'(x)$. Якщо ці величини є однаковими, робиться висновок про відсутність спотворень, в іншому разі — про їхню наявність.

Колізії ознак цілісності

Звернемо увагу на те, що самі по собі ознаки цілісності для споживачів є надлишковою інформацією. Тому часто здійснюються спроби зменшити кількість надлишкових символів *k*, яку іноді доводять до *k* = 1. Досить часто зустрічаються ситуації, коли $k < m$, а тим більше, $k < n$. Тоді при розрядності ознаки цілісності *k* максимальна кількість варіантів цієї ознаки складає 2^k, у той час як кількість варіантів спотворень S_p *n*-розрядного (чи *m*-розрядного) інформаційного об'єкта може бути набагато більшою і досягати в найбільш тяжкому випадку $S_p = 2^l$ (тобто 2^n чи 2^m), де S_p — кількість спотворень кратності, можливої для цієї телекомунікаційної системи.

Це означає, що різні інформаційні об'єкти можуть неминуче мати однакові контрольні ознаки. Це явище має назву *колізій.* Неважко побачити, що причинами колізій є ситуації, що пов'язані, зокрема, з правилами обчислення ознаки цілісності як лишку від розподілу інформаційного об'єкта або на контрольний модуль *P*, або на утворюючий поліном *P*(*x*). Для того щоби зрозуміти такі ситуації, розглянемо значення лишків *m*-розрядних інформаційних об'єктів (чисел) вигляду $A'(x) = A(x) \pm s \cdot P$. У цьому виразі змінна *s* може прийняти будь-яке ціле значення в інтервалі від $s_{\min} = 1$ до $s_{\max} = [S_p / P]$, $s_{\max} = [2^l / P]$, де прямі дужки означають обчислення цілої частини; операція $\pm$ виконується за правилами застосованого коду, наприклад у циклічних кодах — це порозрядне додавання за модулем 2.

Тоді за правилами виконання операцій за модулем для будь-яких значень $A(x)$ маємо

$$A'(x) \bmod R = (A(x) \pm s \cdot P) \bmod P =$$
$$= A(x) \bmod P \pm s \cdot P \bmod P = A(x) \bmod P + 0 = A(x) \bmod P,$$

тобто ознаки цілісності таких об'єктів є однаковими, що означає колізію цих ознак.

В окремих випадках, коли контрольний модуль *P* або утворюючий поліном *P*(*x*) дорівнюють деякій степені двійки, наприклад $P = 2^k$, змінна *s* є цілою величиною: $s_{\max} = [S_p / P] = 2^l / 2^k$. Зрозуміло, що в загальних випадках при обчисленні *s* доцільно застосовувати знак приблизного рівняння так, що $s_{\max} = [2^l / P] \approx 2^l / 2^k$.

Кількість цих колізій:

$$n_{кол} = s_{\max} = [S_p / P], \qquad (2)$$

і в разі, коли не здійснено ніяких заходів щодо зменшення кількості спотворень $S_p = 2^l$, може досягати

$$n_{кол} = [2^l / P]$$

для будь-яких інформаційних об'єктів і контрольних модулів.

При цьому ймовірність колізій $P_{кол}$ може бути визначеною як

$$P_{кол} = n_{кол} / 2^l = [2^l / P] / 2^l \approx 1 / P \approx 2^{-k}.$$

Звернемо увагу на те, що в разі, коли йдеться лише про виявлення факту наявності спотворень, ситуація з наявністю колізій не є критичною: не важливо, виявлено спотворення в інформаційному об'єкті величиною $A(x)$ чи в інформаційному об'єкті величиною $A'(x) = A(x) \pm s \cdot P$. Головним тут є — виявлено спотворення чи ні? Але ситуація змінюється кардинально у разі прагнення зловмисника здійснити приховану модифікацію (умисне спотворення), яка не повинна бути виявленою одержувачем інформації при застосуванні завадостійких кодів. Тоді при модифікації шляхом спотворення інформаційного об'єкта на величину $E(x) = s \cdot P$ $(s = 1, 2, ..., s_{\max})$ виявити спотворення не можливо. Це твердження ілюструється нижче прикладами 1–4.

Приклад 1. Нехай при застосуванні циклічного коду з параметрами $n = 7$, $m = 4$, $k = 3$ щодо первинного інформаційного об'єкта $G(x) = x^3 + x^2 + 1 = 1101$ при утворюючому поліномі $P(x) = x^3 + x + 1 = 1011$ для визначення контрольних ознак із застосуванням методу ділення на утворюючий поліном одержано кодовий багаточлен:

$$F(x) = x^3 G(x) + R(x) = x^6 + x^5 + x^3 + 1.$$

Тоді за відсутності спотворень результат декодування (табл. 1) дасть результат $R(x) = 0$, що свідчить про відсутність спотворень, тобто про правильне невиявлення спотворень.

Таблиця 1

Приклад 1	**Приклад 2**
$x^6 + x^5 + x^3 + 1 \mid x^3 + x + 1$ $x^6 + x^4 + x^3 \mid x^3 + x^2 + x + 1$ $x^5 + x^4 + 1$ $x^5 + x^3 + x^2$ $x^4 + x^3 + x^2 + 1$ $x^4 + x^2 + x$ $x^3 + x + 1$ $x^3 + x + 1$ $R(x) = 0$	$x^6 + x^5 + x^4 + x^2 \mid x^3 + x + 1$ $x^6 + x^4 + x^3 \mid x^3 + x^2 + x + 1$ $x^5 + x^3 + x^2$ $x^5 + x^3 + x^2$ $R(x) = 0$

Приклад 2. Нехай інформаційний об'єкт $F(x)$ за прикладом 1 модифіковано (спотворено) на величину $(x + 1) \cdot P(x) = (x+1) \cdot (x^3 + x + 1) = x^4 + x^2 + x + x^3 + x + 1 = x^4 + x^3 + x^2 + 1$, унаслідок чого він набув вигляду $F'(x) = x^6 + x^5 + x^3 + 1 + x^4 + x^3 + x^2 + 1 = x^6 + x^5 + x^4 + x^2$. Тоді результат декодування модифікованого об'єкта (табл. 1) також дасть результат $R(x) = 0$, що знову свідчить про «відсутність» спо-

творень. Насправді результат декодування дає спотворене значення прийнятого інформаційного об'єкта $G(x) = (x^6 + x^5 + x^4)/x^3 = x^3 + x^2 + x = 1110$, *що є невірним*.

Приклад 3. Нехай при застосуванні циклічного коду з параметрами $n = 7$, $m = 4$, $k = 3$ щодо первинного інформаційного об'єкта $G(x) = x^3 + x^2 + 1 = 1101$ при утворюючому поліномі $P(x) = x^3 + x + 1 = 1011$ для визначення контрольних ознак із застосуванням методу множення на утворюючий поліном одержано кодовий багаточлен

$$F(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1.$$

Тоді за відсутності спотворень результат декодування (табл. 2) дасть результат $R(x) = 0$, що свідчить про відсутність спотворень.

Таблиця 2

Приклад 3	**Приклад 4**
$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \mid x^3 + x + 1$ $x^6 + x^4 + x^3 \mid x^3 + x^2 + 1$ $x^5 + x^2 + x + 1$ $x^5 + x^3 + x^2$ $x^3 + x + 1$ $x^3 + x + 1$ $R(x) = 0$	$x^6 + x^5 + x \mid x^3 + x + 1$ $x^6 + x^4 + x^3 \mid x^3 + x^2 + x$ $x^5 + x^4 + x^3 + x$ $x^5 + x^3 + x^2$ $x^4 + x^2 + x$ $x^4 + x^2 + x$ $R(x) = 0$

Приклад 4. Нехай інформаційний об'єкт $F(x)$ за прикладом 3 модифіковано (спотворено) на величину $(x + 1)\cdot P(x) = (x + 1)\cdot(x^3 + x + 1) = x^4 + x^2 + x + x^3 + x + 1 = x^4 + x^3 + x^2 + 1$, унаслідок чого він набув вигляду $F'(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 + x^4 + x^3 + x^2 + 1 = x^6 + x^5 + x$.

Тоді результат декодування модифікованого об'єкта (табл. 2) також дасть результат $R(x) = 0$, що знову свідчить про «відсутність» спотворень. Насправді результат декодування дає спотворене значення прийнятого інформаційного об'єкта $G(x) = x^3 + x^2 + x = 1110$, *що є невірним*.

Таким чином, у прикладах 1, 2 *та* 3, 4 *два різних інформаційних об'єкти мають однакові контрольні ознаки, тобто маємо їхню колізію. Ця колізія призводить для одержувача повідомлень до наявності невиявлених (пропущених), найчастіше навмисних модифікації, а отже може мати тяжкі наслідки.*

Виходом із цієї ситуації може бути лише варіант побудови такого коду, котрий забезпечує відсутність колізій: $n_{кол} = [S_p / P]$. Це, в свою чергу, є можливим тільки в разі, коли контрольний модуль є більшим за можливу кількість спотворень: $P > S_p$. Зрозуміло, що для зменшення кількості колізій слід зменшувати величину $n_{кол} = [S_p / P]$, мінімальне значення якої $n_{кол} = 0$ досягається при $P > S_p$. Дійсно, у цьому випадку співвідношення $[S_p / P] < 1$, відповідно, $n_{кол} = 0$.

Отже, досягнення цієї мети можливе, по-перше, при збільшенні контрольного модуля при фіксованому значенні кількості спотворень, по-друге, при зменшенні кількості спотворень при фіксованому значенні контрольного модуля та,

по-третє, при одночасному збільшенні контрольного модуля і зменшенні кількості спотворень.

У цьому випадку, тобто при $P > S_p$, ознака цілісності (хеш-функція) вигляду (1) набуває значення $A \bmod P = A - \left[A / P \right] \cdot P = A - l \cdot P$ $R(x) = \sum_{s=1}^{l} a_i c_i \bmod P.$

Отже,

$$R(x) = \sum_{s=1}^{l} a_i c_i \bmod P = A \bmod P = A - \left[A / P \right] \cdot P = A - 0 \cdot P = A,$$

і результуючий об'єкт для зберігання чи передавання може утворюватись у вигляді окремого дубля первинного інформаційного блоку (A, A), чи у вигляді конкатенації первинного об'єкта та його дубля у вигляді $A \| A$.

Таке дублювання іноді може мати сенс, але вкрай обмежено, по-перше, через велику надлишковість, що часто є неприпустимим. По-друге, цей спосіб при такому значенні лише одного ключа перетворення ніякої конфіденційності, навіть самої ознаки цілісності (хеш-функції), не забезпечує. Це свідчить про те, що у цих умовах обчислення хеш-функції як в задачах контролю цілісності, так і, особливо, в задачах криптографічних перетворень значною мірою втрачає сенс.

Але цей спосіб «утворення» ознак цілісності використовується в групових (мажоритарних) методах контролю чи контролю та поновленню цілісності, наприклад шляхом утворення резервних копій інформаційних об'єктів (системного, прикладного програмного забезпечення, баз даних чи просто дуже важливих вихідних даних, результатів обчислень тощо). Такі дублі інформаційних об'єктів (3, 5 та інша їхня непарна кількість) можуть передаватись одночасно відповідною кількістю каналів передачі чи послідовно одним і тим же каналом. Але, оскільки особливістю цих методів є повна відкритість цих копій, то при зберіганні для захисту від одночасної модифікації більшості з копій, нормативними документами Системи технічного захисту інформації України вимагається їхнє збереження у сховищах, які знаходяться під охороною і розташовані бажано в просторово рознесених місцях.

Коли ж первинний інформаційний об'єкт та його ознака цілісності не можуть бути відокремленими, величину модуля, за яким обчислюється ознака цілісності, слід обирати якомога більшою (аж до $P > 2^m$). Тобто задача має протиріччя, яке полягає в тому, що для зменшення кількості колізій контрольний модуль слід мати такий, що забезпечує відсутність колізій та одночасно і властивості з криптографічної стійкості ознак цілісності.

Мінімізація кількості колізій ознак цілісності та надлишковості

Розв'язання цього протиріччя пропонується за рахунок збільшення величини контрольного модуля шляхом утворення єдиного контрольного модуля (в задачах криптографічних перетворень — ключа перетворення) у вигляді добутку f його складових [6, 7] так, що:

$$P = \prod_{i=1}^{f} p_i > 2^m .$$

Такий підхід є еквівалентним застосуванню до інформаційного об'єкта A декількох (f) перетворень (1). Але, на відміну від (1) відповідна сукупність ключів розглядається як один складний модуль (основа), який дорівнює добутку із набору f часткових модулів (основ), вимогою до якого є: $P = \prod_{i=1}^{f} p_i > 2^m$. Унаслідок цього одержується кількість лишків $h_i(A)$, яка є відповідною кількості основ p_i, та зменшеною, відповідно, кількістю колізій: при $A < 2^m$ та $P > 2^m$ кількість колізій дорівнює нулю. Тоді результуючий інформаційний блок може буди записаним у вигляді:

$$A_{рез} = A \| h_1 \| h_2 ... \| h_m .$$

Звернемо увагу, що сукупність основ p_i та відповідних лишків (хеш-функцій) h_i (i =1, 2, …, n) утворює певну систему числення з діапазоном представлення $P = \prod_{i=1}^{f} p_i$. Ця система числення має назву системи лишкових класів, а сукупність лишків $h_1 \| h_2 ... \| h_m$ є представленням сукупного лишку $h(A) = R(A)$ у діапазоні P цієї системи числення, а кожна із зазначених хеш-функцій є лишком від розподілу первинного коду A на сукупність основ цієї системи лишкових класів p_i, тобто $h_i = a_i = A \bmod p_i$.

Оскільки в цьому випадку $P > 2^m$, то кількість колізій дорівнює нулю: $n_{кол} = 0$, тобто протиріччя є розв'язаним.

Окрім того, із теорії лишкових класів відомо [4], що сукупний лишок $R(x) = h(A)$ при величині контрольного модуля — ключа перетворення, яка перевищує діапазон представлення первинних чисел 2^m, тобто при $P = \prod_{i=1}^{f} p_i > 2^m$, однозначно відображає первинний блок A, і є його представленням у вигляді набору лишків: $A_{СЛК} = h_1 \| h_2 ... \| h_m = a_1, a_2, ..., a_m$. Тепер результуючий інформаційний блок може буди записаним у вигляді: $A_{рез} = A \| A_{СЛК}$. Тобто дублювання, а отже і *суттєва надлишковість* мають місце, але *може бути легко усунутим*, якщо для збереження чи передавання відмовитися від первинного інформаційного блоку A і вважати $A_{рез} = A_{СЛК} = a_1, a_2, ..., a_m$. При виборі такої сукупності із f часткових основ, коли складний модуль P перевищує діапазон представлення інформаційних об'єктів 2^m, величина надлишковості може бути незначною. Але при зменшенні такої надлишковості слід забезпечити її достатність для вирішення задач забезпечення цілісності: по-перше, виявлення факту наявності, місця та величини спотворення, а, по-друге, забезпечення неможливості чи, хоч аби, суттєве утруднення прихованої

модифікації за рахунок тих же колізій. Для вирішення *першої групи задач* достатньо скористатися відомостями про те, що при забезпеченні виявлення і виправлення будь-яких спотворень у межах лишку за однією з основ достатньо мати надлишкову (контрольну) основу, величина якої задовольняє умові [4]:

$$p_{m+1} = p_n \geq 2 p_f p_{f-1}, \tag{3}$$

де p_f, p_{f-1} — найбільші з основ із їхньої сукупності p_i (i = 1, 2, …, f).

Звернемо увагу, що за рахунок таких операцій здійснено перетворення в систему лишкових класів, тобто здійснено криптографічне перетворення з ключем у вигляді набору основ p_i (i = 1. 2, …, n), яке за умови, що ключ (сукупність основ p_i (i = 1, 2, …, f) та p_k) є таємним, задовольняє усім вимогам щодо стійкості алгоритмів шифрування [5]. При цьому перетворення в систему лишкових класів потребує забезпечення виконання операції прихованої модифікації за рахунок колізій також у системі лишкових класів $A'_{СЛК} = (A_{СЛК} \pm (s \cdot p_n)_{СЛК})_{СЛК}$. При цьому слід забезпечити додавання в системі лишкових класів чисел

$$A_{СЛК} = a_1, a_2, ..., a_f$$

та

$$(s \cdot p_n)_{СЛК} = (s \cdot p_n) \bmod p_1, (s \cdot p_n) \bmod p_2, ..., (s \cdot p_n) \bmod p_f,$$

що потребує знання кожної із основ p_i (i = 1, 2, …, f) та їхнього взаємного розташування. Секретність ключа забезпечує те, що зловмисник вимушений користуватися для розкриття величин основ і їхнього взаємного розташування методом прямого перебору, а отже криптографічна стійкість розглянутих перетворень досить легко забезпечується в заданих межах.

Розв’язання задачі зменшення кількості колізій є можливим шляхом зменшення кількості спотворень S_p при припустимому значенні контрольного модуля так, що $P > S_p$.

У [1–6] показано, що для визначення кількості спотворень в інформаційному об’єкті слід визначити їхню кількість у наступних ситуаціях:

спотворення відсутні — $C_n^0 - 1$ випадок;

одиночне спотворення — C_n^1 випадків;

двократне спотворення — C_n^2 випадків;

……..

спотворення кратності $t_в$ — $C_n^{t_в}$ випадків;

……..

Наведена вище позначка C_n^m означає обчислення кількості з’єднань із n елементів по m. Таким чином, загальна кількість спотворень кратності $t_в$ і менш дорівнює $\sum_{i=0}^{t_d} C_n^i$, а в разі можливості існування всіх можливих спотворень від $t_в = 0$

до $t_в = n$ кількість спотворень визначається як $S_p = \sum_{i=0}^{n} C_n^i$. Як відомо [1–3], ця сума визначається з урахуванням властивостей коефіцієнтів бінома Ньютона як

$$S_p = \sum_{i=0}^{n} C_n^i = 2^n,$$

що, як відомо з [1], призводить до неможливості застосування будь-яких завадостійких кодів.

Але, якщо можливо обмежитися необхідністю виявлення лише однократних спотворень (наприклад, за рахунок перемежування символів інформаційних об'єктів), то кількість спотворень суттєво зменшується до

$$S_p = \sum_{i=0}^{1} C_n^i \quad n+1,$$

і в цьому випадку кількість надлишкових символів k, що потрібна для контрольного модулю, вибирається з умови $k \geq \log_2 S_p$. Це дозволяє легко виконати наведену вище вимогу $P > S_p$, а отже забезпечити неможливість утворення колізій.

За рахунок викладеного у статті підходу *забезпечується конфіденційність ознак цілісності*, а за умови збереження надлишковості згідно з вимогою (3) досягається одночасно *здатність щодо контролю та поновленню цілісності* інформаційних об'єктів *без колізій*.

1. *Василенко В.С.* Целостность и доступность информационных объектов (монография) / В.С. Василенко, О.Я. Матов. — Saarbrucken, Deutschland: LAMBERT Academic Publishing, 2013. — 95 с. — ISBN 978-3-659-47333-3.

2. *Василенко В.С.* Прикладная теория информации и кодирования (монография) / В.С. Василенко, Е.В. Дубчак. — Saarbrücken, Deutschland: LAMBERT Academic Publishing, 2013. — 129 с. — ISBN 978-3-659-45467-7.

3. *Василенко В.С.* Обеспечение целостности и доступности объектов в информационных сетях (монография) / В.С. Василенко, О.В. Дубчак. — Saarbrücken, Deutschland: LAMBERT Academic Publishing, 2015. — 325 с. — ISBN 978-3-659-20764-8.

4. *Василенко В.С.* Помехоустойчивые коды (монография) / В.С. Василенко. — Saarbrücken, Deutschland: LAMBERT Academic Publishing, 2013. — 101 с. — ISBN 978-3-8484-9206-0.

5. *Василенко В.С.* Код условных вычетов. Контроль целостности и криптографические преобразования (монография) / В.С. Василенко. — Saarbrücken, Deutschland: LAMBERT Academic Publishing, 2013. — 129 с. — ISBN 978-3-659-48203-8.

6. *Василенко В.С.* Поновлення цілісності інформаційних об'єктів в коді умовних лишків. / В.С. Василенко // Матеріали XVIII Міжнародної науково-практичної інтернет-конференції «Проблеми та перспективи розвитку науки на початку третього тисячоліття у країнах Європи та Азії» 29– 30 вересня 2015 р.: зб. наук. праць. — Переяслав-Хмельницький, 2015 р. — С. 119–122.

Надійшла до редакції 13.04.2016