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
Проспект Космонавта Комарова, 1, 03680 Київ, Україна

Криптозахист інформаційних об'єктів шляхом блокових перетворень із позиційної системи числення в систему лишкових класів

Запропоновано використання блокового криптографічного перетворення з використанням системи числення в лишкових класах для задач забезпечення конфіденційності інформаційних об'єктів автоматизованих систем.

Ключові слова: *інформація, конфіденційність, криптографічні перетворення, лишкові класи, системи числення.*

Вступ

Однією із вкрай важливих для сучасних автоматизованих систем є проблема забезпечення конфіденційності та цілісності інформації [1–3], для вирішення якої застосовуються ті чи інші методи, методики або алгоритми.

У багатьох випадках чи не єдиним шляхом забезпечення конфіденційності інформації є її криптографічне перетворення (з певною стійкістю до спроб розкриття її змісту — криптографічною стійкістю).

Слід звернути увагу на те, що одночасне забезпечення і конфіденційності, і цілісності інформаційних об'єктів при використанні відомих алгоритмів досягається послідовним застосуванням процедур криптографічного перетворення та процедур обчислення цифрового підпису. При зворотному перетворенні спочатку перевіряється цілісність інформації, а потім здійснюється її дешифрування. Тобто цей процес є двофазним і при прямому, і при зворотному перетворенні, за рахунок чого продуктивність засобів оброблення інформації дещо знижується.

Для усунення цього недоліку в [4] запропоновано низку кодових перетворень, у тому числі криптографічних із застосуванням процедур кодування шляхом перетворення із позиційної системи числення (ПСЧ) в систему лишкових класів (СЛК) і процедур декодування шляхом перетворення із системи лишкових класів у позиційну систему числення. В [4] показано також, що такі криптографічні пере-

творення (шифрування) вихідного тексту можна здійснити шляхом перемноження матриці-рядка, отриманої при представленні вихідного коду довжиною в k символів, і кодувальної матриці G (див. рисунок) із k рядків і k стовпців. Правила вибору чи формування її елементів визначаються типом перетворення.

$$G = \begin{pmatrix} g_{11} & g_{12} & \cdot & g_{1n} & \cdot & g_{1k} \\ g_{21} & g_{22} & \cdot & g_{2n} & \cdot & g_{2k} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ g_{n1} & g_{n2} & \cdot & g_{nn} & \cdot & g_{nk} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ g_{k1} & g_{k2} & \cdot & \cdot & \cdot & g_{kk} \end{pmatrix}.$$

Загальний вид кодувальної матриці

Код, що отриманий у результаті множення вихідного коду на кодувальну матрицю, є деяким криптографічним перетворенням вихідного коду. Якщо механізм формування елементів кодувальної матриці є секретним, чи механізм формування елементів кодувальної матриці є загальновідомим, але при їхньому формуванні використовуються деякий секретний параметр — ключ, то зашифрований код має визначену криптографічну стійкість, тобто стійкість до спроб криптоаналітиків одержати із зашифрованого коду (часто з використанням певної частки відкритого вихідного тексту) ключ, чи власне вихідний код (текст). Така криптографічна стійкість є основною властивістю таких перетворень і досить часто визначається числом варіантів ключів.

У статті пропонуються методики отримання запропонованих у [4] матриць для прямих і зворотних перетворень із використанням лишкових класів.

Методика побудови та застосування кодувальної матриці для блокового криптоперетворення типу позиційна система числення → система лишкових класів

З урахуванням викладеного в [4], методика (алгоритм) блокового криптографічного перетворення вихідного m-символьного цифрового коду (блоку відкритого тексту з m символів), який вважається деяким числом A у позиційній системі числення, на число в системі числення в лишкових класах $A_{\text{слк}}$ зводиться до наступних процедур (операцій).

1. Представлення сукупності символів обраного позиційного представлення — вихідного слова для кодування у вигляді матриці-рядка розмірності $(1 \times m)$ виду $A = (a_1, a_2, ..., a_i, ..., a_m)$. З цією метою символи вихідного блоку слід розглядати як символи a_i ($i = 1, 2, \ldots, m$) обраного позиційного представлення (цифри в позиційній системі числення числа A) з відповідними ваговими коефіцієнтами. Наприклад, для представлення в десятковій системі числення $C_i = 10^{i-1}$; для двійкового представлення за умови представлення символів вихідного коду як байтів — $C_i = 256^{i-1}$. Неважко зрозуміти, що діапазон представлення таких чисел у першому випадку дорівнює $0 \le A < 10^m$, а в другому — $0 \le A < 256^m$.

2. Узгодження розмірів кодувальної матриці та вихідного слова для кодування. З цією метою необхідно:

а) вибрати сукупність основ системи числення в лишкових класах з $n \geq m$ взаємно простих чисел p_j (j = 1, 2, …, n), де p_j — j-та основа (елемент криптографічного ключа, за допомогою якого забезпечується потрібна криптографічна стійкість (див. далі)). Кількість (n) основ p_j (основ, які в лишкових класах утворюють діапазон представлення чисел («робочий» діапазон СЛК) $P = \prod_{j=1}^{n} p_j$, тобто кількість «робочих» основ) слід обирати такою, щоби діапазон представлення в СЛК «перекривав» діапазон представлення в позиційній системі числення. Зрозуміло, що останнє є можливим за умови $256^{m-1} \leq P$ для двійкового представлення, чи $10^{i-1} \leq P$ для десяткового представлення.

Оскільки в подальшому постане питання про визначення елементів зворотної матриці шляхом перетворення кодувальної матриці в декодувальну, яке є можливим лише для квадратних матриць, то зрозуміло, що як розмірність для кодувальної матриці слід обирати більше із значень m та n. Позначимо розмірність кодувальної матриці як $k = \max(m,n)$. Для узгодження розмірів матриць при $m < k$ вихідну матрицю-рядок (текст для криптоперетворень) $A = (a_1, a_2, ..., a_i, ..., a_m)$ слід доповнити ($s = k - m$) нулями на місцях старших розрядних коефіцієнтів (як відомо при цьому величина чисел у ПСЧ не збільшується). При цьому вихідна матриця A набуде вигляду $A = (0, 0,..., a_{s+1}, a_{s+2}, ..., a_{s+i}, ..., a_k)$, тобто замість розмірності ($1 \times m$) отримає розмірність ($1 \times k$);

б) визначити розмірність кодувальної матриці як ($k \times k$), де $k = m + s$;

в) визначити елементи $g_{ij} = \{c_i\}_{p_j}$ кодувальної матриці G з розмірністю ($k \times k$), де знак $\{c_i\}_{p_j}$ означає обчислення лишку (відрахування) від розподілу c_i на p_j;

3. Здійснення власне криптографічного перетворення $A_{слк} = A \times G$. При цьому слід враховувати, що всі операції повинні здійснюватися за відповідними модулями, тобто при обчисленні першого елемента результуючої матриці-рядка — за модулем p_1, другого — за модулем p_2, i-го — за модулем p_i і т.д.

Проілюструємо застосування цієї методики на наступних прикладах.

***Приклад* 1.** Пряме перетворення чисел із десяткової ПСЧ на систему лишкових класів.

Нехай криптографічному перетворенню підлягає дворозрядне вихідне слово A = 17 (m = 2) з ваговими коефіцієнтами $c_1 = 10^0 = 1$ та $c_2 = 10^2 = 10$. У вигляді матриці-рядка це слово має вигляд A = (1, 7).

Виберемо сукупність основ системи числення в лишкових класах. Нехай це є основи: $p_1 = 2$; $p_2 = 3$; $p_3 = 5$ (n = 3). Тоді діапазон представлення чисел («робочий» діапазон) у СЛК: $P = \prod_{j=1}^{j=3} p_j = 30$.

Визначимо розмірність кодувальної матриці k як $k = \max(m, n) = \max(2, 3) =$ = 3. Для узгодження розмірів матриць ($m < k$) вихідну матрицю $A = (a_1, a_2, a_3)$ слід доповнити одним ($s = k - m$ = 1) нулем на місці старшого розрядного коефіцієнта.

При цьому вихідна матриця A набуде вигляду $A = (0, a_2, a_3) = (0, 1, 7)$ з ваговими коефіцієнтами $c_1 = 10^0 = 1$, $c_2 = 10^1 = 10$ та $c_3 = 10^2 = 100$, тобто замість розмірності (1×2) отримає розмірність (1×3).

Створимо кодувальну матрицю G з розмірністю (3×3), в якості елементів g_{ij} якої будемо використовувати величини $g_{ij} = \{c_i\}_{p_j}$, де знак $\{c_i\}_{pj}$ означає обчислення лишку (відрахування) від розподілу c_i на p_j. Унаслідок цього отримаємо: $g_{11} = \{100\}_2 = 0$, $g_{12} = \{100\}_3 = 1$, $g_{13} = \{100\}_5 = 0$, $g_{21} = \{10\}_2 = 0$, $g_{22} = \{10\}_3 = 1$, $g_{23} = \{10\}_5 = 0$, $g_{31} = \{1\}_2 = 1$, $g_{32} = \{1\}_3 = 1$, $g_{33} = \{1\}_5 = 1$, тобто

$$\mathrm{G} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}.$$

Здійснимо перетворення:

$$A_{слк} = A \times G = (0, 1, 7) \times \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} = (7_2, 8_3, 7_5) = (1, 2, 2).$$

В останньому виразі запис $x_y = x \pmod y$ і означає обчислення лишку від розподілу x на у. Неважко переконатися в правильності виконаного перетворення.

***Приклад* 2.** Пряме перетворення чисел із десяткової ПСЧ у систему лишкових класів для іншої сукупності основ системи числення в лишкових класах. Нехай це є основи: $p_1 = 3$; $p_2 = 7$; $p_3 = 11$ ($n = 3$). Тоді діапазон представлення чисел («робочий» діапазон) у СЛК: $P = \prod_{j=1}^{j=3} p_j = 231$.

Визначимо розмірність кодувальної матриці k. Як і в попередньому прикладі $k = \max(m,n) = 3$. При цьому вихідна матриця A, як і раніше, має вигляд $A = (0, a_2, a_3) = (0, 1, 7)$ з ваговими коефіцієнтами $c_1 = 10^0 = 1$, $c_2 = 10^2 = 10$ та $c_3 = 10^3 = 100$, тобто має розмірність (1×3).

Створимо кодувальну матрицю G з розмірністю (3×3). Внаслідок цього отримаємо: $g_{11} = \{100\}_3 = 1$, $g_{12} = \{100\}_7 = 2$, $g_{13} = \{100\}_{11} = 1$, $g_{21} = \{10\}_3 = 1$, $g_{22} = \{10\}_7 = 3$, $g_{23} = \{10\}_{11} = 10$, $g_{31} = \{1\}_3 = 1$, $g_{32} = \{1\}_7 = 1$, $g_{33} = \{1\}_{11} = 1$, тобто

$$G = \begin{pmatrix} 1 & 2 & 1 \\ 1 & 3 & 10 \\ 1 & 1 & 1 \end{pmatrix}.$$

Здійснимо перетворення:

$$A_{слк} = A \times G = (0\ 1\ 7) \times \begin{pmatrix} 1 & 2 & 1 \\ 1 & 3 & 10 \\ 1 & 1 & 1 \end{pmatrix} = (8_3\ 10_7\ 17_{11}) = (2, 3, 6).$$

Неважко переконатись у правильності виконаного перетворення.

Таким чином, наведені ілюстративні приклади підтверджують правильність запропонованої методики побудови та застосування кодувальних матриць для блокового криптоперетворення типу позиційна система числення → система лишкових класів.

Методики побудови декодувальних матриць для дешифрування (зворотного криптоперетворення) блокового криптоперетворення типу система лишкових класів → позиційна система числення

Із уже викладеного зрозуміло, що для зворотного перетворення необхідно:

1) визначити елементи зворотної матриці G^{-1};

2) здійснити зворотне перетворення $A = A_{слк} \times G^{-1}$.

Для зрозуміння подальших міркувань щодо зворотного перетворень чисел із СЛК у ПСЧ розглянемо процедури визначення елементів зворотної матриці G^{-1} для умов розглянутих вище прикладів прямого перетворення із позиційної десяткової системи числення у систему лишкових класів.

При визначенні елементів зворотної матриці G^{-1} нагадаємо, що така (зворотна) матриця існує, якщо детермінант для прямої матриці G є відмінним від нуля, тобто $\det G \neq 0$.

***Приклад* 3.** Спробуємо отримати зворотну матрицю для перетворення СЛК → ПСЧ для умов прямого перетворення за прикладом 1. Неважко переконатися, що для цього прикладу, нажаль, $\det G = 0$, тобто отримати зворотну матрицю G^{-1} традиційним математичним методом неможливо. Це пояснюється тим, що в матриці G є однаковими перший та другий рядки, а також перший і третій стовпчики, коли за властивостями детермінанта він дорівнює нулю. Останнє, в свою чергу, є наслідком того, що основи $p_1 = 2$ та $p_3 = 5$ є дільниками усіх вагових розрядів ПСЧ. Але аналогічна ситуація може бути і у випадку, коли основами СЛК будуть обрані числа, величина яких перевищує значення вагових коефіцієнтів (наприклад, $c_1 = 10^0 = 1$, $c_2 = 10^1 = 10$, ...). Тоді в кодувальній матриці з'являться рядки, які є лінійними комбінаціями один одного, внаслідок чого за властивостями детермінанта він буде дорівнювати нулю.

Примітка 1. Таке явище призводить до зменшення кількості чисел, які можуть бути використаними як основи СЛК і, зрозуміло, — до зменшення кількості варіантів ключів, що має своїм наслідком зниження криптографічної стійкості коду.

Першим способом уникнення цього ускладнення є вибір таких основ, які не є дільниками вагових розрядів. Для ілюстрації цього підходу розглянемо наступний приклад для умов перетворення того ж самого вихідного слова $A = (1, 7)$ із тими ж, зрозуміло, ваговими коефіцієнтами $c_1 = 10^0 = 1$ та $c_2 = 10^2 = 10$.

***Приклад* 4.** Визначимо елементи зворотної матриці G^{-1} для умов прямого перетворення за прикладом 2. Для цього спочатку перевіримо, що вона існує. Дійсно, для заданих умов

$$\det G = \begin{vmatrix} 1 & 2 & 1 \\ 1 & 3 & 10 \\ 1 & 1 & 1 \end{vmatrix} = 9 \neq 0,$$

тобто зворотна матриця існує. Не важко переконатися, що така матриця має вигляд:

$$G^{-1} = (1/9) \begin{pmatrix} -7 & -1 & 17 \\ 9 & 0 & -9 \\ -2 & 1 & 1 \end{pmatrix}.$$

На розвиток цього прикладу і для перевірки правильності отримання зворотної матриці розглянемо приклади перетворення кодів із СЛК в ПСЧ.

***Приклад* 4.1.** Нехай перше число в СЛК є $A_{\text{слк}} = (1, 1, 1)$. Тоді:

$$A_{\text{ПСЧ}} = A_{\text{слк}} \times G^{-1} = (1, 1, 1) \times (1/9) \begin{pmatrix} -7 & -1 & 17 \\ 9 & 0 & -9 \\ -2 & 1 & 1 \end{pmatrix} = (1/9)\,(0, 0, 9) = (0, 0, 1) = 1.$$

Останнє витікає з того, що запис (0, 0, 1) є скороченим записом поліноміального представлення в десятковій системі числення, коли

$$(0, 0, 1) = 0 \cdot 10^2 + 0 \cdot 10^1 + \cdot 10^0 = 1,$$

що свідчить про правильність виконаного перетворення.

***Приклад* 4.2.** Нехай другим числом у СЛК є $A_{\text{слк}} = (0, 3, 3)$. Тоді:

$$A_{\text{ПСЧ}} = A_{\text{слк}} \times G^{-1} = (0, 3, 3) \times (1/9) \begin{pmatrix} -7 & -1 & 17 \\ 9 & 0 & -9 \\ -2 & 1 & 1 \end{pmatrix} = (1/9)\,(21, 3, -24).$$

Такий вигляд отриманого числа в ПСЧ є досить незвичним. Але його легко перетворити у звичний вигляд, якщо згадати, що при записі чисел у поліноміальній формі слід писати:

$$A_{\text{ПСЧ}} = (1/9)\,(21, 3, -24) = (1/9)\,(21 \cdot 10^2 + 3 \cdot 10^1 + (-24) \cdot 1) = (1/9) \cdot 2106 = 234.$$

Звернемо увагу також на те, що отриманий результат перевищує допустиме значення, тобто число $A_{\text{ПСЧ}}$ вийшло за межі робочого діапазону СЛК: $A_{\text{ПСЧ}} = 234 > 231$. Для вводу цього числа в робочий діапазон слід здійснити операцію

$A_{\text{ПСЧ}} = \{A_{\text{ПСЧ}}\}_{231} = \{234\}_{231} = 3$, що свідчить про правильність виконаного перетворення.

Зауважимо, що останні перетворення пов'язані з наступними властивостями поліноміального представлення чисел та їхнього переводу із СЛК у ПСЧ.

1. Запис чисел у ПСЧ є формою їхнього скороченого поліноміального представлення:

$$\text{А}_{\text{ПСЧ}} = a_{n\text{-}1}\cdot 10^{n\text{-}1} + a_{n\text{-}2}\cdot 10^{n\text{-}2} + \ldots + a_2\cdot 10^2 + a_1\cdot\cdot 10^1 + a_0\cdot\cdot 10^0. \qquad (1)$$

2. Величина чисел у ПСЧ, що отримані внаслідок усіх перетворень, не повинна перевищувати діапазон їхнього представлення в СЛК: $P = \prod_{j=1}^{j=n} p_j$.

3. При представленні чисел у ПСЧ слід враховувати наявність міжрозрядних зв'язків і можливості запозичення із старших розрядів у молодші та переносів із молодших розрядів у старші в разі, коли значення розрядних коефіцієнтів:

а) є меншими ніж нуль;

б) є більшими ніж 10.

Це призводить до того, що результат в останній ілюстрації у вигляді $A_{\text{ПСЧ}} = (1/9)\ (21, 3, -24)$ слід послідовно записати у вигляді

$$A_{\text{ПСЧ}} = (1/9)\ (21, 3, -24)\ (1/9)\ (21, 0, 30 - 24) = (1/9)\ (21, 0, 6) = (1/9)\ (2, 1, 0, 6),$$

по-перше, як наслідок запозичення із другого розряду трьох десятків для отримання невід'ємного значення першого розрядного коефіцієнта, та, по-друге, переносу двох десятків із третього розрядного коефіцієнта як двох одиниць до четвертого розрядного коефіцієнта.

Унаслідок реалізації перших трьох властивостей операцію ділення на множник детермінанта слід здійснювати по відношенню до єдиного десяткового числа у формі (1), отримавши при цьому $A_{\text{ПСЧ}} = 2106/9 = 234$ та $A_{\text{ПСЧ}} = \{234\}_{231} = 3$.

Такі ж наслідки можна отримати, здійснивши операції за п. 3, по відношенню до елементів декодувальної матриці, звернувши увагу на те, що результат множення вектора-рядка $A_{\text{слк}}$ на зворотну матрицю G^{-1} можна записати у вигляді

$$A_{\text{ПСЧ}} = A_{\text{слк}} \times G^{-1} = (0, 3, 3) \times (1/9) \begin{pmatrix} -7 & -1 & 17 \\ 9 & 0 & -9 \\ -2 & 1 & 1 \end{pmatrix} =$$

$$= (1/9)\ [(0\cdot(-7) + 3\cdot 9 + 3\cdot(-2)), (0\cdot(-1) + 3\cdot 0 + 3\cdot 1), (0\cdot 17 + 3\cdot(-9) + 3\cdot 1)],$$

де в кожній із круглих дужок записані результати обчислення вагових коефіцієнтів ПСЧ.

Тоді після врахування вагових коефіцієнтів

$$A_{\text{ПСЧ}} = (1/9)\ [(0\cdot(-7) + 3\cdot 9 + 3\cdot(\text{-}2))\cdot 10^2 + (0\cdot(-1) + 3\cdot 0 + 3\cdot 1)\cdot 10^1 + (0\cdot 17 + 3\cdot(-9) + 3\cdot\ 1)\cdot 10^0],$$

групування щодо елементів матриці-рядка

$$A_{\text{ПСЧ}} = (1/9)\ \{0\cdot\ [(-7)\cdot 100 + (-1)\cdot 10 + 17\cdot 1] + 3\cdot[9\cdot 100 + 0\cdot 10 + (-9)\cdot\ 1] + \\ + 3\cdot[(-2)\cdot 100 + 1\cdot 10 + 1\cdot 1]\} = (1/9)\ [0\cdot(-700 - 10 + 17) + 3\cdot(900 - 9) + \\ + 3\cdot(-200 + 10 + 1)] = (1/9)\cdot[0\cdot(-693) + 3\cdot 891 + 3\cdot(-189)]$$

та ділення на величину множника детермінанта отримаємо:

$$A_{\text{ПСЧ}} = 0\cdot(-77) + 3\cdot 99 + 3\cdot\ (-21).$$

Для позбавлення від від'ємних величин введемо результати обчислення в межі робочого діапазону:

$$A = \{A_{\text{ПСЧ}}\}_{231} = \{\{0\cdot(-77)\}_{231} + \{3\cdot 99\}_{231} + 3\cdot\{(-21)\}_{231}\}_{231} = \{\{0\cdot(-77 + 231) + \\ + \{3\cdot 99\}_{231} + \{3\cdot(-21 + 231)\}_{231}\}_{231} = \{\{0\cdot 154 + \{3\cdot 99\}_{231} + \{3\cdot 210\}_{231}\}_{231} = \\ = \{0 + 66 + 168\}_{231} = \{234\}_{231} = 3.$$

Такий довгий шлях достатньо елементарних розрахунків ми зробили лише для того, щоб звернути увагу на проміжний результат останнього розрахунку у вигляді

$$\{A_{\text{ПСЧ}}\}_{\text{Р}} = \{\{0\cdot 154 + \{3\cdot 99\}_{P} + \{3\cdot 210\}_{P}\}_{P},$$

що можна трактувати як результат операції

$$A_{\text{ПСЧ}} = A_{\text{слк}}\times G^{-1} = (0, 3, 3)\times\begin{pmatrix} 1 & 5 & 4 \\ 0 & 9 & 9 \\ 2 & 1 & 0 \end{pmatrix} = \{6\cdot 10^2 + 30\cdot 10^1 + 27\}_{231} = \{927\}_{231} = 3.$$

Звернемо увагу також, що до зворотної матриці G^{-1} у вигляді

$$G^{-1} = \begin{pmatrix} 1 & 5 & 4 \\ 0 & 9 & 9 \\ 2 & 1 & 0 \end{pmatrix}$$

можна прийти шляхом низки наступних перетворень:

$$G^{-1} = (1/9)\begin{pmatrix} -7 & -1 & 17 \\ 9 & 0 & -9 \\ -2 & 1 & 1 \end{pmatrix} = (1/9)\begin{pmatrix} -7 & 0 & 7 \\ 8 & 9 & 1 \\ -2 & 1 & 1 \end{pmatrix} = (1/9)\begin{pmatrix} 7-700=-693 \\ 891 \\ 11-200=-189 \end{pmatrix} = \begin{pmatrix} -077 \\ 099 \\ -021 \end{pmatrix} = \\ = \begin{pmatrix} -077 \\ 099 \\ -021 \end{pmatrix} + \begin{pmatrix} 2 & 3 & 1 \\ 0 & 0 & 0 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 5 & 4 \\ 0 & 9 & 9 \\ 2 & 1 & 0 \end{pmatrix}.$$

У цій низці перетворень використані операції міжрозрядних запозичень і переносів, а також операції введення результатів у межі робочого діапазону.

І, нарешті, покажемо, що ця матриця є не що інше, як розклад за елементами матриці ортогональних базисів з обраними основами системи числення в лишкових класах. Дійсно, для обраного набору основ $p_1 = 3$, $p_2 = 7$, $p_3 = 11$ ($n = 3$) із діапазоном представлення чисел («робочим» діапазоном) $P = \prod_{j=1}^{j=3} p_j = 231$, константами $P_1 = 231/3 = 77$, $P_2 = 231/7 = 33$, $P_3 = 231/11 = 21$, маємо «ваги» ортогональних базисів системи $m_1 = 2$, $m_2 = 3$, $m_3 = 10$, що в наслідку дає значення ортогональних базисів системи $\boldsymbol{B_1} = 77 \cdot 2 = \mathbf{154}$, $\boldsymbol{B_2} = 33 \cdot 3 = \mathbf{099}$, $\boldsymbol{B_3} = 21 \cdot 10 = \mathbf{210}$.

Таким чином, із викладеного витікає, що елементи матриці для зворотного перетворення із СЛК у ПСЧ можна визначати шляхом класичних математичних перетворень лише в окремих випадках. Більш універсальним є визначення таких матриць, виходячи із властивостей коду, тобто як значення ортогональних базисів системи. Останнє було визначено в [4] при розгляді питання про завадостійкі перетворення, коли як зворотну матрицю G^{-1} запропоновано використати спрощену зворотну матрицю виду

$$\mathrm{G}^{-1} = \begin{pmatrix} g_{11} & B_{21} \\ g_{12} & B_{22} \\ . & . \\ g_{1k} & B_{2k} \end{pmatrix}.$$

Такий підхід розв’язує проблему щодо визначення матриць для декодування (для зворотного перетворення із СЛК у ПСЧ) у разі, коли детермінант кодувальної матриці дорівнює нулю. Тим самим знімаються і обмеження з вибору основ СЛК і, таким чином, обмеження щодо криптографічної стійкості коду (див. примітку 1).

1. *Нормативний* документ Системи технічного захисту інформації «Загальні положення про захист інформації в комп’ютерних системах від несанкціонованого доступу» (НД ТЗІ 1.1-002-99).

2. *Нормативний* документ Системи технічного захисту інформації «Критерії оцінки захищеності інформації в комп’ютерних системах від НСД» (НД ТЗІ 2.5-004-99).

3. *Нормативний* документ Системи технічного захисту інформації «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» [НД ТЗІ 2.5-005-99].

4. *Василенко В.С.* Варіант завадостійкого криптографічного перетворення / В.С. Василенко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — 2004. — Вип. 8. — С. 101–108.

Надійшла до редакції 14.02.2012