УДК 681.3.06

ОЦІНКА ЕФЕКТИВНОСТІ КАСКАДНИХ ТЕОРЕТИКО-КОДОВИХ СХЕМ ЗАХИСТУ ІНФОРМАЦІЇ

М.М. Ляпа*, В.М. Лисенко*, В.І. Грабчак*, О.В. Лисенко**
**Військовий інститут РВ і А Сумського державного університету*
***Сумський державний університет*

Розглядаються кількісні показники оцінки інформаційної прихованості (криптографічної стійкості), часові і ємнісні труднощі каскадних теоретико-кодових схем із замаскованим алгеброгеометричним кодом зовнішнього ступеня.

ПОСТАВЛЕННЯ ПРОБЛЕМИ В ЗАГАЛЬНОМУ ВИГЛЯДІ І АНАЛІЗ ЛІТЕРАТУРИ

Проведений аналіз стану і перспективи розвитку системи управління військами (силами) і зброєю показав, що в умовах підвищення швидкоплинності операцій (бойових дій), необхідності негайного реагування на динамічні зміни в обстановці, зростання обсягів і різноплановості завдань, вирішального значення чинника часу в управлінні військами існуюча система управління не повною мірою відповідає імовірнісно-часовим вимогам, що ставляться. Комплекси автоматизації та зв'язку, що стоять на озброєнні, морально і фізично застаріли та не дозволяють забезпечити сучасні вимоги щодо інформаційної скритності та достовірності передачі даних в перспективній АСУВ.

Перспективним напрямом в розвитку комплексних механізмів забезпечення інформаційної скритності та достовірності передачі даних є каскадні теоретико-кодові схеми, що функціонують в режимі маскування кодових слів під випадкову послідовність [1]. В роботі представлені результати проведених досліджень властивостей розроблених каскадних теоретико-кодових схем і запропоновані практичні рекомендації щодо застосування розроблених технічних рішень для інтегрованого забезпечення інформаційної прихованості та достовірності передачі даних.

Метою статті є дослідження стійкості, часової та ємнісної складності каскадних теоретико-кодових схем із замаскованими алгеброгеометричними кодами на зовнішньому ступені узагальненого каскадного коду порядку m = 5-10. При цьому як код зовнішнього ступеня розглядається алгеброгеометричний код, побудований по еліптичних кривих (еліптичний код).

Основна частина. Одним з основних показників оцінки ефективності таємних систем є криптографічна стійкість [2-4]. Вона розцінюється як найважливіший чинник при оцінці безпеки криптоалгоритму та визначається такими імовірнісно-часовими показниками криптографічної стійкості:

– безпечний час $T_Б$, що характеризує час безпечної роботи даного криптоалгоритму за умови застосування противником різних методів криптоаналізу;

– вірогідність правильного відновлення ключа шифрування P_K, ключа розшифрування P_{K*} і відкритого тексту P_M за умови застосування противником різних методів криптоаналізу.

За визначенням [5] алгебраїчно заданий узагальнений каскадний код порядку m однозначно визначається n_2 квадратними двійковими

матрицями H_0^j, $j = \overline{1, n_2}$ порядку n_1 (які задають (n_1, k_i, d_{1i}) коди першого ступеня) і $m+1$ груповими над $GF(2^{a_i})$, $i = \overline{1, m+1}$ кодами другого ступеня з параметрами (n_2, b_i, d_{2i}).

Формування каскадної теоретико-кодової схеми здійснюється шляхом маскування кодів зовнішнього ступеня узагальненого каскадного коду, а процес формування кодограм відповідає формуванню кодового слова замаскованого каскадного коду із додаванням до нього випадкового вектора помилки.

Параметри еліптичних кодів, які використовуються як коди зовнішнього ступеня узагальненого каскадного коду та характеристики відповідних каскадних теоретико-кодових схем, що рекомендуються до практичного використання для інтегрованого підвищення інформаційної прихованості передачі даних для $R = 1/2$, подані в табл. 1.

Проведемо дослідження стійкості розроблених теоретико-кодових схем до криптоаналітичних атак противника.

У загальній класифікації всі атаки противника можна класифікувати так:

1) атака з відомою кодограмою;
2) атака з підібраною кодограмою;
3) атака з відомим відкритим текстом;
4) атака з підібраним відкритим текстом.

Як показано в [6], вдала реалізація противником будь-якої з перелічених атак приведе до знаходження однієї з допустимих матриць - лінійно еквівалентної матриці G. Це приведе до того, що противник зможе формувати кодограми (знизить імітостійкість системи), проте для їх декодування і декодування кодограм, сформованих уповноваженим користувачем системи, йому необхідна матриця H - ключ зворотного перетворення. Для пошуку матриці H йому потрібно буде знайти одне (конкретне) розв'язання системи рівнянь:

$$HG^T = \begin{pmatrix} h_{11} & h_{12} & \cdots & h_{1N} \\ h_{21} & h_{22} & \cdots & h_{2N} \\ \cdots & \cdots & \cdots & \cdots \\ h_{(N-K)1} & h_{(N-K)2} & \cdots & h_{(N-K)N} \end{pmatrix} \begin{pmatrix} g_{11} & g_{12} & \cdots & g_{1N} \\ g_{21} & g_{22} & \cdots & g_{2N} \\ \cdots & \cdots & \cdots & \cdots \\ g_{K1} & g_{K2} & \cdots & g_{KN} \end{pmatrix}^T = 0, \qquad (1)$$

що при простому підборі потребує спроб

$$\delta \le \upsilon \cdot \sum_{i=0}^{m+1} q^{(N-K)^2}, \qquad (2)$$

де υ - число варіантів побудови узагальненого каскадного коду. При невідомому порядку узагальненого каскадного коду - $\nu = 2^{n_1-1}$, при відомому порядку - $\nu = C_{n_1-1}^{m+1}$.

У разі використання як ключа параметрів еліптичної кривої - коефіцієнтів багаточлена, який задає вид кривої, для приховування коду досить приховати вид багаточлена кривої. Для даного випадку еліптичний код однозначно задається багаточленом

$$y^2z + a_1xyz + a_2yz^2 = x^3 + a_3x^2z + a_4xz^2 + a_5z. \qquad (3)$$

Таблиця 1 – Параметри каскадних теоретико-кодових схем, що рекомендуються до практичного використання для підвищення інформаційної прихованості та достовірності передачі даних

$GF(2^a)$	(n, k, d)	$m = 5$	$m = 6$	$m = 7$	$m = 8$	$m = 9$	$m = 10$
$GF(2^3)$	14, 8, 6	$l_M = 120$ $l_E = 252$ $l_K = 1680$ $l_{K^*} = 3900/75$	$l_M = 144$ $l_E = 294$ $l_K = 2016$ $l_{K^*} = 4680/90$	$l_M = 168$ $l_E = 336$ $l_K = 2352$ $l_{K^*} = 5460/105$	$l_M = 192$ $l_E = 378$ $l_K = 2688$ $l_{K^*} = 6240/120$	$l_M = 216$ $l_E = 420$ $l_K = 3024$ $l_{K^*} = 7020/135$	$l_M = 240$ $l_E = 462$ $l_K = 3360$ $l_{K^*} = 7800/150$
$GF(2^4)$	25, 13, 12	$l_M = 260$ $l_E = 600$ $l_K = 6500$ $l_{K^*} = 15880/100$	$l_M = 312$ $l_E = 700$ $l_K = 7800$ $l_{K^*} = 19056/120$	$l_M = 364$ $l_E = 800$ $l_K = 9100$ $l_{K^*} = 22232/140$	$l_M = 416$ $l_E = 900$ $l_K = 10400$ $l_{K^*} = 25408/160$	$l_M = 468$ $l_E = 1000$ $l_K = 11700$ $l_{K^*} = 28584/180$	$l_M = 520$ $l_E = 1100$ $l_K = 13000$ $l_{K^*} = 31760/200$
$GF(2^5)$	44, 23, 21	$l_M = 575$ $l_E = 1320$ $l_K = 25300$ $l_{K^*} = 61625/125$	$l_M = 690$ $l_E = 1540$ $l_K = 30360$ $l_{K^*} = 73950/150$	$l_M = 805$ $l_E = 1760$ $l_K = 35420$ $l_{K^*} = 86275/175$	$l_M = 920$ $l_E = 1980$ $l_K = 40480$ $l_{K^*} = 98600/200$	$l_M = 1035$ $l_E = 2200$ $l_K = 45540$ $l_{K^*} = 110925/225$	$l_M = \mathit{1150}$ $l_E = \mathit{2420}$ $l_K = \mathit{50600}$ $l_{K^*} = \mathit{123250/250}$
$GF(2^6)$	81, 42, 39	$l_M = 1260$ $l_E = \mathit{2916}$ $l_K = 102060$ $l_{K^*} = 249750/150$	$l_M = 1516$ $l_E = 3402$ $l_K = 122472$ $l_{K^*} = \mathit{299700}/180$	$l_M = 1764$ $l_E = 3888$ $l_K = 142884$ $l_{K^*} = 349650/210$	$l_M = 2016$ $l_E = 4374$ $l_K = 163296$ $l_{K^*} = 399600/240$	$l_M = 2268$ $l_E = 4860$ $l_K = 183708$ $l_{K^*} = 449500/270$	$l_M = 2520$ $l_E = 5346$ $l_K = 204120$ $l_{K^*} = 499500/300$

Це однорідний багаточлен з п'ятьма невідомими, отже, для приховування еліптичного коду досить приховати від противника п'ять коефіцієнтів у виразі (3). У цьому випадку об'єм ключа (у бітах) зворотного відображення задається виразом

$$l_{K^*} = 5 \cdot \sum_{i=1}^{m+1} a_i \ .$$

Число переборів, яке необхідне противнику для злому ключа зворотного відображення каскадної теоретико-кодової схеми, визначається виразом

$$\delta^* \geq 2^{5 \cdot \sum_{i=1}^{m+1} a_i} .$$

У таблиці 2 наведені результати дослідження стійкості розроблених каскадних теоретико-кодових схем із замаскованими алгеброгеометричними кодами на зовнішньому ступені узагальненого каскадного коду порядку m = 5-10. Дані характеризують безпечний час роботи даного криптоалгоритму $T_{БК}$ і вірогідність правильного відновлення ключа шифрування P_K при спробі противника розкрити матрицю H, а також безпечний час $T_{БК*}$, що характеризує час безпечної роботи за умови спроби противника злому ключа зворотного відображення (п'ять коефіцієнтів) і вірогідність його відновлення P_{K*} для каскадних теоретико-кодових схем, що рекомендуються.

Таким чином, як показали проведені дослідження, застосування теоретико-кодових схем дозволяє ефективно забезпечити інформаційну прихованість передаваних повідомлень і протистояти можливим атакам противника.

Проведемо оцінку часової та ємнісної складності розроблених алгоритмів формування та декодування кодограм в каскадних теоретико-кодових схемах захисту інформації [7].

Для формування кодограми в каскадній теоретико-кодовій схемі необхідно виконати кодування $m + 1$ кодами зовнішнього та внутрішнього ступенів. Для кодування всіма кодами зовнішнього ступеня методом множення матриць необхідно виконати $n_2 \cdot \sum_{i=1}^{m+1} b_i = n_2 \cdot k$ операцій множення та складання елементів над полями $GF(2^{a_i})$.

Для кодування всіма кодами внутрішнього ступеня методом множення матриць необхідно виконати $n_2 \cdot n_1 \cdot \sum_{i=1}^{m} a_i$ операцій множення та складання двійкових елементів.

Якщо припустити, що одна операція складання/множення двох елементів з $GF(2^{a_i})$ еквівалентна a_i операціям складання/множення двійкових елементів, тоді результуюча часова складність алгоритму формування кодограми визначатиметься виразом

$$S_B = n_2 \cdot \sum_{i=1}^{m+1} a_i \cdot b_i + n_2 \cdot n_1 \cdot \sum_{i=1}^{m} a_i = n_2 \cdot k + n_2 \cdot n_1 \cdot \sum_{i=1}^{m} a_i \ . \qquad (4)$$

Таблиця 2 – Результати дослідження стійкості розроблених каскадних теоретико-кодових схем

$GF(2^a)$		$m = 5$	$m = 6$	$m = 7$	$m = 8$	$m = 9$	$m = 10$
$GF(2^3)$	P_K	$2{,}5 \cdot 10^{-38}$	$2{,}4 \cdot 10^{-39}$	$2{,}2 \cdot 10^{-40}$	$2 \cdot 10^{-41}$	$1{,}7 \cdot 10^{-42}$	$1{,}5 \cdot 10^{-43}$
	$T_{БК}$	$7{,}8 \cdot 10^{15}$ років	$7{,}5 \cdot 10^{16}$ років	$6{,}8 \cdot 10^{17}$ років	$6{,}2 \cdot 10^{18}$ років	$5{,}3 \cdot 10^{19}$ років	$4{,}7 \cdot 10^{20}$ років
	P_{K*}	$3{,}8 \cdot 10^{-22}$	$1{,}2 \cdot 10^{-27}$	$4 \cdot 10^{-31}$	$1{,}3 \cdot 10^{-36}$	$4{,}3 \cdot 10^{-40}$	$1{,}4 \cdot 10^{-45}$
	$T_{БК*}$	1,2 років	37500 років	$1{,}3 \cdot 10^{9}$ років	$4{,}1 \cdot 10^{13}$ років	$1{,}3 \cdot 10^{18}$ років	$4{,}4 \cdot 10^{22}$ років
$GF(2^4)$	P_K	$1{,}2 \cdot 10^{-181}$	$2{,}3 \cdot 10^{-182}$	$4{,}2 \cdot 10^{-183}$	$7{,}6 \cdot 10^{-184}$	$1{,}4 \cdot 10^{-186}$	$2{,}4 \cdot 10^{-187}$
	$T_{БК}$	$3{,}7 \cdot 10^{158}$ років	$7{,}2 \cdot 10^{159}$ років	$1{,}3 \cdot 10^{161}$ років	$2{,}4 \cdot 10^{162}$ років	$4{,}4 \cdot 10^{163}$ років	$7{,}5 \cdot 10^{164}$ років
	P_{K*}	$1{,}3 \cdot 10^{-30}$	$1{,}3 \cdot 10^{-36}$	$1{,}4 \cdot 10^{-42}$	$1{,}5 \cdot 10^{-48}$	$1{,}5 \cdot 10^{-54}$	$1{,}6 \cdot 10^{-60}$
	$T_{БК*}$	$4 \cdot 10^{7}$ років	$4{,}1 \cdot 10^{13}$ років	$4{,}3 \cdot 10^{19}$ років	$4{,}5 \cdot 10^{25}$ років	$4{,}8 \cdot 10^{31}$ років	$5 \cdot 10^{37}$ років
$GF(2^5)$	P_K	$\approx 10^{-673}$	$\approx 10^{-675}$	$\approx 10^{-677}$	$\approx 10^{-679}$	$\approx 10^{-681}$	$\approx 10^{-683}$
	$T_{БК}$	$\approx 10^{651}$ років	$\approx 10^{653}$ років	$\approx 10^{655}$ років	$\approx 10^{657}$ років	$\approx 10^{659}$ років	$\approx 10^{661}$ років
	P_{K*}	$4{,}2 \cdot 10^{-37}$	$1{,}4 \cdot 10^{-45}$	$4{,}8 \cdot 10^{-52}$	$1{,}6 \cdot 10^{-60}$	$5{,}4 \cdot 10^{-67}$	$1{,}8 \cdot 10^{-75}$
	$T_{БК*}$	$1{,}3 \cdot 10^{15}$ років	$4{,}5 \cdot 10^{22}$ років	$1{,}5 \cdot 10^{30}$ років	$5 \cdot 10^{37}$ років	$1{,}7 \cdot 10^{45}$ років	$5{,}6 \cdot 10^{52}$ років
$GF(2^6)$	P_K	$\approx 10^{-2748}$					
	$T_{БК}$	$\approx 10^{2726}$ років					
	P_{K*}	$1{,}4 \cdot 10^{-45}$	$1{,}5 \cdot 10^{-54}$	$1{,}6 \cdot 10^{-63}$	$1{,}8 \cdot 10^{-72}$	$1{,}9 \cdot 10^{-81}$	$2 \cdot 10^{-90}$
	$T_{БК*}$	$4{,}5 \cdot 10^{22}$ років	$4{,}8 \cdot 10^{31}$ років	$5{,}1 \cdot 10^{40}$ років	$5{,}5 \cdot 10^{49}$ років	$5{,}9 \cdot 10^{58}$ років	$6{,}4 \cdot 10^{67}$ років

Спростимо отриманий вираз. Вважаємо, що $\forall a_i = \frac{n_1}{m+1}$, $n_2 = n_1 = \sqrt{n}$, $k = \frac{n}{2}$. Тоді, після підстановки в (4) отримаємо:

$$S_B = n_2 \cdot k + n_2 \cdot n_1 \cdot \sum_{i=1}^{m} a_i = \frac{n \cdot \sqrt{n}}{2} + \frac{m \cdot n \cdot \sqrt{n}}{m+1} = \left(\frac{1}{2} + \frac{m}{m+1}\right) \cdot n \cdot \sqrt{n} .$$

Оцінимо ємнісну складність алгоритмів формування кодограми. Для кодування всіма кодами зовнішнього ступеня методом множення матриць необхідно зберігати породжувальні матриці всіх кодів другого ступеня. Для цього необхідно

$$n_2 \cdot \sum_{i=1}^{m+1} b_i \cdot a_i = n_1 \cdot k$$

двійкових елементів пам'яті. Для кодування всіма кодами внутрішнього ступеня методом множення матриць необхідно зберігати трикутну матрицю H_0 порядку n_1, тобто необхідно $\frac{n_1^2}{2}$ двійкових елементів пам'яті. Ємнісна складність

$$S_E = n_2 \cdot k + \frac{n_1^2}{2} \qquad (5)$$

двійкових елементів пам'яті. Спростимо, як і раніше, отриманий вираз. Вважаємо, що

$$n_2 = n_1 = \sqrt{n} , \; k = \frac{n}{2} .$$

Тоді після підстановки в (5) маємо

$$S_E = \frac{n \cdot \sqrt{n}}{2} + \frac{n}{2} = \frac{1}{2}\left(\sqrt{n} + 1\right) \cdot n \quad .$$

За умови попереднього введення та підготовки ключових даних, декодування кодограми полягає в знятті дії матриць маскування та декодуванні кодового слова узагальненого каскадного коду.

Всього для зняття дії всіх матриць $\Lambda^i = P^i \cdot D^i$ і X^i буде потрібно $n_2^2(m+1) + \sum_{i=1}^{m+1} b_i^2 \cdot a_i$ часових інтервалів. Ємнісна складність складе $n_2{}^2 + \sum_{i=1}^{m+1} b_i{}^2 \cdot a_i$ двійкових елементів пам'яті. Аналіз алгоритму декодування кодового слова узагальненого каскадного коду показує, що складність його реалізації як функція розміру завдання визначається сумою труднощів реалізації алгоритмів декодування кодами зовнішнього і внутрішнього ступенів узагальненого каскадного коду. З урахуванням складності реалізації операцій над елементами з $GF(2^{a_i})$ тимчасова складність декодування кодового слова узагальненого каскадного коду

складе $\sum_{i=1}^{m+1}({t_{1i}}^2 + a_i \cdot t_{2i}^2)$ тимчасових інтервалів, де t_{1i} і t_{2i} – виправна здатність кодів першого та другого ступенів, відповідно. Ємнісна складність складе ${n_2}^2 + \sum_{i=1}^{m+1} {b_i}^2 \cdot a_i$ двійкових елементів пам'яті.

З урахуванням складності зняття дії матриць маскування остаточні вирази оцінки часової та ємнісної складності алгоритмів декодування запишуться у такому вигляді:

$$S_B = n_2^2(m+1) + \sum_{i=1}^{m+1}\left({b_i}^2 \cdot a_i + {t_{1i}}^2 + a_i \cdot {t_{2i}}^2\right), \qquad (6)$$

$$S_E = {n_2}^2 + \sum_{i=1}^{m+1}\left({b_i}^2 \cdot a_i + {t_{1i}}^2 + a_i \cdot {t_{2i}}^2\right). \qquad (7)$$

Вважаємо, що $\forall a_i = \frac{n_1}{m+1}$, $\forall \mathrm{t}_{2i} = \frac{n_2}{4}$, $n_2 = n_1 = \sqrt{n}$. Тоді після підстановки в (6) і (7) отримаємо:

$$S_B = \frac{17 \cdot n \cdot (m+1)}{16} + \frac{5 \cdot n \cdot \sqrt{n}}{16},$$

$$S_E = n + \frac{n \cdot (m+1)}{16} + \frac{5 \cdot n \cdot \sqrt{n}}{16}.$$

В таблиці 3 представлені результати дослідження складності реалізації алгоритмів формування S_B, S_E і декодування кодограм S_{B*}, S_{E*} в пропонованих каскадних теоретико-кодових схемах. Для порівняння в таблиці наведені дані труднощі реалізації алгоритмів формування $S_{B\epsilon}$, $S_{E\epsilon}$ і декодування кодограм $S_{B\epsilon}$, $S_{E\epsilon}$ еквівалентним двійковим лінійним блоковим *(n, k, d)* кодом.

Аналіз даних, наведених в таблиці, показує, що для коротких кодограм (довжиною в сотні символів) виграш у складності реалізації алгоритмів кодування і декодування складає один - два порядки.

При зміні порядку узагальненого каскадного коду складність реалізації алгоритмів декодування змінюється слабо, що практично не робить істотного впливу на остаточний вибір параметрів каскадної теоретико-кодової схеми.

ВИСНОВКИ

Таким чином, як показали проведені дослідження, практичне застосування каскадних теоретико-кодових схем дозволяє ефективно забезпечити імовірнісно-часові показники інформаційної прихованості повідомлень, які передаються (безпечний час $T_B > 200$ років, вірогідність розкриття ключових даних $P_K < 10^{-25} \div 10^{-35}$), і протистояти можливим атакам противника.

Дослідження часової і ємнісної складності запропонованих схем показало, що їх реалізація для коротких кодограм (декілька сотень бітів) значно (на один - два порядки) простіша порівняно з традиційними кодовими конструкціями та її можна порівняти з широковідомими блоково-симетричними криптоалгоритмами.

Таблиця 3 – Залежності складності реалізації алгоритмів формування і декодування кодограм в запропонованих каскадних теоретико-кодових схемах

$GF(2^a)$		$m = 5$	$m = 6$	$m = 7$	$m = 8$	$m = 9$	$m = 10$
	$S_B/ S_{BЄ}$	5334/31752	6841/43218	8469/56448	10207/71442	12050/88200	13993/106722
	$S_{B*}/ S_{BЄ*}$	2857/79380	3762/108045	4781/141120	5911/178605	7152/220500	8503/266805
	$S_E/ S_{EЄ}$	2126/31752	2667/43218	3247/56448	3864/71442	4514/88200	5196/106722
	$S_{E*}/ S_{EЄ*}$	1597/79380	1998/108045	2429/141120	2887/178605	3372/220500	3883/266805
$GF(2^3)$	$S_B/ S_{BЄ}$	19596/180000	25135/245000	31113/320000	37500/405000	44272/500000	51408/605000
$GF(2^4)$	$S_{B*}/ S_{BЄ*}$	8418/450000	10994/612500	13871/800000	17044/1012500	20507/1250000	24257/1512500
	$S_E/ S_{EЄ}$	7648/180000	9610/245000	11714/320000	13950/405000	16311/500000	18791/605000
	$S_{E*}/ S_{EЄ*}$	5418/450000	6794/612500	8271/800000	9844/1012500	11507/1250000	13257/1512500
	$S_B/ S_{BЄ}$	63944/871200	82017/1185800	101525/1548800	122367/1960200	144465/2420000	167750/2928200
$GF(2^5)$	$S_{B*}/ S_{BЄ*}$	23402/2178000	30339/2964500	38034/3872000	46466/4900500	55622/6050000	65486/7320500
	$S_E/ S_{EЄ}$	24639/871200	30987/1185800	37798/1548800	45042/1960200	52695/2420000	60734/2928200
	$S_{E*}/ S_{EЄ*}$	16802/2178000	21099/2964500	25714/3872000	30626/4900500	35822/6050000	41286/7320500
	$S_B/ S_{BЄ}$	209952/4251528	269294/5786802	333344/7558272	401777/9565938	4743320/11809800	550785/14289858
$GF(2^6)$	$S_{B*}/ S_{BЄ*}$	67797/10628820	87311/14467005	108808/18895680	132226/23914845	157515/29524500	184631/35724645
	$S_E/ S_{EЄ}$	80190/4251528	100915/5786802	123160/7558272	146827/9565938	171834/11809800	198113/14289858
	$S_{E*}/ S_{EЄ*}$	53217/10628820	66899/14467005	81592/18895680	97234/23914845	113775/29524500	131171/35724645

SUMMARY

There are under consideration the quantitative indices of information secrecy estimate (cryptographical durability), time and volumetrical complete of the cascade theoretic – code schemes with the application of algebra – geometrical code of external degree.

СПИСОК ЛІТЕРАТУРИ

1. Кузнецов А.А., Грабчак В.И., Евсеев С.П. Каскадные кодовые схемы защиты информации // Системи обробки інформації. – 2005 – Вип. 9 (49). – С. 206 – 211.
2. Захист інформації в комп'ютерних системах від несанкціонованого доступу / За ред. С.Г. Лаптєва. – К., 2001. – 321 с.
3. Шеннон К. Теория связи в секретных системах // К. Шеннон. Работы по теории информации и кибернетике. – М.: Изд-во иностранной литературы, 1963. – С. 333–402.
4. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Издательство ТРИУМФ, 2003. – 816 с.
5. Блох Э.Л., Зяблов В.В. Обобщенные каскадные коды. – М.: Связь, 1976. – 240с.
6. Кузнецов А.А., Евсеев С.П., Кужель И.Е., Грабчак В.И. Криптоанализ секретных систем, построенных с использованием алгебраических блоковых кодов. // Системи обробки інформації. – 2005 – Вип. 8(48). – С. 209 –216.
7. Кузнецов А.А., Грабчак В.И. Алгоритмы формирования и декодирования кодограмм в каскадных теоретико-кодовых схемах. // Проблеми інформатики і моделювання: Матеріали Шостої міжнародної науково-технічної конференції. – Харків: НТУ „ХПІ", 2006. – С. 15.

М.М. Ляпа, канд. техн. наук, доцент
Військовий інститут РВ і А Сумського державного університету

В.М. Лисенко, канд. техн. наук, доцент
Військовий інститут РВ і А Сумського державного університету

В.І. Грабчак
Військовий інститут РВ і А Сумського державного університету

О.В. Лисенко
Сумський державний університет

Надійшла до редакції 20 березня 2007 р.