

*Н.В. ПРЕВИСОКОВА*, канд. техн. наук, доц., Прикарпатський національний університет імені Василя Стефаника, Івано-Франківськ

## **АНАЛІЗ ЕФЕКТИВНОСТІ МЕТОДУ КОДУВАННЯ ІНФОРМАЦІЇ НА ОСНОВІ ОРТОГОНАЛЬНОГО ПЕРЕТВОРЕННЯ ГАЛУА**

Пропонується метод кодування інформації на основі ортогонального перетворення в системах функцій Галуа. Визначено ефективність кодування на основі перетворення Галуа та здійснено порівняльний аналіз з іншими методами кодування на основі перетворень та методом імпульсно-кової модуляції в задачах зменшення надлишковості інформації. Іл.: 1. Табл.: 1. Бібліогр.: 9 назв.

**Ключові слова:** кодування на основі перетворення, ефективність кодування, функцій Галуа, ортогональне перетворення, імпульсно-кова модуляція.

**Постановка проблеми.** Швидкий розвиток комп'ютерних і телекомунікаційних систем призводить до виникнення необхідності постійного розвитку, вдосконалення та модифікації методів і алгоритмів зменшення надлишковості інформації [1, 2].

Особливість сучасних методів обробки інформаційних потоків полягає в пошуку і застосуванні найбільш ефективних перетворень, а також методів кодування інформації, і розглядати ці завдання необхідно комплексно.

**Аналіз літератури.** Відома група методів зменшення надлишковості інформації заснована на застосуванні до інформаційного потоку деякого ортогонального перетворення, а також подальшого квантування і кодування [1 – 3]. Ступінь зменшення надлишковості інформації та якість обробки залежать від обох цих етапів і від їх узгодженості з типом інформаційного потоку, який характеризується статистичними властивостями останнього.

Найпоширенішим методом кодування є імпульсно-кова модуляція, яка використовується як основа для порівняння інших методів і схем [2 – 6].

Метод кодування інформації на основі перетворення суттєво відрізняється від імпульсно-кової модуляції, яка застосовується безпосередньо до інформаційного потоку. Кодування на основі перетворення є непрямим методом, при якому до інформаційного потоку застосовується унітарне математичне перетворення, а отримані в результаті коефіцієнти перетворення квантуються і кодуються [1, 3], що дозволяє ефективно розв'язати задачі зменшення надлишковості при зберіганні та передаванні інфопотоків. Переваги методу кодування з

перетворенням над імпульсно-ковою модуляцією залежно від властивостей заданого вхідного вектора досліджені в літературі [2 – 6].

Оптимальне для кодування інформаційних потоків перетворення Карунена-Лоева [1 – 3] є єдиним унітарним перетворенням, в якому досягається повна декореляція коефіцієнтів, потребує знаходження власних значень та власних векторів для кожного вхідного інфопотоку, тому складно реалізується на практиці [1 – 3]. Це зумовлює необхідність пошуку, побудови та дослідження нових базисів, які дозволяють наблизити показники ефективності до оптимальних.

Ефективність застосування відомих у класі теоретико-числових ортогональних перетворень Уолша та Хаара досліджено в роботах [1, 3]. Водночас показано, що дані перетворення не забезпечують оптимального розв'язання задач обробки і залежать від особливостей та характеристик аналізованих інформаційних потоків. У роботі [7] розроблено одновимірне ортогональне перетворення на основі системи функцій Галуа [8], властивість рекурсивного формування яких дозволяє використовувати апарат циркулянтних перетворень і зменшити обчислювальну складність алгоритмів. Водночас дослідження методу кодування на основі даного перетворення не проводилось, що обмежує області ефективного застосування даного методу обробки інформації. Це зумовило необхідність вирішення задачі побудови ортогональних систем Галуа, виконання дискретних перетворень та кодування інформації на їх основі, а також визначення ефективності кодування з перетворенням порівняно з імпульсно-ковою модуляцією.

**Мета статті.** Дослідження та аналіз методу кодування інформації на основі ортогонального перетворення Галуа, визначення його ефективності та порівняння з іншими методами кодування на основі перетворень та імпульсно-ковою модуляцією в задачах зменшення надлишковості інформації для підвищення точності подання одновимірних інформаційних потоків.

**Кодування на основі перетворення.** Дискретне ортогональне перетворення виконується в системі  $N$  лінійно-незалежних (ортогональних) векторів  $\{\varphi_k(j)\}$  на інтервалі  $0 \leq j \leq N-1$ , яка називається базисом перетворення [1 – 3] і задовольняє властивість

$$\sum_{j=0}^{N-1} \varphi_k(j) \varphi_l(j) = \begin{cases} 1, & k = l, \\ 0, & k \neq l, \end{cases}$$

де  $j = 0, 1, \dots, N-1$  – змінна часу,  $k = 0, 1, \dots, N-1$ . Базисні вектори  $\{\varphi_k(j)\}$  є рядками матриці перетворення  $\Phi = [\varphi_k(j)]$  розміру  $N \times N$ .

У матричній формі дискретне перетворення вхідного вектора

відліків інформаційного потоку  $X$  розміру  $N$  у базисі, заданому матрицею  $\Phi$ , подається згідно

$$Y = \Phi X, \quad (1)$$

де  $Y$  – вектор коефіцієнтів перетворення.

Під кодуванням на основі перетворення розуміють квантування коефіцієнтів перетворення із наступним кодуванням, визначене у [2, 3]

$$\tilde{Y} = Q\{X\}.$$

Відновлення сигналу за квантованими коефіцієнтами вектора  $\tilde{Y}$  визначається як

$$\tilde{X} = \Phi^{-1}\tilde{Y}.$$

Квантування і кодування коефіцієнтів перетворення інформаційного потоку використовується для зменшення надлишковості з втратами.

Для оцінювання ефективності кодування на основі перетворення в заданому базисі використовується статистична модель вхідного сигналу [2, 3, 5, 6]. У даній моделі вхідний  $N$ -координатний вектор  $X$  розглядається як вибірка випадкового процесу. Елементи вектора  $X$  є реалізацією одновимірною марківського процесу першого порядку з нульовим математичним сподіванням, одиничною дисперсією, заданого коваріаційною матрицею  $C_X$ ,  $(i, j)$ -й елемент якої дорівнює  $\rho^{|i-j|}$ ,  $0 \leq \rho \leq 1$  – коефіцієнт кореляції між сусідніми елементами.

Для ортогонального перетворення (1) коваріаційна матриця  $C_Y$  вектора коефіцієнтів перетворення визначається як математичне сподівання  $C_Y = E[YY^T] = \Phi C_X \Phi^T = \{c_Y(i, j)\}$  [2, 3, 5, 6]. Елементи головної діагоналі матриці  $C_Y$  є дисперсіями спектральних компонент  $\sigma^2(i) = c_Y(i, i)$ .

Ефективність кодування інформаційного потоку  $X$  визначається квантуванням, характеристики якого залежать від функції щільності імовірності.

Одним із відомих методів оптимального квантування коефіцієнтів перетворення є процедура Ллойда-Макса [2, 5], що забезпечує мінімальне спотворення елементів вектора перетворення.

Показником ефективності кодування на основі перетворення (англ. transform coding) порівняно з імпульсно-кодуючою модуляцією є відношення середнього арифметичного дисперсій коефіцієнтів перетворення до їх середнього геометричного, яке відображає у скільки

разів менша похибка відновлення при кодуванні на основі перетворення порівняно з безпосередньою імпульсно-кодовою модуляцією [4, 6]

$$GTC = \frac{1}{N} \frac{\sum_{i=1}^N \sigma^2(i)}{\left(\prod_{i=1}^N \sigma^2(i)\right)^{1/N}}. \quad (2)$$

**Побудова базисів ортогональних перетворень Галуа.** Серед основних теоретико-числових базисів [8] дискретних ортогональних перетворень ортонормованими та повними є системи функцій Уолша та Хаара [1, 3].

Система функцій Уолша [3] визначається як добуток функцій Радемахера  $Rad(n, \theta) = \text{sign}(\sin(2^n \pi \theta))$  на інтервалі  $0 \leq \theta < 1$

$$Wal(i, \theta) = Rad(1, \theta)^{b_0} Rad(2, \theta)^{b_1} \dots Rad(n, \theta)^{b_{n-1}} = \prod_{k=0}^{n-1} (Rad(k+1, \theta))^{b_k},$$

де  $i = 0, 1, \dots, 2^n - 1$  – порядковий номер функції;  $i = b_{n-1}b_{n-2} \dots b_1b_0$  – подання в кодї Грея.

Система функцій Хаара  $Har(n, \theta, j)$  означається [3]

$$Har(n, \theta, l) = \begin{cases} 2^{\frac{n-1}{2}} \text{sign}(\sin 2^n \pi \theta), & l/2^{n-1} \leq \theta < (l+1)/2^{n-1}, \\ 0 & \text{при інших } \theta \in [0, 1), \end{cases}$$

де  $n = 0, 1, \dots, \log_2 N$ ;  $l = 0, 1, \dots, 2^{n-1} - 1$ , ( $l = 0$  при  $n = 0$ ).

Базисами дискретного ортогонального перетворення в системах функцій Галуа є повні ортогональні системи  $\{G(n, \theta, i)\}$  [7] різних порядків  $n$ , одержані із рекурсивних систем функцій Галуа [8].

Рекурсивні системи функцій Галуа  $\{Gal(n, \theta, i)\}$  [8] утворюються відповідно до породжуючого вектора поля Галуа  $GF(2^n)$ , елементами якого є коефіцієнти незвідного полінома  $p(x)$  характеристики 2 з коефіцієнтами із поля  $GF(2)$  (табл.1).

Наприклад, у полі  $GF(2^3)$  із початкових векторів  $(g_0, g_1, g_2) = (1, 1, 1)$  і  $(g_0, g_1, g_2) = (0, 0, 0)$  формуються чотири рекурсивні послідовності  $g_0, g_1, g_2, \dots, g_{2^n-2}$  за правилами, які відповідають

породжуючим векторам:  $(1, 0, 1, 1) \rightarrow g_{j+3} = g_j \oplus g_{j+2}; (1, 1, 0, 1) \rightarrow$   
 $\rightarrow g_{j+3} = g_j \oplus g_{j+1}; (1, 0, 1, \bar{1}) \rightarrow g_{j+3} = \overline{g_j \oplus g_{j+2}}; (1, 1, 0, \bar{1}) \rightarrow$   
 $\rightarrow g_{j+3} = \overline{g_j \oplus g_{j+1}}.$

Таблиця 1  
 Приклади поліномів  $p(x)$  характеристики 2 з коефіцієнтами із поля  $GF(2)$  та відповідні їм породжуючі вектори

$n$	Породжуючий поліном $p(x)$	Породжуючі вектори
3	$x^3 + x + 1$	$(1,0,1,1), (1,0,1,\bar{1})$
3	$x^3 + x^2 + 1$	$(1,1,0,1), (1,1,0,\bar{1})$
4	$x^4 + x + 1$	$(1,0,0,1,1), (1,0,0,1,\bar{1})$
4	$x^4 + x^3 + 1$	$(1,1,0,0,1), (1,1,0,0,\bar{1})$
4	$x^4 + x^2 + 1$	$(1,0,1,0,1), (1,0,1,0,\bar{1})$
5	$x^5 + x^2 + 1$	$(1,0,0,1,0,1), (1,0,0,1,0,\bar{1})$
5	$x^5 + x^3 + 1$	$(1,0,1,0,0,1), (1,0,1,0,0,\bar{1})$
6	$x^6 + x + 1$	$(1,0,0,0,0,1,1), (1,0,0,0,0,1,\bar{1})$
6	$x^6 + x^5 + 1$	$(1,1,0,0,0,0,1), (1,1,0,0,0,0,\bar{1})$

Кожна одержана послідовність містить підпослідовність із  $n-1$  елементів, які дорівнюють нулю  $(g_j, g_{j+1}, \dots, g_{j+n-2}) = (0, 0, \dots, 0)$ . Дана підпослідовність доповнюється ще одним нульовим елементом  $(g_j, g_{j+1}, \dots, g_{j+n-2}, 0)$  так, щоб довжина всієї утвореної послідовності, яка позначається  $\{v_j\}$ , становила  $N = 2^n$ ,  $j = 0, 1, \dots, N-1$ .

Функції рекурсивної системи  $\{Gal(n, \theta, i)\}$  в точках  $\theta = j/N$  інтервалу  $\theta \in [0; 1)$  визначаються із послідовності  $\{v_j\}$  та доозначаються до неперервних на інтервалах  $\theta \in [j/N; (j+1)/N)$ :

$$Gal(n, \theta, 0) = Gal(n, j/N, 0) = 1 - 2v_j,$$

$$Gal(n, \theta, i + 1) = Gal(n, \theta + 1/N, i),$$

де  $n = 1, 2, \dots$  – порядок функції;  $N = 2^n$  – кількість функцій у системі.

Оскільки  $v_j = 1$  або  $v_j = 0$ , то функції  $Gal(n, \theta, i) = \pm 1$ .

Ортогональні функції  $\{G(n, \theta, i)\}$  [7] одержують застосуванням процедури ортогоналізації Грама-Шміда [9] до функцій системи  $\{Gal(n, \theta, i)\}$ :

$$G(n, \theta, 0) = 1, \quad (3)$$

$$G(n, \theta, k + 1) = Gal(n, \theta, k) - \sum_{i=0}^k \frac{\langle Gal(n, \theta, k), G(n, \theta, i) \rangle}{\|G(n, \theta, i)\|_{L_2}^2} G(n, \theta, i), \quad (4)$$

де  $k = 0, 1, \dots, N - 1$  – порядковий номер функції;  $\|G(n, \theta, i)\|_{L_2}^2$  – норма в просторі інтегровних з квадратом функцій  $L_2[0,1]$ ;  $\langle Gal_m(n, \theta, k + 1), G(n, \theta, i) \rangle$  – скалярний добуток.

Таким чином, на основі породжуючих векторів полів  $GF(2^n)$  порядків  $n \geq 2$ , основна частина яких наведена у табл. 1, за формулами (3), (4) побудовано сімейство систем ортогональних функцій Галуа  $\{G(n, \theta, i)\}$  із  $N = 2^n$  функцій, які характеризуються порядком  $n$ .

**Ефективність кодування на основі перетворення Галуа.** Дискретне матричне ортогональне перетворення Галуа [7] одновимірного інформаційного потоку  $\{X(0), X(1), \dots, X(N - 1)\}$  визначається як добуток

$$Y = GX, \quad (5)$$

де  $Y = [Y(0), Y(1), \dots, Y(N - 1)]^T$  – транспонований вектор спектральних коефіцієнтів перетворення Галуа;  $X = [X(0), X(1), \dots, X(N - 1)]^T$  – траспонований вхідний вектор;  $G$  – матриця розміру  $N \times N$  значень ортогональних функцій Галуа в точках  $\theta = j / N$ .

У побудованих ортогональних базисах Галуа (3), (4) виконано перетворення (5), досліджено ефективність кодування на основі даного перетворення та здійснено порівняльний аналіз з кодуванням на основі перетворень Уолша і Хаара у задачах зменшення надлишковості інформаційних потоків. Дослідження перетворення здійснено на моделі вхідного одновимірного інформаційного потоку, яка застосовується для визначення ефективності перетворень і подана в першій частині статті.

З метою визначення ефективності кодування на основі розробленого перетворення обчислено коефіцієнт  $GTC$  згідно (2), який відображає в скільки разів менша середньоквадратична похибка відновлення інформаційного потоку при кодуванні на основі перетворення порівняно з використанням імпульсно-кодової модуляції. Обчислені для перетворень Уолша ( $GTC_{wal}$ ), Хаара ( $GTC_{har}$ ) та Галуа з

породжуючими векторами  $(1, 0, 1, 1)$  та  $(1, 1, 0, 1)$  ( $GTC_{gal(1,0,1,1)}$  та  $GTC_{gal(1,1,0,1)}$ ) значення показника  $GTC$  в залежності від коефіцієнта кореляції  $\rho$  між сусідніми елементами вибірки розміру  $N = 8$  та розміру  $N = 64$  наведено на рис.

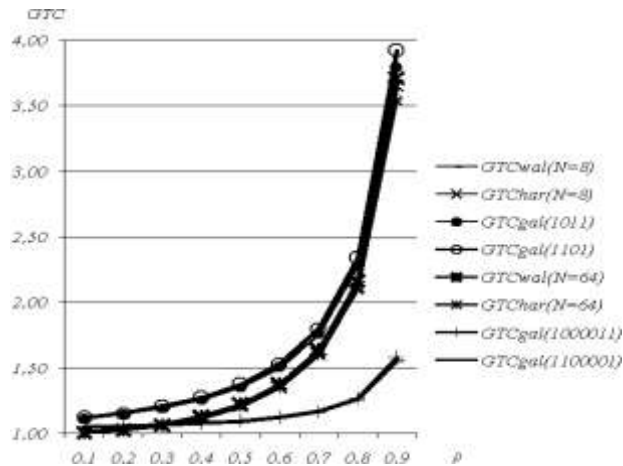


Рис. Відношення похибок відновлення при кодуванні на основі перетворення розмірів  $N = 8$  та  $N = 64$  та імпульсно-кодової модуляції

На основі виконаних обчислень показника  $GTC$  та аналізу рис. можна зробити висновки, що для всіх досліджених довжин перетворень  $GTC_{gal} > 1$ , що визначає більшу ефективність кодування на основі перетворення Галуа порівняно з імпульсно-ковою модуляцією. Використання ортогонального перетворення Галуа розміру  $N = 8$  для всіх досліджених значень  $\rho$  і для векторів розмірів від  $N = 16$  до  $N = 256$  із коефіцієнтом  $0,1 \leq \rho \leq 0,3$  забезпечує вищий показник  $GTC$ . З обчислених відношень  $k_{GTCGW} = GTC_{gal} / GTC_{wal}$ ,  $k_{GTCGH} = GTC_{gal} / GTC_{char}$  та одержаних оцінок  $1,1 < k_{GTCGW} < 1,14$ ,  $1,1 < k_{GTCGH} \leq 1,14$  слідує, що застосування методу кодування на основі ортогонального перетворення Галуа порівняно з перетвореннями Уолша та Хаара дозволяє зменшити середньоквадратичну похибку відновлення інформаційних потоків у 1,1 – 1,14 разів.

**Висновки.** Запропоновано і здійснено дослідження ефективності методу кодування одновимірних інформаційних потоків на основі перетворення в ортогональних системах Галуа, породжених різними

векторами полів  $GF(2^n)$ . Пропонований метод полягає в квантуванні і кодуванні коефіцієнтів ортогонального перетворення Галуа.

Результати проведених досліджень дають можливість зробити висновок, що запропонований метод кодування інформації на основі ортогонального перетворення Галуа порівняно із відомими перетвореннями та методом імпульсно-кової модуляції дозволяє збільшити точність відновлення даних і може використовуватись для кодування та зменшення надлишковості інформаційних потоків.

**Список літератури:** 1. Сэлмон Д. Сжатие данных, изображений и звука / Д. Сэлмон. – М.: Техносфера, 2004. – 368 с. 2. Akansu N. Multiresolution Signal Decomposition: Transforms, Subbands, and Wavelets (Second Edition) / N. Akansu, R.A. Haddad. – San Diego, USA: Academic Press, 2001. – 499 p. 3. Ахмед Н. Ортогональные преобразования при обработке цифровых сигналов / Н. Ахмед, К.Р. Рао. – М.: Связь, 1980. – 248 с. 4. O. Yilmaz. Quantization of Eigen Subspace for Sparse Representation / O. Yilmaz, A.N. Akansu // IEEE Transactions on Signal Processing. – 2015. – Vol. 63. – №. 14. – P. 3616-3625. 5. Torun M.U. An Efficient Method to Derive Explicit KLT Kernel for First-Order Autoregressive Discrete Process / M.U. Torun, A.N. Akansu // IEEE Trans. on Signal Processing. – Aug. 2013. – Vol. 61. – №. 15. – P. 3944–3953. 6. Гнатив Л.А. Методы синтеза эффективных ортогональных преобразований высокой и низкой корреляции и их быстрых алгоритмов для кодирования и сжатия цифровых изображений / Л.А. Гнатив, Е.С. Шевчук // Кибернетика и системный анализ. – 2002. – № 6. – С. 104–117. 7. Превисокова Н.В. Метод обробки інформації на основі дискретного ортогонального перетворення Галуа / Н.В. Превисокова // Вісник Хмельницького нац. ун-ту. Технічні науки. – 2010. – № 2 (146). – С. 149–156. 8. Петришин Л.Б. Теоретичні основи перетворення форми та цифрової обробки інформації в базисі Галуа: Навчальний посібник / Петришин Л.Б. – К.: ІзіМН МОУ, 1997. – 237 с. 9. Солодовников А.И. Основы теории и методы спектральной обработки информации / А.И. Солодовников, А.М. Спиваковский. – Л.: Изд-во Ленингр. ун-та, 1986. – 272 с.

#### **References:**

1. Salomon, D. (2004), "A Guide to Data Compression", Tehnosfera, Moscow, 368 p.
2. Akansu, N. Haddad, R.A. (2001), *Multiresolution Signal Decomposition: Transforms, Subbands, and Wavelets*. 2nd ed., Academic Press, San Diego, 499 p.
3. Ahmed, N. and Rao, K. (1980), *Orthogonal Transforms for Digital Signal Processin*, Svjaz, Moscow, 248 p.
4. Yilma, O. and Akansu, A.N. (2015), "Quantization of Eigen Subspace for Sparse Representation", *IEEE Transactions on Signal Processing*, Vol. 63, No. 14, pp. 3616-3625.
5. Torun, M.U. and Akansu, A.N. (2013), "An Efficient Method to Derive Explicit KLT Kernel for First-Order Autoregressive Discrete Process", *IEEE Trans. on Signal Processing*, Vol. 61, No. 15, pp. 3944-3953.
6. Gnativ, L.A. and Shevchuk, E.S. (2002), "Methods used for synthesis of efficient orthogonal transforms of high and low correlation and their fast algorithms for digital image coding and compression", *Cybernetics and Systems Analysis*, No. 6, pp. 104–117.
7. Prevysokova, N.V., (2010), "The method of information processing based on discrete orthogonal transformation Galois", *Herald of Khmelnytskyi national university*, No. 2 (146), pp.149–156.
8. Petryshyn, L.B. (1997), *Theoretical Foundations conversion and digital forms of information processing in the base of Galois*, IziMN MOU, Kiev, 237 p.



9. Solodovnikov, A.I. and Spivakovski, A.M. (1986), *Fundamentals of the theory and methods of information spektralnoy obrabotku*, Leningrad University Publishing, Leningrad, 272 p.

*Надійшла (received) 30.03.2016*

*Статью представил д.т.н., проф. завідувач кафедри комп'ютерної інженерії та електроніки ДВНЗ "Прикарпатський національний університет ім. Василя Стефаника" Козут І.Т.*

Prevysokova Natalija, Cand. Tech. Sci., Docent  
Vasyl Stefanyk Precarpathian National University  
Str. Shevchenko, 57, Ivano-Frankivsk, Ukraine, 76000  
Tel.: (034) 259-60-86, e-mail: nataliia.prevysokova@pu.if.ua

УДК 621.391, 519.651

**Аналіз ефективності методу кодування інформації на основі ортогонального перетворення Галуа / Н.В. Превисокова // Вісник НТУ "ХПІ". Серія: Інформатика та моделювання. – Харків: НТУ "ХПІ". – 2016. – № 21 (1193). – С. 92 – 101.**

Пропонується метод кодування інформації на основі ортогонального перетворення в системах функцій Галуа. Визначено ефективність кодування на основі перетворення Галуа та здійснено порівняльний аналіз з іншими методами кодування на основі перетворень та методом імпульсно-кової модуляції в задачах зменшення надлишковості інформації. Іл.: 1. Табл.: 1. Бібліогр.: 9 назв.

**Ключові слова:** кодування на основі перетворення, ефективність кодування, функції Галуа, ортогональне перетворення, імпульсно-кова модуляція.

УДК 621.391, 519.651

**Анализ эффективности метода кодирования информации на основе ортогонального преобразования Галуа / Н.В. Превисокова // Вестник НТУ "ХПИ". Серія: Інформатика и моделирование. – Харьков: НТУ "ХПИ". – 2016. – № 21 (1193). – С. 92 – 101.**

Предлагается метод кодирования информации на основе ортогонального преобразования в системах функций Галуа. Определена эффективность кодирования на основе преобразования Галуа и осуществлен сравнительный анализ с другими методами кодирования на основе преобразований и методом импульсно-кової модуляции в задачах уменьшения избыточности информации. Ил.: 1. Табл.: 1. Библиогр.: 9 назв.

**Ключевые слова:** кодирование на основе преобразования, эффективность кодирования, функции Галуа, ортогональное преобразование, импульсно-кова модуляция.

UDC 621.391, 519.651

**Efficiency analysis of the method transform coding information on the Galois functions base / N.V. Prevysokova // Herald of the National Technical University "KhPI". Subject issue: Information Science and Modelling. – Kharkov: NTU "KhPI". – 2016. – № 21 (1193). – P. 92 – 101.**

There have proposed method transform coding information on the Galois orthogonal functions base. A family of Galois orthogonal functions is formed and it is calculated orthogonal transform on this family base. The efficiency of Galois transform coding is calculated and comparative analysis with other transform coding methods and pulse code modulation is performed to solve the data compression problems. Figs.: 1. Tabl.: 1. Refs.: 9 titles.

**Keywords:** transform coding, efficiency of Galois transform, Galois functions, orthogonal transform, pulse code modulation.