

МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ  
Одеський національний політехнічний університет

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ  
МЕТОДИ В МОДЕЛЮВАННІ

INFORMATICS AND MATHEMATICAL  
METHODS IN SIMULATION

Том 1, номер 2

Volume 1, No. 2

Одеса – 2011  
Odesa - 2011

**Інформатика та математичні методи в моделюванні**

Науковий журнал

**Виходить** 4 рази на рік

**Заснований** Одеським національним політехнічним університетом у 2011 році

**Свідоцтво** про державну реєстрацію  
КВ № 17610 - 6460Р від 04.04.2011р.

**Головний редактор:** *Г.О. Оборський*

**Заступник головного редактора:**

*А.А. Кобозєва*

**Відповідальний редактор:** *І.І. Бобок*

**Редакційна колегія:**

*Т.О. Банах, П.І. Бідюк, Н.Д. Вайсфельд,  
А.Ф. Верлань, Г.М. Востров,  
Г.С. Гайворонська, О.Ф. Дащенко,  
В.Б. Дудикевич, Л.Є. Євтушик,  
М.Б. Копитчук, С.В. Ленков, Є.В. Малахов,  
А.Д. Мілка, С.А. Нестеренко,  
М.С. Никитченко, С.А. Положаєнко,  
О.В. Рибальський, В.Д. Русов, А.В. Усов,  
С.В. Філіппова, В.О. Хорошко, М.С. Яджак*

**Informatics and mathematical methods in simulation**

Scientific journal

**Published** 4 times a year

**Founded** by Odessa National Polytechnic University in 2011

**Certificate** of State Registration

КВ № 17610 - 6460Р of 04.04.2011

**Editor-in-chief:** *G.A. Oborsky*

**Associate editor:** *A.A. Kobozeva*

**Executive editor:** *I.I. Bobok*

**Editorial Board:**

*T. Banakh, P. Bidyuk, A. Daschenko,  
V. Dudykevich, L. Evtushik, S. Filippova,  
G. Gayvoronskaya, V. Horoshko,  
N. Kopytchuk, S. Lenkov, E. Malakhov,  
A. Milka, S. Nesterenko, N. Nikitchenko,  
S. Polozhaenko, V. Rusov, O. Rybalsky,  
A. Usov, N. Vaysfeld, A. Verlan, G. Vostrov,  
M. Yadzhak*

**Друкується** за рішенням редакційної колегії та Вченої ради Одеського національного політехнічного університету

**Оригінал-макет** виготовлено редакцією журналу

---

**Адреса редакції:** 1, проспект Шевченка, Одеса, 65044, Україна

Телефон: +38 048 734 8506

Web: <http://immm.opu.ua>

E-mail: [immm.ukraine@gmail.com](mailto:immm.ukraine@gmail.com)

**Editorial address:** 1, Ave. Shevchenko, Odessa, 65044, Ukraine

Tel.: +38 048 734 8506

Web: <http://immm.opu.ua>

E-mail: [immm.ukraine@gmail.com](mailto:immm.ukraine@gmail.com)

© **Одеський національний політехнічний університет, 2011**

---

## ЗМІСТ / CONTENTS

---

**А.А. Шумейко, Е.А. Шумейко**

О ПОСТРОЕНИИ АСИМПТОТИЧЕСКИ ОПТИМАЛЬНОЙ  
КУСОЧНО-ЛИНЕЙНОЙ РЕГРЕССИИ 99

**Р.В. Грищук**

ІЄРАРХІЧНА ДИФЕРЕНЦІАЛЬНО-ІГРОВА МОДЕЛЬ В ЗАДАЧАХ  
ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ 107

**С.А. Положаенко, С.Д. Кузниченко**

МОДЕЛИРОВАНИЕ ПРОЦЕССА ПРОПИТКИ ГРУНТА ЧЕРЕЗ  
ОСНОВАНИЕ ЗЕМЛЯНОГО ГИДРОТЕХНИЧЕСКОГО  
СООРУЖЕНИЯ 116

**Я.М. Николайчук, М.М. Касянчук, І.З Якименко, Т.М. Долинюк**

ТЕОРЕТИЧНІ ОСНОВИ ВИКОНАННЯ МОДУЛЯРНИХ ОПЕРАЦІЙ  
МНОЖЕННЯ ТА ЕКСПОНЕНЦІЮВАННЯ В ТЕОРЕТИКО –  
ЧИСЛОВОМУ БАЗИСІ КРЕСТЕНСОНА-РАДЕМАХЕРА 123

**В.В. Карпінець, Ю.Є. Яремчук**

ВИРІШЕННЯ ПРОБЛЕМИ ЗМЕНШЕННЯ РІВНЯ СПОТВОРЕНЬ  
ВЕКТОРНИХ ЗОБРАЖЕНЬ ВНАСЛІДОК ВБУДОВУВАННЯ  
ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ 131

**Leonid V. Verozub**

THE SIGNIFICANCE OF GEODESIC MAPPINGS OF RIEMANNIAN  
SPACES IN GRAVITATION THEORY 141

**Ф.И. Егоров, Е.О. Тискина, В.А. Хорошко**

ОПРЕДЕЛЕНИЕ ОПТИМАЛЬНОЙ ПЕРИОДИЧНОСТИ ФОРМ  
ОБСЛУЖИВАНИЯ В СЛОЖНОЙ СИСТЕМЕ 148

|                                                                                                                                               |            |
|-----------------------------------------------------------------------------------------------------------------------------------------------|------------|
| <b>М.П. Комар, И.О. Палий, Р.П. Шевчук, Т.Б. Федысив</b><br><b>НЕЙРОСЕТЕВОЙ ПОДХОД К ОБНАРУЖЕНИЮ СЕТЕВЫХ АТАК<br/>НА КОМПЬЮТЕРНЫЕ СИСТЕМЫ</b> | <b>156</b> |
| <b>О.И. Бодюл, И.В. Дубро, Е.С. Бодюл, А.В. Шаталов</b><br><b>К ВОПРОСУ О РАНЖИРОВАНИИ КРИТЕРИЕВ ОПАСНОСТИ<br/>ГАЛОГЕНОУГЛЕВОДОРОДОВ</b>      | <b>164</b> |
| <b>В.С. Ситников, Д.М. Шатохин</b><br><b>КОМБИНИРОВАННЫЙ АЛГОРИТМ ПОВЫШЕНИЯ ВЕРОЯТНОСТИ<br/>РАСПОЗНАВАНИЯ ДВУМЕРНЫХ ИЗОБРАЖЕНИЙ</b>           | <b>174</b> |
| <b>А.А. Кобозева</b><br><b>НОВИЙ ПІДХІД ДО ПРОБЛЕМИ СТЕГАНОВАНАЛІЗУ</b>                                                                       | <b>183</b> |

# О ПОСТРОЕНИИ АСИМПТОТИЧЕСКИ ОПТИМАЛЬНОЙ КУСОЧНО-ЛИНЕЙНОЙ РЕГРЕССИИ

А.А. Шумейко<sup>1</sup>, Е.А. Шумейко<sup>2</sup>

<sup>1</sup> ОКВУЗ «Институт предпринимательства «Стратегия»,  
ул. Гагарина, 38, Желтые Воды, 52201, Украина; e-mail: shumeiko\_a@ukr.net

<sup>2</sup> Universität Konstanz,  
Universitätsstraße 10, D-78464 Konstanz, Germany; e-mail: Yevgen.Shumeyko@uni-konstanz.de

В работе предложена конструкция кусочно-линейной регрессии, асимптотически совпадающей с наилучшей. Доказано, что задача построения кусочно-линейной регрессионной модели сводится к построению кубического интерполяционного сплайна от второй первообразной искомой функции.

**Ключевые слова:** сплайн-регрессия, кусочно-линейная регрессия, оптимизация разбиений

## Введение

Нельзя преувеличить сферу использования регрессионных моделей. Как правило, в роли используемой регрессионной функции берется конструкция, исходящая из известных физических, экономических или каких-то других законов, в зависимости от решаемой задачи. В случае если априорной информации недостаточно для установления закона, описывающего исходные данные, используется какой-либо универсальный аппарат. Как правило, для такого рода задач используют сплайны. Одной из наиболее распространенных сплайновых моделей являются ломаные или кусочно-линейные функции. Задаче построения сплайн-регрессионных моделей посвящено достаточно много работ (см, например, [1], [2], [3]). Но, как правило, регрессионная модель строится для заданного фиксированного разбиения, что существенно сужает задачу, так как оптимизация узлов регрессионной модели приводит не только к уменьшению ошибки, полученной при использовании данной регрессионной модели, но и может использоваться для установления точки изменения закона распределения исходных данных, что очень важно для задач диагностики. Для разного вида сплайнов задачи оптимизации узлов рассматривались, например, в работах [4], [5].

## Постановка задачи и цель исследований

Пусть  $\Delta_n : 0 = t_0 < t_1 < \dots < t_{n-1} < t_n = T$  – произвольное разбиение отрезка  $[0, T]$  и  $S_r(\Delta_n)$  – множество всех сплайнов порядка  $r$  минимального дефекта по разбиению  $\Delta_n$ , то есть множество функций с непрерывной  $r-1$ -й производной на  $[0, T]$ , совпадающих на каждом промежутке  $(t_{i,n}, t_{i+1,n})$  ( $i = 0, 1, \dots, n-1$ ) с алгебраическим полиномом степени не выше  $r$ .

Через  $P(\Delta_n)$  обозначим оператор отображающий  $C^\rho$  в  $S_r(\Delta_n)$ ,  $\rho \geq r - k$ . При фиксированном  $r$  последовательность  $\{P^*(\Delta_n^*)\}_{n=1}^\infty$  будем называть асимптотически наилучшей сплайн-регрессией для функции  $x(t)$ , если при  $n \rightarrow \infty$

$$\int_a^b (x(t) - P^*(\Delta_n^*, t))^2 dt = \inf_{\Delta_n} \inf \left\{ \int_a^b (x(t) - P(\Delta_n, t))^2 dt \mid P(\Delta_n) \in S_r(\Delta_n) \right\} (1 + o(1)). \quad (1)$$

Целью данных исследований является решение задачи (1) в случае кусочно-линейной регрессии.

## Основная часть

Пусть на отрезке  $[0, T]$  в узлах разбиения  $\Delta_n$  заданы значения функции  $x_i$ ,  $i = 0, 1, \dots, n$ . Кубический сплайн  $s_3(x, \Delta_n) = s_3(\{x_i\}_{i=0}^n, \Delta_n)$  называется интерполяционным с граничными условиями  $s_3^{(i)}(x, \Delta_n, 0) = x(0)$ ,  $i = 0, 1$  и  $s_3^{(i)}(x, \Delta_n, T) = x(T)$ ,  $i = 0, 1$ , если

$$s_3(x, \Delta_n, t_i) = x_i, \quad i = 0, 1, \dots, n.$$

Если  $x_i = Ti/n$ ,  $i = 0, 1, 2, \dots, n$ , то вместо  $s_3''(x, \{Ti/n\}_{i=0}^n, t)$  будем писать  $s_3(\{x_i\}_{i=0}^n)$ .

**Теорема 1.** Пусть  $x \in L_2^3$  такова, что  $x''$  обращается в ноль на конечном числе отрезков или точек из  $[0, T]$  и  $X(t)$  вторая первообразная  $x(t)$  такая, что  $X'(0) = 0$  и  $X(0) = 0$ . Выберем  $M_i$  из условий

$$\lambda_i M_{i-1} + 2M_i + \mu_i M_{i+1} = \frac{6}{h_{i-1} + h_i} \left( \frac{X_{i+1} - X_i}{h_i} - \frac{X_i - X_{i-1}}{h_{i-1}} \right), \quad i = 1, 2, \dots, n-1,$$

где  $\mu_i = \frac{h_{i-1}}{h_{i-1} + h_i}$ ,  $\lambda_i = 1 - \mu_i$ .

Тогда

$$\inf \left\{ \|x - s_1(\Delta_n)\|_2 \mid s_1(\Delta_n) \in S_1(\Delta_n) \right\} = \|x - s_3''(\{M_i\}_{i=0}^n, \Delta_n)\|_2.$$

Выберем узлы  $t_i^*$  разбиения  $\Delta_n^*$  из условия

$$\int_0^{t_i^*} \left( \left| s_3''(\{M_i\}_{i=0}^n, t) \right| + \frac{1}{n^\gamma} \right)^\alpha dt = \frac{i}{n} A_n, \quad A_n = \int_0^T \left( \left| s_3''(\{M_i\}_{i=0}^n, t) \right| + \frac{1}{n^\gamma} \right)^\alpha dt,$$

тогда при  $n \rightarrow \infty$

$$\inf_{\Delta_n} \inf \left\{ \|x - s_1(\Delta_n)\|_2 \mid s_1(\Delta_n) \in S_1(\Delta_n) \right\} = \|x - s_3''(\{M_i\}_{i=0}^n, \Delta_n^*)\|_2 (1 + o(1)) = \frac{\theta}{n^2} \|x''\|_\alpha + o\left(\frac{1}{n^2}\right),$$

где  $\theta = \frac{1}{2!} \left( \int_0^1 t^2 (1-t)^2 dt \right)^{1/2}$  и  $\alpha = 2/5$ .

Доказательству теоремы предпошлем следующее вспомогательное утверждение (см., например, [4]).

**Теорема 2.** Пусть  $x \in L_2^3$  такова, что  $x''$  обращается в ноль на конечном числе отрезков или точек из  $[0, T]$ , и  $s_1(x, \Delta_n, t)$  интерполяционная ломаная по разбиению  $\Delta_n$ . Тогда при  $n \rightarrow \infty$

$$\inf_{\Delta_n} \|x - s_1(x, \Delta_n)\|_2 = \frac{\theta}{n^2} \|x''\|_\alpha + o\left(\frac{1}{n^2}\right).$$

### Доказательство

Действительно,

$$\begin{aligned} \varepsilon(x, \Delta_n, t) &= x(t) - s_1(x, \Delta_n, t) = x(t) - x_{i-1}(1-\tau) - x_i\tau = (x(t) - x_{i-1})(1-\tau) + (x(t) - x_i)\tau = \\ &= (1-\tau) \int_{t_{i-1}}^t x'(u) du - \tau \int_t^{t_i} x'(u) du = \int_{t_{i-1}}^{t_i} K(t, u) x'(u) du, \end{aligned}$$

где

$$K(t, u) = \begin{cases} (1-\tau), & u \in [t_{i-1}, t], \\ \tau, & u \in (t, t_i] \end{cases}$$

Интегрируя последнее соотношение по частям и учитывая, что  $K(t, u)$ , как функция по  $u$ , в среднем равна нулю на промежутке  $[t_{i-1}, t_i]$ , получаем для  $t \in [t_{i-1}, t_i]$

$$x(t) - s_1(x, \Delta_n, t) = \int_{t_{i-1}}^{t_i} \aleph(t, u) x''(u) du,$$

где

$$\aleph(t, u) = \begin{cases} (u - t_{i-1})(1-\tau), & u \in [t_{i-1}, t], \\ -(u - t_i)\tau, & u \in (t, t_i] \end{cases}$$

Замечая, что для  $t \in [t_{i-1}, t_i]$ , функция  $\aleph(t, u)$  знакопостоянна, можем записать

$$m_i^- |\aleph(t)| \leq |\varepsilon(x, \Delta_n, t)| \leq m_i^+ |\aleph(t)|,$$

где

$$\aleph(t) = \int_{t_{i-1}}^{t_i} \aleph(t, u) du = \frac{1}{2!} (t - t_{i-1})(t_i - t)$$

и

$$m_i^- = \min \{ \|x''(t)\| \mid t \in [t_{i-1}, t_i] \}, \quad m_i^+ = \max \{ \|x''(t)\| \mid t \in [t_{i-1}, t_i] \}.$$

Сделав замену переменных  $\tau = t - t_{i-1}$ , получим

$$\|\mathbb{S}\|_{2[t_{i-1}, t_i]} = h_i^{1/\alpha} \theta$$

и, следовательно,

$$m_i^- h_i^{1/\alpha} \theta \leq \|\varepsilon(x, \Delta_n)\|_{2[t_{i-1}, t_i]} \leq m_i^+ h_i^{1/\alpha} \theta. \quad (2)$$

Таким образом, получаем

$$\|x(t) - s_1(x, \Delta_n, t)\|_2^2 \geq \theta^2 \sum_{i=0}^n |m_i^- h_i^{1/\alpha}|^2 = \theta^2 \sum_{i=0}^n \left( \int_{t_{i-1}}^{t_i} |y_n^-(t)|^\alpha dt \right)^{2/\alpha},$$

где  $y_n^-(t)$  есть кусочно-постоянная функция, равная  $m_i^-$  для  $t \in [t_{i-1}, t_i]$ .

Далее нам понадобится следующее простое утверждение: для любого  $n = 1, 2, \dots$  и  $\alpha > 1$  при условиях

$$A_i > 0, \quad \sum_{i=1}^n A_i = A \quad (3)$$

справедливо соотношение

$$\min \left\{ \sum_{i=1}^n A_i^\alpha \mid A_i \right\} = A^\alpha n^{1-\alpha},$$

причем минимум правой части достигается при  $A_i^* = A/n$ .

Действительно, составим функцию Лагранжа

$$L(\lambda, A_1, A_2, \dots, A_n) = \sum_{i=1}^n A_i^\alpha - \lambda \left( \sum_{i=1}^n A_i - A \right).$$

Для нахождения минимума функции Лагранжа, найдем производную по  $A_i$  ( $i = 1, 2, \dots, n$ ) и приравняем ее нулю

$$\frac{\partial}{\partial A_i} L(\lambda, A_1, A_2, \dots, A_n) = -\lambda + \alpha A_i^{\alpha-1} = 0, \quad i = 1, 2, \dots, n.$$

Решением этой системы является

$$A_i^* = \left( \frac{\lambda}{\alpha} \right)^{\frac{1}{\alpha-1}}, \quad i = 1, 2, \dots, n.$$

Отсюда и из (3) получаем



$$A_i^* = A/n,$$

и экстремальное значение этой задачи равно

$$\sum_{i=1}^n (A_i^*)^\alpha = \sum_{i=1}^n \frac{A^\alpha}{n^\alpha} = \frac{A^\alpha}{n^{\alpha-1}}.$$

Отсюда и из предыдущего получаем, что для любой функции  $y \in C$ , произвольного набора  $t_i \in [0, T]$  и любого  $\beta \in (0, \infty)$  выполняется неравенство

$$\sum_{i=1}^n \left( \int_{t_{i-1}}^{t_i} |y(t)| dt \right)^{\beta+1} \geq \frac{1}{n^\beta} \left( \int_a^b |y(t)| dt \right)^{\beta+1}.$$

Следовательно, для любого разбиения  $\Delta_n$

$$\|x - s_1(x, \Delta_n)\|_2 \geq \frac{\theta}{n^2} \left( \int_a^b |y_n^-(t)|^\alpha dt \right)^{1/\alpha}.$$

Ясно, что если при  $n \rightarrow \infty$  интеграл  $\int_a^b |y_n^-(t)|^\alpha dt$  не стремится к  $\int_a^b |x''(t)|^\alpha dt$ , а значит и ошибка приближения  $\|x - s_1(x, \Delta_n)\|_2$  не стремится к нулю. Таким образом, получаем

$$\|x - s_1(x, \Delta_n)\|_2 \geq \frac{\theta}{n^2} \|x''\|_\alpha + o\left(\frac{1}{n^2}\right). \quad (4)$$

Пусть  $z_n(t)$  произвольная последовательность функций, такая, что при  $n \rightarrow \infty$

$$\|z_n - x''\|_\infty \leq \varepsilon_n, \quad (5)$$

где

$$\varepsilon_n = \frac{1}{n^\gamma} \left( 1 - \frac{A \|x''\|_C}{n^{2(\alpha+1)}} \right), \quad A = \int_a^b |x''(t)|^\alpha dt, \quad \gamma = (3\alpha + 2)^{-1}.$$

Выберем узлы  $t_i^*$  разбиения  $\Delta_n^*$  из условия

$$\int_a^{t_i^*} \left( |z_n(t)| + \frac{1}{n^\gamma} \right)^\alpha dt = \frac{i}{n} A_n, \quad \text{где } A_n = \int_a^b \left( |z_n(t)| + \frac{1}{n^\gamma} \right)^\alpha dt.$$

Тогда

$$\int_{t_{i-1}^*}^{t_i^*} \left( |z_n(t)| + \frac{1}{n^\gamma} \right)^\alpha dt = \frac{1}{n} A_n, \quad i = 1, 2, \dots, n. \quad (6)$$

Учитывая, что  $A_n \rightarrow A$  при  $n \rightarrow \infty$ , получаем, что при достаточно больших  $n$  будут иметь место неравенства

$$h_i \leq \frac{A_n}{n^{1-\alpha\gamma}} \leq \frac{2A}{n^{1-\alpha\gamma}}.$$

Из неравенства (2) имеем

$$\|\varepsilon(x, \Delta_n^*)\|_{2[t_{i-1}^*, t_i^*]} \leq m_i^+ h_i^{1/\alpha} \theta = \theta \left( \int_{t_{i-1}^*}^{t_i^*} |m_i^+|^\alpha dt \right)^{1/\alpha},$$

а так как найдется точка  $\xi \in [t_{i-1}^*, t_i^*]$  такая, что

$$m_i^+ = \max \{ |x''(t)| : t \in [t_{i-1}^*, t_i^*] \} = x''(t) + x'''(\xi)(t_i^* - t),$$

то получаем

$$\begin{aligned} \|\varepsilon(x, \Delta_n^*)\|_{2[t_{i-1}^*, t_i^*]} &\leq \theta \left( \int_{t_{i-1}^*}^{t_i^*} (|x''(t)| + \|x'''\|_\infty h_i)^\alpha dt \right)^{1/\alpha} \leq \theta \left( \int_{t_{i-1}^*}^{t_i^*} (|z_n(t)| + \varepsilon_n + 2A\|x'''\|_\infty n^{\alpha\gamma-1})^\alpha dt \right)^{1/\alpha} = \\ &= \theta \left( \int_{t_{i-1}^*}^{t_i^*} \left( |z_n(t)| + \frac{1}{n^\gamma} \right)^\alpha dt \right)^{1/\alpha}. \end{aligned}$$

Отсюда и из (6) сразу получаем

$$\|\varepsilon(x, \Delta_n^*)\|_{2[t_{i-1}^*, t_i^*]} \leq \theta \left( \frac{A_n}{n} \right)^{1/\alpha}.$$

Следовательно,

$$\inf_{\Delta_n} \|x - s_1(x, \Delta_n)\|_2 \leq \left( \sum_{i=1}^n \|\varepsilon(x, \Delta_n^*)\|_{2[t_{i-1}^*, t_i^*]}^2 \right)^{1/2} \leq \frac{\theta}{n^2} A_n^{1/\alpha}$$

и при  $n \rightarrow \infty$

$$\inf_{\Delta_n} \|x - s_1(x, \Delta_n)\|_2 \leq \frac{\theta}{n^2} \|x''\|_\alpha + o\left(\frac{1}{n^2}\right),$$

что вместе с (6) и завершает доказательство теоремы 2.

Перейдем к доказательству основного утверждения.

В соответствии с теоремой Холлидея (см., например, [6], с. 155)

$$\min \left\{ \int_0^T (x''(t) - \ell''(t))^2 dt \mid \ell(t) \in S_3(\Delta_n) \right\} = \int_0^T (x''(t) - s_3''(x, \Delta_n, t))^2 dt,$$

таким образом,

$$\min \left\{ \int_0^T (x(t) - \ell(t))^2 dt \mid \ell(t) \in S_1(\Delta_n) \right\} = \int_0^T (x(t) - s_3''(X, \Delta_n, t))^2 dt,$$

где  $X(t)$  – вторая первообразная  $x(t)$  такая, что  $X'(0) = 0$  и  $X(0) = 0$ .

Кроме того, если для интерполяционного сплайна  $s_3(x, \Delta_n) = s_3(\{x_i\}_{i=0}^n, \Delta_n)$  положим

$$s_3''(x, \Delta_n, t_i) = M_i, \quad i = 0, 1, \dots, n,$$

то для  $t \in [t_i, t_{i+1}]$  сплайн  $s_3(x, \Delta_n)$  можно записать в виде

$$s_3(x, \Delta_n, t) = x_i(1-t) + x_{i+1}t - \frac{h_i^2}{6}t(1-t)((2-t)M_i + (1+t)M_{i+1}),$$

где  $M_i$  находятся из условий

$$s_3''(x, \Delta_n, t_i - 0) = s_3''(x, \Delta_n, t_i + 0), \quad i = 1, \dots, n-1, \quad (7)$$

и определяются системой

$$\lambda_i M_{i-1} + 2M_i + \mu_i M_{i+1} = \frac{6}{h_{i-1} + h_i} \left( \frac{x_{i+1} - x_i}{h_i} - \frac{x_i - x_{i-1}}{h_{i-1}} \right).$$

Тогда

$$s_3''(x, \Delta_n, t) = M_i(1-t) + M_{i+1}t,$$

то есть  $s_3''(x, \Delta_n, t) = s_1(\{M_i\}_{i=0}^n, \Delta_n, t)$ .

Кроме того, из [7] с.115 имеем

$$|x''(t) - s_3''(x, \Delta_n, t)| \leq \frac{3}{8} h_{\max}^2 \|x^{(4)}\|_{\infty}, \quad h_{\max} = \max_{i=0,1,\dots,n-1} h_i,$$

то есть,  $s_3''(\{M_i\}_{i=0}^n, \{Ti/n\}_{i=0}^n, t)$  удовлетворяет условию (5).

Сопоставляя полученные результаты и утверждение теоремы 2, сразу получаем теорему 1.

## Выводы

В работе решена задача построения асимптотически оптимальной кусочно-линейной регрессионной модели. Для построения асимптотически оптимального раз-

биения кусочно-линейной регрессии построен конструктивный алгоритм, основанный на интерполяционных сплайнах.

### Список литературы

1. Marsh L. Spline Regression Models / L. Marsh, D. Cormier // Sage university papers. Series: Quantitative Applications in Social Sciences. – 2002. – 69 p.
2. Thermaratnam R. S-Estimation for Penalized Regression Splines / R. Thermaratnam, G. Claeskens, C. Croux, M. Selibian-Barrera // Journal of Computational and Graphical Statistics. – 2010. – Vol.19, Iss.3. – PP. 609-625.
3. Berry S. Bayesian Smoothing and Regression Splines for Measurement Error Problems. / S. Berry, R. Carroll, D. Ruppert // Journal of the American Statistical Association. – 2002. – Vol.97, Iss.457. – PP. 160-169.
4. Лигун А.А. Асимптотические методы восстановления кривых / А.А. Лигун, А.А. Шумейко. – К.: Институт математики НАН Украины, 1997. – 358 с.
5. Де Бор К. Практическое руководство по сплайнам : Пер. с англ. – М.: Радио и связь, 1985. – 304 с.
6. Алберг Дж. Теория сплайнов и ее приложения / Дж. Алберг, Э. Нильсон, Дж. Уолш. – М.: Мир, 1972. – 320 с.
7. Завьялов Ю.С. Методы сплайн-функций / Ю.С. Завьялов, Б.И. Квасов, В.Л. Мирошниченко. – М.: Наука, 1980. – 352 с.

О.О. Шумейко, Є.О. Шумейко

### ПРО ПОБУДОВУ АСИМПТОТИЧНО ОПТИМАЛЬНОЇ КУСКОВО-ЛІНІЙНОЇ РЕГРЕСІЇ

В роботі запропоновано одну конструкцію кусково-лінійної регресії, яка асимптотично співпадає з оптимальною. Доведено, що задача побудови кусково-лінійної регресії зводиться до побудови кубічного інтерполяційного сплайну від другої похідної даної функції.

**Ключові слова:** сплайн-регресія, кусково-лінійна регресія, оптимізація розбивок

A. Shumeyko, Y. Shumeyko

### CONSTRUCTION OF AN ASYMPTOTICALLY OPTIMAL POLYGONAL REGRESSION

The paper presents the construction of polygonal regression asymptotically coincides with the best solution. Proved the problem of constructing a polygonal regression model reduces to the construction of a cubic spline interpolation of the second integral of function.

**Keywords:** spline regression, piecewise linear regression, optimization of partitions

# ІЄРАРХІЧНА ДИФЕРЕНЦІАЛЬНО-ІГРОВА МОДЕЛЬ В ЗАДАЧАХ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Р.В. Грищук

Житомирський військовий інститут імені С.П. Корольова Національного авіаційного університету,  
проспект Миру, 22, Житомир, 10004, Україна; e-mail: RuslanGRV@rambler.ru

Показано, що задача оцінювання ефективності систем захисту інформації полягає в побудові відповідної адекватної моделі з урахуванням багатокритерійного підходу. Як таку модель запропоновано ієрархічну диференціально-ігрову модель. Для побудови моделі використано методи диференціально-ігрового моделювання на основі диференціальних перетворень та метод вкладних скалярних згорток.

**Ключові слова:** ієрархічна диференціально-ігрова модель, критерій, вкладена скалярна згортка, система захисту інформації

## Вступ

Високотехнологічний розвиток сучасного інформаційного суспільства породжує одну з кардинальних проблем сучасності – проблему захисту інформації. Як показує практичний досвід [1], захисту в сучасних умовах потребує практично будь-яка інформація, що становить цінність для її власника з точки зору нецільового застосування її, неавторизованими користувачами.

З метою мінімізації наслідків від несанкціонованого доступу (НСД) до інформації неавторизованими користувачами провідні експерти з інформаційної безпеки відводять важливу роль подальшому підвищенню ефективності діючих та перспективних систем захисту інформації (СЗІ) [1–8]. Так, створюючи нову, або удосконалюючи діючу СЗІ розробник повинен враховувати значну множину факторів, які впливають на захищеність інформації в системі. Досить часто такі фактори мають рандомізоване походження та знаходяться в протиріччі один до одного. Нехтування хоча б одним з них призводить до неадекватності СЗІ висунутим вимогам щодо забезпечення заданого рівня захищеності інформації. Тому, в рамках означеної проблеми, актуальною науковою задачею є задача розробки принципово нових засобів захисту інформації – нових СЗІ, що за умов невизначеності забезпечують заданий рівень захищеності інформації. Оскільки натурні експерименти є високовартісними, то першим кроком на шляху до розв’язання даної задачі є створення нових математичних методів та моделей оцінювання ефективності діючих та перспективних СЗІ з урахуванням багатокритерійного підходу.

Аналіз останніх досліджень і публікацій показав, що питанням підвищення ефективності СЗІ присвячено ряд праць як вітчизняних [1–5], так і закордонних вчених [6–10] та ін. Не зважаючи на фундаментальну та прикладну спрямованість праць [1, 4, 8, 10] та [2, 3, 5–7, 9] відповідно, у більшості з них недостатньо уваги приділено питанням забезпечення заданого рівня захищеності інформації системою захисту. При побудові відповідних моделей не враховуються показники якісного функціонування СЗІ. Також не враховуються обмеження на витрати ресурсів, які мінімально необхідні для забезпечення СЗІ заданого рівня захищеності інформації, а також рандомізована

природа факторів, що впливають на її захищеність. Тому питання про відсутність формалізованих підходів щодо забезпечення заданого рівня захищеності інформації СЗІ в умовах багатфакторності досі залишається відкритим та потребує розв'язання.

Метою статті є розробка адекватної математичної моделі для оцінювання ефективності діючих та перспективних СЗІ, яка ґрунтуватиметься на багатокритерійному підході щодо урахування усієї множини факторів, які впливають на якість функціонування СЗІ та захищеність інформації в ній.

## Основний зміст досліджень

*Постановка задачі.* Виходячи з досліджень [12] та узагальненої постановки задачі багатокритерійної оптимізації ієрархічних структур [14], формалізуємо задачу оцінювання ефективності СЗІ на прикладі СЗІ поданої в [15].

Нехай множина станів в яких може перебувати СЗІ [15] описується системою диференціальних рівнянь Колмогорова-Чепмена загального вигляду [12]

$$\frac{dP_i(t)}{dt} = f_i(\lambda_i(t), \mu_i(t), \beta, \gamma, \varphi, \rho, P_0(t), P_1(t), \dots, P_7(t)), \quad i = 0, 1, \dots, 7, \quad (1)$$

де  $P_i(t)$  – змінні стану процесу, що моделюється, 7 – вимірний фазовий простір  $R_7$ , що характеризує процеси в області  $P \in R_7$  з відповідним значенням ймовірності перебування СЗІ у даному стані;  $f_i = (f_0, f_1, \dots, f_7)$  – дійсні функції, визначені на прямому добутку  $P \times E_\lambda \times E_\mu$  вказаних множин;  $\lambda_i(t)$ ,  $\mu_i(t)$  – інтенсивності потоків розподілу інформаційних ресурсів гравця, що захищається та нападає, які відповідно належать  $\Lambda \in E_\lambda$ ,  $M \in E_\mu$  замкненим обмеженням у евклідових просторах  $R_\lambda$  і  $R_\mu$  множинами, що визначають можливі стратегії гравців;  $\beta_i$  – інтенсивність відмов СЗІ;  $\gamma_i$  – інтенсивність знаходження вразливостей у СЗІ;  $\varphi_i$  – інтенсивність усунення вразливостей;  $\rho_i$  – інтенсивність створення нової інформації.

Система (3) справедлива за дотримання умов нормування

$$\sum_{i=0}^7 P_i(t) = 1, \quad (2)$$

де  $P_0(t_0) = \dots = P_6(t_0) = 0$ ,  $P_7(t_0) = 1$  – початкові умови.

Розподіл інтенсивностей потоків  $\lambda_i(t)$  і  $\mu_i(t)$  нестационарний, але обмежений за величиною

$$\lambda_{i \min}(t) \leq \lambda_i(t) \leq \lambda_{i \max}(t) \quad (3)$$

та

$$\mu_{i \min}(t) \leq \mu_i(t) \leq \mu_{i \max}(t), \quad (4)$$

де  $\lambda_{i \min}(t)$  і  $\mu_{i \min}(t)$  – мінімальні, а  $\lambda_{i \max}(t)$  і  $\mu_{i \max}(t)$  – максимальні інтенсивності потоків захисних дій та інформаційних атак, відповідно, які задано на аргументі  $t$ , що обмежується тривалістю інформаційного конфлікту  $T$ ,  $t \in [t_0, T]$ . Такі ж обмеження накладаються й на інтенсивності  $\beta_i$ ,  $\gamma_i$ ,  $\varphi_i$  та  $\rho_i$  відповідно, тобто

$$\beta_{i\min} \leq \beta_i \leq \beta_{i\max}, \quad (5)$$

$$\gamma_{i\min} \leq \gamma_i \leq \gamma_{i\max}, \quad (6)$$

$$\varphi_{i\min} \leq \varphi_i \leq \varphi_{i\max}, \quad (7)$$

$$\rho_{i\min} \leq \rho_i \leq \rho_{i\max}. \quad (8)$$

Керуючі параметри  $\lambda_i(t)$  і  $\mu_i(t)$ , які мають місце в кожний момент часу  $t$ , в залежності від стану процесу  $P$ , називають стратегіями гравців [16].

*Зауваження.* Кількість рівнянь у системі (1) відповідає кількості станів, у яких може перебувати СЗІ під впливом відповідних інтенсивностей  $\lambda_i(t)$ ,  $\mu_i(t)$ ,  $\beta_i$ ,  $\gamma_i$ ,  $\varphi_i$  та  $\rho_i$ .

Потрібно розробити ієрархічну диференціально-ігрову модель оцінювання ефективності СЗІ.

*Вибір методу розв'язання.* На сучасному етапі розвитку науки і техніки перспективним підходом на шляху розв'язання прикладних задач захисту інформації є системний аналіз проблеми, що вирішується [11]. Системний аналіз СЗІ полягає в потребі вивчення усієї сукупності критеріїв, які впливають на ефективність її функціонування та зводиться до побудови та дослідження їх ієрархічних моделей.

У [12] автором обґрунтовано новий підхід до створення перспективних СЗІ. Показано, що диференціально-ігровий підхід, на основі якого пропонується створювати перспективні СЗІ, наприклад такі, як системи виявлення атак, відкриває можливості врахування динаміки процесів нападу на інформацію, що протікають в системі, їх рандомізованої природи, а також адекватно відображають антагонізм інтересів суб'єктів інформаційного конфлікту – гравців (методів НСД та методів захисту інформації (МЗІ)). Антагонізм, породжений протиріччям інтересів і цілей методів НСД і МЗІ, є джерелом інформаційного конфлікту, який, у свою чергу як системне явище характеризується структурними, динамічними та теоретико-ігровими властивостями, нехтувати жодною з яких неможливо. Так застосування теорії диференціальних ігор для моделювання процесів нападу на інформацію як універсальної моделі динамічних оптимізаційних задач вимагає використання складних і сучасних методів та засобів моделювання. Тому як такий апарат у [12] використано диференціальні перетворення академіка НАН України Г.Є. Пухова [13].

Застосування операційного методу диференціальних перетворень дозволяє розв'язувати складні диференціально-ігрові задачі в області зображень з відсутнім неперервним аргументом і зводити їх до більш простих, які легко розв'язуються відомими методами. На відміну від інших операційних методів, наприклад інтегральних перетворень Лапласа, Мелліна, Фур'є тощо, область моделювання диференціальними перетвореннями не обмежується лінійними рівняннями. Їх перевагою над іншими операційними методами є можливість проведення моделювання в аналітичному, цілочислово-аналітичному та цілочисловому вигляді та відсутність методичної похибки методу [13]. Властивість адаптованості диференціальних перетворень до вибору форми моделювання підвищує ефективність методів аналізу і синтезу складних динамічних систем, до яких відносять і СЗІ та процесів, що моделюються, а відсутність методичної похибки забезпечує адекватність моделей реальним процесам.

Так, нехай ефективність СЗІ в цілому визначається ієрархічною системою векторів

$$I^{(j-1)} = \{I_i^{(j-1)}\}_{i=1}^{n^{(j-1)}}, \quad j \in [2, m], \quad (9)$$

де  $I^{(j-1)}$  – вектор критеріїв на  $(j-1)$  рівні ієрархії, який виступає компонентою, на основі якої оцінюється якість альтернативи на  $j$ -му рівні;  $m$  – кількість рівнів ієрархії;  $n^{(j-1)}$  – кількість властивостей, що оцінюються на  $(j-1)$ -му рівні ієрархії.

Зауваження. Один і той же критерій  $(j-1)$ -го рівня може оцінювати декілька властивостей  $j$ -го рівня ієрархії [15].

Припущення. Нехай кожен з компонентів векторного критерію (9) має однаковий пріоритет.

Знайдемо аналітичну  $I^*$  та якісну оцінку ефективності даної альтернативи. Для цього застосуємо метод вкладених скалярних згорток професора Вороніна А.М. [18]. Суть даного методу полягає у здійсненні ітераційної послідовності операцій зваженої скалярної згортки критеріїв кожного рівня ієрархії від нижнього до верхнього рівня на основі обраної схеми компромісу, яку в формалізованому вигляді можна подати моделлю вигляду

$$\{I^{(j-1)} \rightarrow I^{(j)}\}, \quad j \in [2, m], \quad (10)$$

де задача пошуку ефективності усієї ієрархічної системи в цілому виражається задачею визначення скалярної згортки критеріїв на верхньому рівні ієрархії, тобто

$$I^* = I^{(m)}. \quad (11)$$

Згідно з [17, 18], для коректного застосування рекурентної формули (10) доцільно обрати як схему компромісів – нелінійну схему компромісів (НСК) [14]. Для адекватності її застосування необхідно і достатньо виконання умов невід’ємності усіх частинних критеріїв, їх мінімізації та обмеженості, тобто

$$0 \leq I_i \leq I_{i \max}, \quad I = \{I_i\}_{i=1}^n, \quad (12)$$

де  $I$  – вектор обмежень. Тоді оцінка  $k$ -ї властивості альтернативи на  $j$ -му рівні ієрархії із застосуванням НСК матиме вигляд

$$I_k^{(j)}(I_{0k}^{(j-1)}) = \sum_{i=1}^{n_k^{(j-1)}} [1 - I_{0ik}^{(j-1)}]^{-1}, \quad k \in [1, n^{(j)}], \quad (13)$$

де  $I_{0ik}^{(j-1)}$  – компоненти нормованого вектору  $I_0^{(j-1)}$ , що застосовуються при оцінюванні  $k$ -ї властивості альтернативи на  $j$ -му рівні ієрархії;  $n_k^{(j-1)}$  – кількість альтернатив;  $n^{(j)}$  – кількість властивостей, що оцінюються на  $j$ -му рівні. У виразі (13) усі критерії  $(j-1)$ -го рівня нормовані згідно виразу  $I_0 = I/I_{\max}$ .

Крім того, відповідно до методу вкладених скалярних згорток [17] вираз (13) для відображення його суті згідно з рекурентним виразом (10), потребує нормування. Відносний нормований критерій  $I_{0k}^{(j)}$  при цьому повинен мінімізуватися,  $I_{0k}^{(j)} \in [0; 1]$ . Нормування відносного нормованого критерію  $I_{0k}^{(j)}$ , за якого досягається його мінімізація дає змогу подати наступний рекурентний вираз для розрахунку аналітичних оцінок властивостей альтернатив на усіх рівнях ієрархії [17]

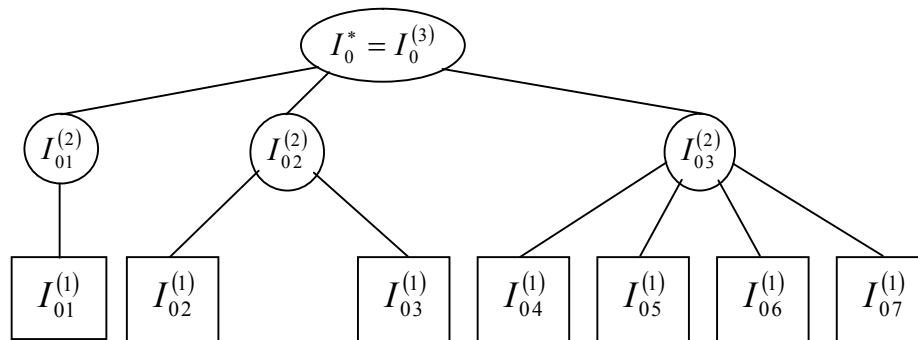


$$I_{0k}^{(j)} = 1 - \left\{ \sum_{i=1}^{n_k^{(j-1)}} [1 - I_{0ik}^{(j-1)}]^{-1} \right\}^{-1}, \quad k \in [1, n^{(j)}], \quad j \in [2, m]. \quad (14)$$

Результат оцінювання згідно з (14) узгоджується з інтервальною нормованою оберненою шкалою, з якою можна ознайомитися наприклад у [17, 18]. Як наслідок є можливість отримання якісної (лінгвістичної) оцінки альтернативи – ефективності СЗІ.

*Розв'язок.* Для знаходження розв'язку поставленої задачі згідно методу вкладених скалярних згорток [17] визначимо рівні ієрархії моделі, а згідно диференціально-ігрового методу моделювання на основі диференціальних перетворень [12] з позиції гравця захисту – визначимо частинні критерії, що визначають ефективність СЗІ [15].

Аналіз системи диференціальних рівнянь Колмогорова-Чепмена (1) показує, що в моделі, яка розробляється можливо виділити три рівні ієрархії рис. 1.



**Рис. 1.** Структурна схема ієрархії критеріїв для оцінювання ефективності СЗІ

Так, ефективність СЗІ за рівнем забезпечення заданого рівня захищеності характеризується невідомою оцінкою критерію  $I_{01}^{(1)}$ , за рівнем витрат ресурсів гравців захисту та нападу – відповідно критеріями  $I_{02}^{(1)}$  та  $I_{03}^{(1)}$ . Показник якісного функціонування СЗІ оцінюється наступними критеріями –  $I_{04}^{(1)}, \dots, I_{07}^{(1)}$ .

Усі частинні критерії  $I_{01}^{(1)}, \dots, I_{07}^{(1)}$ ,  $I_{01}^{(2)}$ ,  $I_{02}^{(2)}$  та  $I_{03}^{(2)}$  (див. рис. 1) є нормованими та зведеними до одного способу екстремізації – мінімізації. Як видно з рис. 1 критерії нижчого рівня приймають участь в оцінюванні властивостей вищого рівня.

Виходячи з рекурентної формули (14) перший етап композиції критеріїв полягає в отриманні виразу для аналітичної оцінки рівня захищеності інформації, що забезпечує досліджувана СЗІ (другий рівень ієрархії), тобто

$$I_{01}^{(2)} = 1 - \left\{ \sum_{i=1}^{n_1^{(1)}} [1 - I_{0i1}^{(1)}]^{-1} \right\}^{-1}, \quad (15)$$

де  $n_1^{(1)} = 1$ ;  $I_{011}^{(1)} = I_{01}^{(1)}$ .

Для отримання відповідної аналітичної оцінки (15) визначимо фізичний зміст критерію, що входить до її складу.

З позиції гравця, що захищається перший критерій  $I_1$  обирається виходячи з потреби забезпечення заданого рівня захищеності інформації, що реалізує досліджувана СЗІ, тобто

$$I_1 = \frac{1}{T} \int_{t_0}^T P_7(t) dt, \quad (16)$$

при обмеженнях (12), де  $I_{1\max} = 1$ .

Привівши до мінімізації частинний критерій  $I_{01}^{(2)}$  та скориставшись (15) в аналітичному вигляді визначимо оптимальні й апріорно невідомі інтенсивності гравців захисту  $\lambda_{\min}^{opt}(t)$  та нападу  $\mu_{\max}^{opt}(t)$  відповідно до диференціально-ігрового методу [12]

$$\begin{cases} \frac{\partial I_{01}^{(2)}}{\partial \lambda} = 0; \\ \frac{\partial I_{01}^{(2)}}{\partial \mu} = 0; \end{cases} \rightarrow \begin{cases} \frac{\partial(1-I_{01})}{\partial \lambda} = 0; \\ \frac{\partial(1-I_{01})}{\partial \mu} = 0; \end{cases} \rightarrow \begin{cases} \lambda^{opt}; \\ \mu^{opt}; \end{cases} \rightarrow \begin{cases} \frac{\partial^2(1-I_{01})}{\partial \lambda^2} > 0; \\ \frac{\partial^2(1-I_{01})}{\partial \mu^2} < 0; \end{cases} \rightarrow \begin{cases} \lambda_{\min}^{opt}; \\ \mu_{\max}^{opt}. \end{cases} \quad (17)$$

Якщо прийняти відповідно до [15] наступні значення для показників, що описують якість функціонування СЗІ з параметрами  $\beta = 0.0027$ ,  $\gamma = 0.0328$ ,  $\varphi = 0.0328$  та  $\rho = 1$  за добу ( $T = 1$ ), то скориставшись диференціально-ігровим методом [12] згідно виразу (17) матимемо

$$\begin{cases} \lambda_{\min}^{opt} = 0.5251; \\ \mu_{\max}^{opt} = 0.9645. \end{cases} \quad (18)$$

Для отримання кількісної оцінки ефективності СЗІ за критерієм забезпечення заданого рівня захищеності з урахуванням (18) згідно (15) маємо

$$I_{01}^{(2)} = 1 - 0.66 = 0.34. \quad (19)$$

Співставлення з інтервальною нормованою оберненою шкалою [17, 18] дозволяє стверджувати, що СЗІ за даним критерієм *добре* забезпечує заданий рівень захищеності.

Оцінимо ефективність СЗІ за витратами ресурсів захисту. Оцінка витрат ресурсів обох гравців в аналітичному вигляді має наступний вигляд (другий рівень ієрархії (див. рис. 1))

$$I_{02}^{(2)} = 1 - \left\{ \sum_{i=1}^{n_2^{(1)}} [1 - I_{0i2}^{(1)}]^{-1} \right\}^{-1}, \quad (20)$$

де  $n_2^{(1)} = 2$ ;  $I_{012}^{(1)} = I_{02}$ ;  $I_{022}^{(1)} = I_{03}$ .

Для цього визначимо другий частинний критерій  $I_2$ , що обирається гравцем захисту для забезпечення заданого рівня захищеності (16) у вигляді

$$I_2 = \frac{1}{T} \int_{t_0}^T \lambda_i^2(t) dt, \quad (21)$$

при обмеженнях (12), де  $I_{2\max} = \lim_{t \rightarrow T} I_2$ .

Гравцем захисту також припускається те, що середні витрати ресурсів гравця нападу визначаються як

$$I_3 = \frac{1}{T} \int_{t_0}^T \mu_i^2(t) dt. \quad (22)$$

Ресурс гравця нападу обмежений, тобто  $I_{3\max} = \lim_{t \rightarrow T} I_3$ .

З позиції гравця захисту заданий рівень захищеності (16) забезпечуватиметься при оптимальних витратах ресурсів захисту (18), при цьому розподіл частинних критеріїв (21) та (22) екстремізується згідно виразу

$$\begin{cases} I_2 \rightarrow \min; \\ I_3 \rightarrow \max. \end{cases} \quad (23)$$

Звівши до єдиного способу екстремізації (мінімізації) частинні критерії (23) та скориставшись (20), отримаємо кількісну оцінку ефективності СЗІ за витратами ресурсів захисту

$$I_{02}^{(2)} = 1 - \frac{1}{\frac{1}{1-0.5} + \frac{0.93}{0.47}} = 0.75. \quad (24)$$

У відповідності до шкали [17, 18] якість витрат ресурсів СЗІ для забезпечення заданого рівня захищеності є *низькою*.

Оцінимо ефективність СЗІ за властивістю урахування показника якісного функціонування. Так із рекурентної формули (14) маємо

$$I_{03}^{(2)} = 1 - \left\{ \sum_{i=1}^{n_3^{(1)}} [1 - I_{0i3}^{(1)}]^{-1} \right\}^{-1}, \quad (25)$$

де  $n_3^{(1)} = 4$ ;  $I_{013}^{(1)} = I_{04}$ ;  $I_{023}^{(1)} = I_{05}$ ;  $I_{033}^{(1)} = I_{06}$ ;  $I_{043}^{(1)} = I_{07}$ .

З позиції гравця захисту критерії  $I_{04}$ ,  $I_{05}$ ,  $I_{06}$  та  $I_{07}$  розподіляються наступним чином

$$\begin{cases} I_{04} \rightarrow \min; \\ I_{05} \rightarrow \max; \\ I_{06} \rightarrow \max; \\ I_{07} \rightarrow \max. \end{cases} \quad (26)$$

Мінімізуювши частинні критерії (22) та скориставшись виразом (25) отримаємо кількісну оцінку ефективності СЗІ за властивістю урахування показника якісного функціонування [15]. Маємо

$$I_{03}^{(2)} = 1 - \frac{1}{\frac{1}{1-0.0027} + \frac{1}{0.0328} + \frac{1}{0.0328} + 1} \approx 0.98. \quad (27)$$

За інтервальною нормованою оберненою шкалою [17, 18] ефективність СЗІ за даною групою критеріїв є незадовільною.

Заключний (другий) етап композиції критеріїв згідно рекурентного виразу (14) набуває вигляду

$$I_0^* = I_0^{(3)} = 1 - \left\{ \sum_{i=1}^{n_3^{(2)}} [1 - I_{0i3}^{(1)}] \right\}^{-1}, \quad (28)$$

де  $n_4^{(2)} = 3$ ;  $I_{013}^{(2)} = I_{01}^{(2)}$ ;  $I_{023}^{(2)} = I_{02}^{(2)}$ ;  $I_{033}^{(2)} = I_{03}^{(2)}$ .

Підставивши, отримаємо

$$I_0^* = 1 - \frac{1}{\frac{1}{1-0.34} + \frac{1}{1-0.75} + \frac{1}{1-0.98}} = 0.98. \quad (29)$$

Отже, за даною аналітичною оцінкою ефективність СЗІ [15] в цілому є незадовільною.

## Висновки

Вперше, з використанням методу диференціально-ігрового моделювання на основі диференціальних перетворень та методу вкладених скалярних згорток розроблено ієрархічну диференціально-ігрову модель оцінювання ефективності СЗІ. На відміну від відомих, розроблена модель не обмежується числом параметрів, за якими оцінюється СЗІ. Застосування моделі в задачах захисту інформації дозволяє отримувати кількісні та якісні оцінки ефективності систем захисту інформації.

## Список літератури

1. Ленков С.В. Методы и средства защиты информации : монография [в 2-х т.] Т. 2. Информационная безопасность / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. – К.: Арий, 2008. – 344 с.
2. Паціра Є.В. Організація систем виявлення атак в умовах нечіткості : дис. канд. техн. наук: 05.13.21 «Системи захисту інформації» / Є.В. Паціра. – К., 2005. – 178 с.
3. Технології виявлення вторгнень з використанням шаблонів Data Mining / [К.В. Колесніков, В.Ю. Шадхін, Ю.П. Швед та ін.] // Вісник ЧДТУ. – Черкаси: ЧДТУ, 2009. – № 1. – С. 15–18.
4. Кобозева А.А. Анализ информационной безопасности: монография / А.А. Кобозева, В.О. Хорошко. – К.: ДУИКТ, 2009. – 251 с.
5. Шматок С.О. Методика оцінки ефективності пакету заходів для захисту інформації / С.О. Шматок, В.Б. Міщенко, Т.А. Вещицька [та ін.] // Збірник наукових праць ЦНДІ ЗС України. – К.: ЦНДІ ЗС України, 2007. – № 4. – С. 173–188.
6. Лошин П. Обнаружение атак [Электронный ресурс] / П. Лошин. // Открытые системы. – Режим доступа до мат.: <http://www.osp.ru/cw/2001/17/40355>.
7. Mantel H. A Uniform Framework for the Formal Specification and Verification of Information Flow Security: Diss. Doctor der Ingenieurwissenschaften / Heiko Mantel. – Saarbrücken, 2003. – 275 p
8. Biskup J. Security in computing systems: challenges, approaches and solutions: monogr. / J. Biskup. – Berlin: Springer, 2009. – 694 p.
9. Бобров А. Системы обнаружения вторжений. Intrusion Detection System – IDS [Электронный ресурс] / А. Бобров. – Режим доступа: <http://www.icmm.ru/~masich/win/lexion/ids/ids.html>.
10. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства / В.Ф. Шаньгин. – М.: ДМК Пресс, 2008. – 544 с.

11. Згуровський М.З. Основи системного аналізу / М.З. Згуровський, Н.Д. Панкратова. – К.: ВНУ, 2007. – 544 с.
12. Гришук Р.В. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень : монографія / Р.В. Гришук. – Житомир: РУТА, 2010. – 280 с.
13. Пухов Г.Е. Дифференциальные преобразования и математическое моделирование физических процессов : монография / Г.Е. Пухов. – К.: Наук. думка, 1986. – 160 с.
14. Воронин А.Н. Многокритериальная оптимизация иерархических структур / А. Н. Воронин // Проблемы інформатизації та управління. – К.: НАУ, 2004. – № 11. – С. 101–104.
15. Пономарёв А.А. Решение задачи оценки времени преодоления систем защиты информации / А.А. Пономарёв // Актуальные проблемы безопасности информационных технологий: Сб. мат. междунар. науч.-практ. конф. – М.: ФГУП, 2008. – С. 81–85.
16. Васильев В.В. Моделирование задач оптимизации и дифференциальных игр / В.В. Васильев, В.Л. Баранов – К.: Наукова думка, 1989. – 286 с.
17. Воронин А.Н. Вложенные скалярные свертки векторного критерия / А. Н. Воронин // Проблемы управления и информатики. – 2003. – № 5. – С. 10–21.
18. Воронин А.Н. Декомпозиция и композиция свойств альтернатив в многокритериальных задачах принятия решений / А.Н. Воронин // Кибернетика и системный анализ. – 2009. – № 1. – С. 117–122.

Р.В. Гришук

#### ИЕРАРХИЧЕСКАЯ ДИФФЕРЕНЦИАЛЬНО-ИГРОВАЯ МОДЕЛЬ ОЦЕНИВАНИЯ ЭФФЕКТИВНОСТИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Показано, что задача оценивания эффективности систем защиты информации сводится к построению соответствующей адекватной модели на основе векторного подхода. В качестве такой модели предложено иерархическую дифференциально-игровую модель. Для построения модели использованы методы дифференциально-игрового моделирования на основе дифференциальных преобразований и метод вложенных скалярных сверток. Приведено модельный пример.

**Ключевые слова:** иерархическая дифференциально-игровая модель, критерий, вложенная скалярная свертка, система защиты информации

R.V. Gryschuk

#### HIERARCHICAL DIFFERENTIAL-GAMING MODEL FOR EVALUATION EFFICIENCY OF INFORMATION SYSTEMS PROTECTION

It is shown that the solution to evaluate efficiency of information systems protection is amounted to a construction of the appropriate adequate model based on vector approach. The hierarchical differential-gaming model is offered as such tool. For the construction of model the methods of differential-gaming simulation based on differential transformations and method of embedded scalar convolution are applied. Model example is given.

**Keywords:** hierarchical differential-gaming model, criterion, embedded scalar convolution, information system protection

# МОДЕЛИРОВАНИЕ ПРОЦЕССА ПРОПИТКИ ГРУНТА ЧЕРЕЗ ОСНОВАНИЕ ЗЕМЛЯНОГО ГИДРОТЕХНИЧЕСКОГО СООРУЖЕНИЯ

С.А. Положаенко<sup>1</sup>, С.Д. Кузниченко<sup>2</sup>

<sup>1</sup> Одесский национальный политехнический университет,  
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: polozhaenko@mail.ru

<sup>2</sup> Одесский государственный экологический университет,  
ул. Львовская, 15, Одесса, 65016, Украина

Предложено решение задачи фильтрации жидкости через основание земляного гидротехнического сооружения с помощью метода математического и численного моделирования аномальных диффузионных процессов, основанного на применении и развитии аппарата вариационных неравенств.

**Ключевые слова:** аномальные диффузионные процессы, математическое моделирование, вариационные неравенства

## Постановка проблемы

Процесс просачивания жидкости через сложно структурированные пластовые горизонты можно отнести к классу диффузионных процессов, которые характеризуются аномальностью протекания физических явлений. Аномальность проявляется в нарушении линейного закона фильтрации – закона Дарси, и является характерной для определенных классов систем «жидкость / пористая среда». Аномальный характер протекания процесса диффузии в данном случае обусловлен приобретением жидкостью псевдопластических реологических свойств в результате взаимодействия с физической средой (например, глиной и глинизированными породами).

Рассмотрим земляное гидротехническое сооружение (бассейн) для которого построим математическую модель фильтрации жидкости через его основание. Выполним адаптацию данной математической модели к реальным условиям и проведем ее численное исследование, что важно на этапе проектирования гидротехнического сооружения для оценки возможного влияния пропитки на динамику уровня грунтовых вод.

По физике протекающих процессов данная модель описывает фильтрацию жидкости в скелете пористой среды. Особенностью предлагаемой математической модели может служить то, что поверхность раздела между влажной (пропитанной) и сухой частями грунта под основанием бассейна рассматривается как некоторая мембрана с односторонней проводимостью. Такое предположение вытекает из условия, что грунт под основанием бассейна имеет пусть малые, но конечные значения пористости и проницаемости [1]. В этом случае микроструктурирование грунта обуславливает существенно односторонний характер градиента пропитки под основанием бассейна.

Математически адекватным описанием данного физического процесса может служить аппарат вариационных неравенств, применяемый для построения математической модели реологии аномальных жидкостей [2].

## Материалы и методы исследования

При разработке математической модели будем использовать расчетную схему, представленную на рис. 1 (для простоты предлагается симметричность схемы бассейна).

Задача пропитки (фильтрации) ставится для бассейна, ограниченного с боковых сторон непроницаемыми плотинами, и достаточно протяженного по пространственной координате  $z_1$  (т.е. предполагается выполненным условие  $L \gg l$ ). Грунт под основанием бассейна имеет известные физические характеристики: пористость  $m(z)$  и проницаемость  $k(z)$  (рассматривается линейный случай). Основой для построения математической модели рассматриваемого процесса явились модели предложенные в [2, 3].

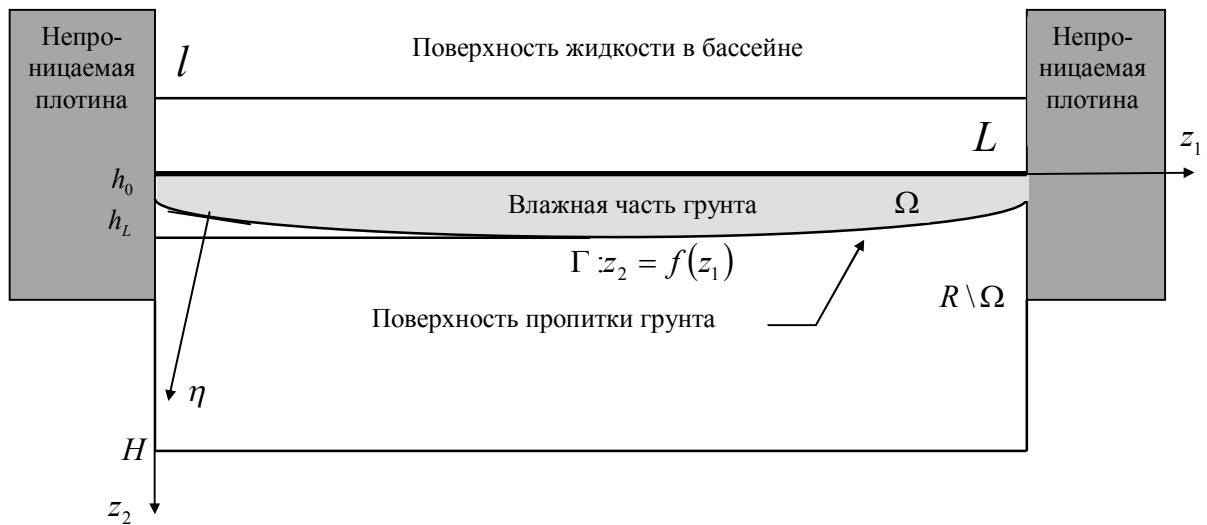


Рис. 1. Схема пропитки грунта под основанием бассейна

Предполагается, что задача рассматривается в прямоугольнике  $R = \phi(z), z = [z_1, z_2]$ , который является поперечным сечением под основанием плотины. Неизвестной в задаче является (в поперечном сечении) влажная часть  $\Omega \subset R$  грунта. Формализуем постановку задачи и приведем ее к вариационному неравенству.

Пусть  $L, h_L, h_0, H \in R$  — геометрические размеры пространственной области, причем  $L > 0$ ,  $0 < h_0 < H$ ,  $0 < h_L < H$ . Необходимо найти функцию  $z_2 = f(z_1)$ ,  $0 \leq z_1 \leq L'$ , с  $f(0) = h_0$  и  $f(z_1) > h$ , представляющую собой уравнение поверхности раздела влажной и сухой частей плотины ( $L' = 0.5L$  — ввиду симметричности схемы бассейна). При решении поставленной задачи воспользуемся функцией пьезометрического напора жидкости

$$u(z), \forall z \in \overline{\Omega},$$

где  $\overline{\Omega}$  — замыкание  $\Omega$  (т.е.  $\overline{\Omega} = \Omega \cup \Sigma$ );  $\Sigma$  — граница области  $\Omega$ .

Данное замечание следует из условия  $u(z) \equiv f(z_1)$ , причем, для неизвестной части  $\Gamma$  общей границы  $\Sigma$ , можно записать

$$\Gamma: z_2 = f(z_1), 0 < z_1 < L'. \quad (1)$$

Для определения множества функций, на котором будем искать решение задачи, введем в рассмотрение функцию  $v(z) = u(z) - f(z_1)$  и вариацию  $\zeta(z) = \min[u(z) - f(z_1)]$ ,

непрерывные на  $\overline{\Omega}$  и обращающиеся в нуль на границе  $\Gamma$ . Запишем очевидные соотношения

$$\begin{aligned} \int_R \left( \frac{\partial v}{\partial z_1} \cdot \frac{\partial \zeta}{\partial z_1} + \frac{\partial v}{\partial z_2} \cdot \frac{\partial \zeta}{\partial z_2} \right) dz &= \int_{\Omega} \left( \frac{\partial v}{\partial z_1} \cdot \frac{\partial \zeta}{\partial z_1} + \frac{\partial v}{\partial z_2} \cdot \frac{\partial \zeta}{\partial z_2} \right) dz = \\ &= \int_{\Omega} \left( \frac{\partial u}{\partial z_1} \cdot \frac{\partial \zeta}{\partial z_1} + \frac{\partial u}{\partial z_2} \cdot \frac{\partial \zeta}{\partial z_2} \right) dz_1 dz_2 - \int_{\Omega} \frac{\partial f(z_1)}{\partial z_2} \cdot \frac{\partial \zeta}{\partial z_2} dz. \end{aligned}$$

Первый член в последнем выражении тождественно равен нулю. Тогда окончательно можно записать

$$- \int_{\Omega} \frac{\partial f(z_1)}{\partial z_2} \cdot \frac{\partial \zeta}{\partial z_2} dz_1 dz_2 = - \int_R I_{\Omega} \frac{\partial \zeta}{\partial z_2} dz,$$

где  $I_{\Omega}$  – характеристическая функция в  $\Omega$ , причем она тождественно равна нулю везде на  $R \setminus \Omega$ , т.е. последний интеграл не равен нулю только в области  $\Omega$ .

Из приведенных соотношений очевидно равенство

$$- \left\{ \frac{\partial^2 [u - f(z_1)]}{\partial z_1^2} + \frac{\partial^2 [u - f(z_1)]}{\partial z_1^2} \right\} = \frac{\partial}{\partial z_2} I_{\Omega} \text{ в } R. \quad (2)$$

Задача (2) интегрируется

$$\omega(z) = \int_0^{f(z_1)} \{u(z) - f(z_1)\} dz_2, \quad \forall z \in \Omega$$

или, с учетом ранее принятых обозначений, имеем

$$- \left( \frac{\partial^2 \omega}{\partial z_1^2} + \frac{\partial^2 \omega}{\partial z_2^2} \right) = -I_{\Omega} \text{ в } R,$$

а значит,

$$- \left[ \frac{\partial^2 \omega}{\partial z_1^2} (v - \omega) + \frac{\partial^2 \omega}{\partial z_2^2} (v - \omega) \right] \geq -(v - \omega) \quad (3)$$

почти везде в  $R$  для любой  $v(z) \geq 0$  в  $R$ .

Таким образом, приходим к выводу, что в качестве выпуклого множества  $K$  допустимых функций для искомого вариационного неравенства необходимо взять множество неотрицательных  $\omega(z)$  с соответствующими граничными условиями:

$$\omega(0, z_2) = \begin{cases} \frac{1}{2L'} (h_0^2 - z_2^2), & 0 \leq z_2 \leq h_0, \\ 0, & h_0 < z_2 \leq H, \end{cases} \quad (4)$$



$$\omega(L', z_2) = \begin{cases} \frac{1}{2L'}(h_L^2 - z_2^2), & 0 \leq z_2 \leq h_L, \\ 0, & h_L < z_2 \leq H, \end{cases} \quad (5)$$

$$\omega(z_1, 0) = \frac{1}{2l}h_L^2 + [(h_0^2 - h_L^2)z_1], \quad 0 \leq z_1 \leq L'. \quad (6)$$

Таким образом, получено решение поставленной задачи в следующем виде. Для совокупности  $\{f, u\}$  при  $u(z) \in H^1(\Omega)$  (где  $H^1(\Omega)$  – гильбертово пространство непрерывно дифференцируемых функций) и гладкой  $f(z_1)$ , функция  $\omega(z)$  является решением следующей задачи Коши

$$\omega(z) = 0 \text{ на } \Gamma : z_2 = f(z_1), 0 < z_1 < L',$$

$$\frac{\partial \omega(z)}{\partial z_2} = \frac{\partial [u(z) - f(z_1)]}{\partial z_2} \text{ в } \Omega; \quad \omega(z) = 0, \quad \forall z \in R \setminus \Omega, \quad (7)$$

$$\omega(z) \in K : \int_R \left\{ \frac{\partial \omega}{\partial z_1} \left[ \frac{\partial (v - \omega)}{\partial z_1} \right] + \frac{\partial \omega}{\partial z_2} \left[ \frac{\partial (v - \omega)}{\partial z_2} \right] \right\} dz \geq - \int_R (v - \omega) dz, \quad \forall v(z) \in K,$$

где  $K$  определяет множество допустимых функций, причем функция  $\omega(z)$  – представляет собой искомое решение поставленной задачи реологии.

Неравенство (7), дает возможность отыскать неизвестную границу  $\Gamma : z_2 = f(z_1), 0 < z_1 < L'$ , представляющую собой поверхность раздела между влажной и сухой частями грунта под основанием бассейна.

Выполним адаптацию вариационного неравенства (7) для решения прикладных задач. Функцию пьезометрического давления  $u(z)$  выразим через физические величины и пространственные параметры, поддающиеся непосредственному измерению,

$$u(z) = l + \frac{m}{\gamma} P(z), \quad (8)$$

где  $l$  – уровень жидкости в бассейне (заметим, что математически  $l \equiv z_2$  или  $l = Cz_2$ );  $m$  – пористость грунта;  $\gamma$  – удельный вес жидкости;  $P(z)$  – функция давления жидкости в бассейне.

С учетом (8) запишем (7) относительно искомой функции  $f(z_1)$

$$\begin{aligned} f(z_1) \in K : \int_R \left\{ \left[ \frac{\partial Cz_2}{\partial z_1} + \frac{m}{\gamma} \frac{\partial P(z)}{\partial z_1} \right] - \frac{\partial f(z_1)}{\partial z_1} \right\} \left\{ \frac{\partial v}{\partial z_1} - \left[ \frac{\partial Cz_2}{\partial z_1} + \frac{m}{\gamma} \frac{\partial P(z)}{\partial z_1} \right] - \frac{\partial f(z_1)}{\partial z_1} \right\} + \\ + \left\{ \left[ C + \frac{m}{\gamma} \frac{\partial P(z)}{\partial z_2} \right] - \frac{\partial f(z_1)}{\partial z_2} \right\} \left\{ \frac{\partial v}{\partial z_2} - \left[ C + \frac{m}{\gamma} \frac{\partial P(z)}{\partial z_2} \right] - \frac{\partial f(z_1)}{\partial z_2} \right\} \right\} dz \geq \\ \geq \int_R \{v - [Cz_2 - f(z_1)]\} dz \quad \forall v(z) \in K, \end{aligned} \quad (9)$$

которое дополним граничным условием задачи Коши

$$f(z_1) = 0, \forall z \in R \setminus \Omega. \quad (10)$$

Неравенство (9) для граничного условия вида (10) решается с помощью подхода, предложенного в [4].

### Результаты исследования и их анализ

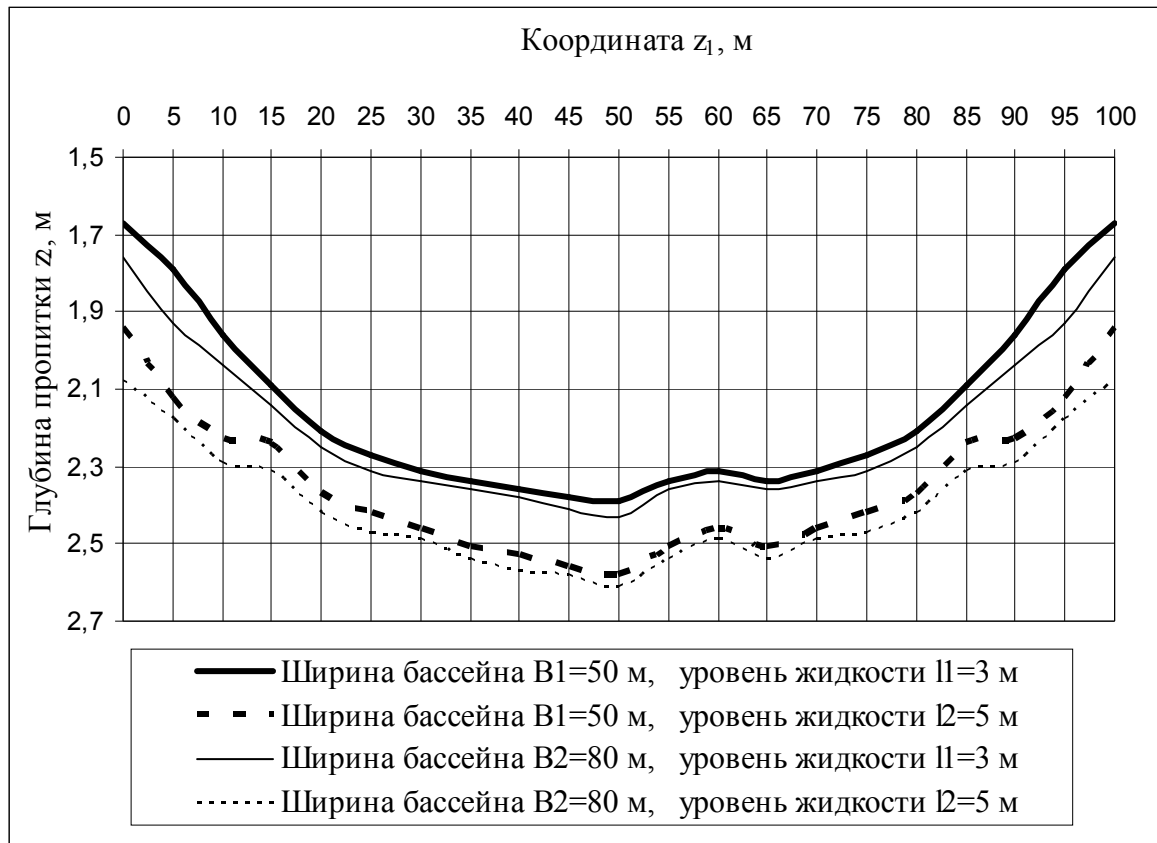
Используем расчетную схему (рис. 1) и соотношения (8)-(10) для моделирования процесса пропитки грунта под основанием бассейна прямоугольной формы при исходных данных в соответствии с табл. 1.

**Таблица 1.**

Исходные данные для моделирования процесса пропитки грунта под основанием гидротехнического сооружения (бассейна)

| № п/п | Наименование параметра                                 | Обозначение  | Единица измерения | Значение                 |
|-------|--------------------------------------------------------|--------------|-------------------|--------------------------|
| 1     | Длина бассейна                                         | $L$          | м                 | 100                      |
| 2     | Ширина бассейна                                        | $B$          | м                 | $B_1 = 50$<br>$B_2 = 80$ |
| 3     | Шаг дискретизации по пространственной координате $z_1$ | $\Delta z_1$ | м                 | 5                        |
| 4     | Уровень жидкости в бассейне                            | $l$          | м                 | $l_1 = 3$<br>$l_2 = 5$   |
| 5     | Пористость грунта                                      | $m$          | %                 | 15                       |
| 6     | Удельный вес жидкости                                  | $\gamma$     | кг/м <sup>3</sup> | 1000                     |
| 7     | Удельное давление жидкости                             | $P_y$        | кг/м <sup>2</sup> | 1000                     |

Моделирование выполним для двух значений уровня жидкости в бассейне  $l_1$  и  $l_2$ , а также для разных соотношений длины  $L$  и ширины  $B$  бассейна. Результаты моделирования приведены на рис. 2.



**Рис. 2.** Результати моделювання процесу пропитки ґрунту під основою гідротехнічного спорудження (басейна)

Анализ результатов моделирования позволяет сделать следующие выводы. Соотношение длины  $L$  и ширины  $B$  бассейна практически не влияет на глубину пропитки  $z_2$ , но заметно оказывает влияние на форму границы  $\Gamma: z_2 = f(z_1)$ ,  $0 < z_1 < L'$  (с ростом ширины  $B$  бассейна граница  $\Gamma$  имеет меньший “завал” вблизи стенок бассейна). Значительно большее влияние на глубину пропитки  $z_2$  оказывает уровень жидкости в бассейне  $l$ . Поэтому проводимые исследования должны быть учтены при анализе уровня грунтовых вод в месте строительства гидротехнического сооружения. Моделирование дает возможность оценить безопасный уровень жидкости в бассейне, обеспечивающий надежную сухую грунтовую прослойку между влажной пропитанной частью под его основанием и горизонтами грунтовых вод (последние могут быть определены пробными бурениями или моделированием).

### Список литературы

1. Киндерлерер Д. Введение в вариационные неравенства и их приложения / Д. Киндерлерер, Г. Стампакья. – М.: Мир, 1983. – 256 с.
2. Положаенко С.А. Модель процесса аномальной реологии с односторонней проводимостью границы // Труды Одесского политехнического университета. – 2000. – Вып. 1(10). – С. 124-129.
3. Положаенко С.А. Математическая модель фильтрации грунтовых вод для класса гидротехнических земляных сооружений // Вісник Одеської державної академії будівництва та архітектури. – 2005. – Вип. 17. – С. 206-210.
4. Верлань А.Ф. Математическое моделирование аномальных диффузионных процессов / А.Ф. Верлань, С.А. Положаенко, Н.Г. Сербов. – К.: Наукова думка, 2011. – 416 с.

С.А. Положаєнко, С.Д. Кузніченко

# МОДЕЛЮВАННЯ ПРОЦЕСУ ПРОСОЧЕННЯ ҐРУНТУ ЧЕРЕЗ ОСНОВУ ЗЕМЛЯНОЇ ГІДРОТЕХНІЧНОЇ СПОРУДИ

Розглянуто рішення задачі фільтрації рідини через основу земляної гідротехнічної споруди за допомогою методу математичного та чисельного моделювання аномальних дифузійних процесів на основі застосування і розвитку апарату варіаційних нерівностей.

**Ключові слова:** аномальні дифузійні процеси, математичне моделювання, варіаційні нерівності.

S. Polozhaenko, S. Kuznichenko

# MODELING OF GROUND ACROSS THE BASE IMPREGNATION GROUND WATER PLANTS

Proposed solution of the problem of fluid filtration through the bottom of an earthen hydraulic structures by using the mathematical and numerical modeling of anomalous diffusion processes based on the application and development apparatus of variational inequalities.

**Keywords:** anomalous diffusion processes, mathematical modeling, variational inequalities

# ТЕОРЕТИЧНІ ОСНОВИ ВИКОНАННЯ МОДУЛЯРНИХ ОПЕРАЦІЙ МНОЖЕННЯ ТА ЕКСПОНЕНЦІЮВАННЯ В ТЕОРЕТИКО–ЧИСЛОВОМУ БАЗИСІ КРЕСТЕНСОНА-РАДЕМАХЕРА

Я.М. Николайчук, М.М. Касянчук, І.З. Якименко, Т.М. Долинюк

Тернопільський національний економічний університет,  
вул. Львівська, 11, Тернопіль, 46020, Україна; email: kasyanchuk@ukr.net

Дана стаття ілюструє теоретичні основи виконання операцій модулярного множення та експоненціювання при застосуванні теоретико–числових базисів Радемахера та Крестенсона. Отримано нові аналітичні вирази обчислювальної складності запропонованих високопродуктивних алгоритмів.

**Ключові слова:** система залишкових класів, теоретико–числові базиси, базис Крестенсона, базис Радемахера, модулярне множення, модулярне експоненціювання

## Вступ

Аналіз наукових тенденцій розвитку теорії та перспективних інформаційних технологій покращення ефективності опрацювання інформаційних потоків в комп'ютерних мережах, проведений на основі новітніх публікацій, потребує поглибленого дослідження теоретичних засад базисів Крестенсона та Радемахера. Слід зауважити, що найбільш фундаментально досліджено цілочисельну форму в системі залишкових класів, яка утворюється на основі прямого перетворення теоретико-числового базису (ТЧБ) Крестенсона.

Тому є доцільним дослідити інші форми систем залишкових класів, які можуть бути використані для реалізації високопродуктивних алгоритмів модулярного множення та експоненціювання, а також виконати порівняльний аналіз різних ТЧБ з базисом Радемахера, який породжує двійкову систему числення на основі відповідних критеріїв.

## Постановка задачі та мета дослідження

Однією з найважливіших операцій у всіх асиметричних алгоритмах шифрування, зокрема RSA та Ель-Гамала, є модулярні операції множення та експоненціювання. Вони також лежать в основі алгоритмів електронного цифрового підпису, криптографічних протоколів, розв'язування задач обчислювальної, прикладної та дискретної математики [1], визначення стійкості еліптичних кривих методом пошуку їх порядку за допомогою алгоритму Шуфа [2] тощо. Існуючі алгоритми (стандартний, швидкого множення, Blakey, Монтгомері, бінарні і т.д. [3]) характеризуються значною обчислювальною складністю [4]. Для підвищення ефективності їх обчислення багатьма авторами запропоновано різні підходи, алгоритми, але в основному з використанням десяткової системи числення. Тому розробка ефективного алгоритму з використанням теоретико-числового базису Крестенсона [5] для зменшення алгоритмічної складності формуван-

ня, збільшення швидкодії на основі матричних моделей та розробка спеціалізованих програмно-апаратних засобів є актуальною задачею.

### Високопродуктивний алгоритм модулярного множення

Розглянемо два  $n$ -розрядних числа  $a = a_{n-1}2^{n-1} + \dots + a_i2^i + \dots + a_12 + a_0$  та  $b = b_{n-1}2^{n-1} + \dots + b_j2^j + \dots + b_12 + b_0$ , де  $a_i, b_j = 0, 1$ ,  $n$  – розрядність модуля  $p$ . Для знаходження результату їх множення за модулем  $p$  побудуємо матрицю, представлену в таблиці 1, де  $\|c_{ij}\| = 2^{i+j} \bmod p$ .

Добуток чисел  $a$  та  $b$  отримуємо за формулою [6]:

$$a \cdot b = \left( \sum_{i=1}^{n-1} \left( \sum_{j=1}^{n-1} a_i b_j \right) 2^{i+j} \bmod p \right) \bmod p, \quad (1)$$

де  $a_i, b_j = 1$ , тобто  $c_{ij}$  знаходиться на перетині стовбця та рядка, для яких відповідні  $a_i$  та  $b_j$  дорівнюють 1.

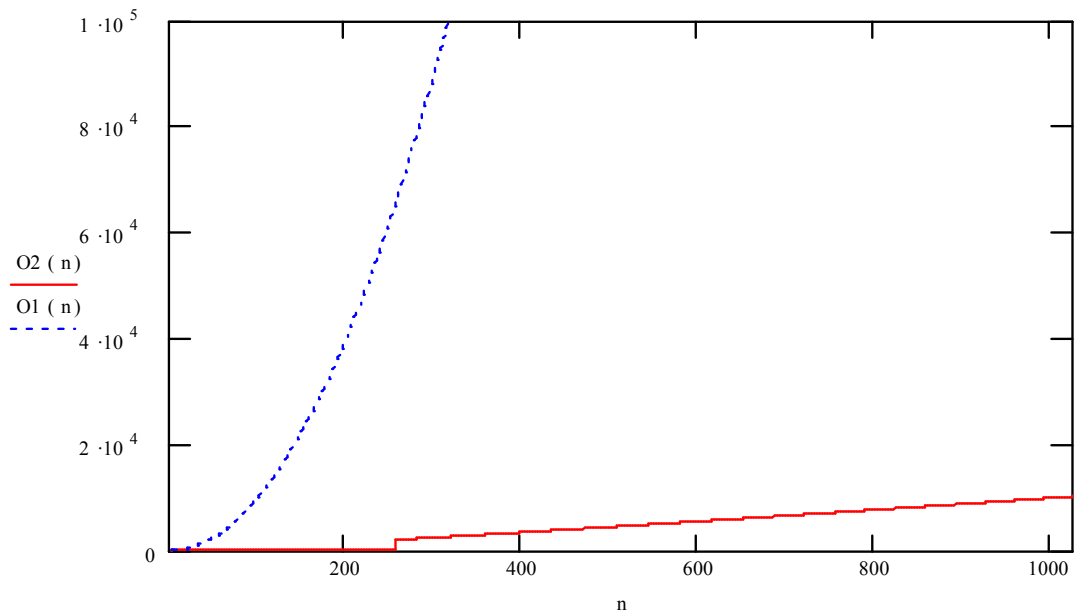
Таким чином, отриманий новий алгоритм заміни операції множення, яка має квадратичну обчислювальну складність  $O1(n) = n^2$ , операцією додавання з логарифмічною складністю  $O2(n) = \begin{cases} (\log_2 n)^2, & \text{якщо } n < 256 \\ n \cdot (\log_2 n), & \text{в інших випадках} \end{cases}$ .

Результати дослідження ефективності даного алгоритму наведені на рисунку 1.

**Таблиця 1.**

Матриця множення в базисі Радемахера–Крестенсона

|           |                |     |              |     |              |              |
|-----------|----------------|-----|--------------|-----|--------------|--------------|
|           | $b_{n-1}$      | ... | $b_j$        | ... | $b_1$        | $b_0$        |
| $a_{n-1}$ | $c_{n-1\ n-1}$ | ... | $c_{n-1\ j}$ | ... | $c_{n-1\ 1}$ | $c_{n-1\ 0}$ |
| ...       | ...            | ... | ...          | ... | ...          | ...          |
| $a_i$     | $c_{i\ n-1}$   | ... | $c_{ij}$     | ... | $c_{i1}$     | $c_{i0}$     |
| ...       | ...            | ... | ...          | ... | ...          | ...          |
| $a_1$     | $c_{1\ n-1}$   | ... | $c_{1j}$     | ... | $c_{11}$     | $c_{10}$     |
| $a_0$     | $c_{0\ n-1}$   | ... | $c_{0j}$     | ... | $c_{01}$     | $c_{00}$     |



**Рис. 1.** Обчислювальна складність операції модулярного множення

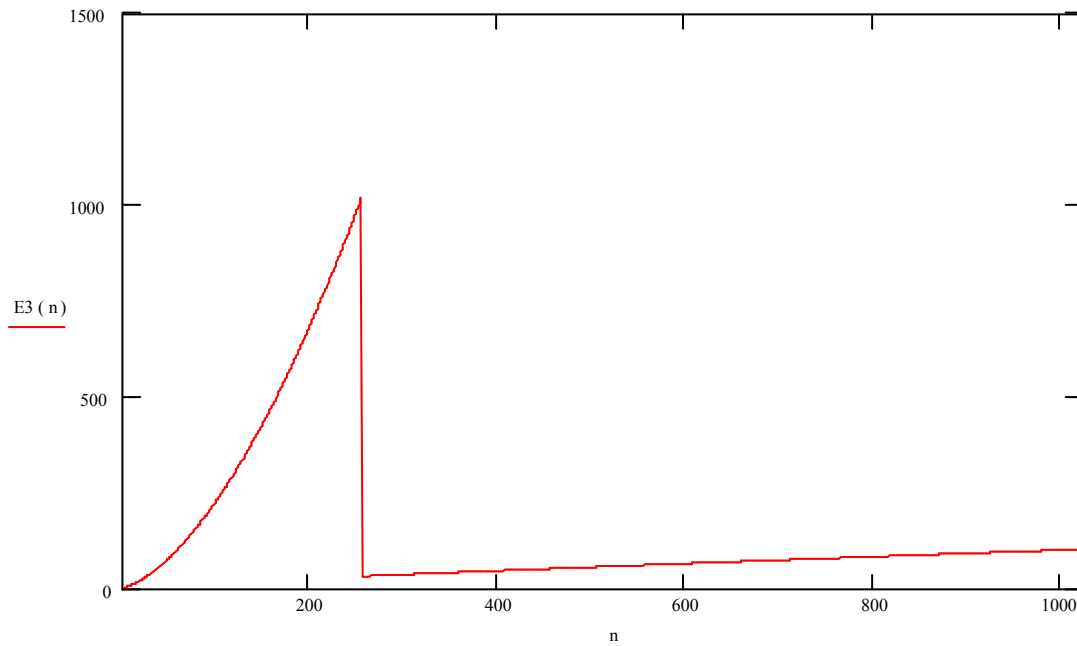
З рис. 1 видно, що при зростанні розрядності компонентів дискретного логарифма  $n > 256$  відомий алгоритм не може бути фізично реалізований з використанням сучасної мікропроцесорної техніки, особливо з врахуванням наступної операції піднесення до степеня, яка включає множення. А запропонований алгоритм з використанням базису Крестенсона дозволяє реалізувати можливості суттєвого підвищення захисту інформаційних потоків від несанкціонованого доступу, які характеризуються ознаками незворотності [7].

Ефективність запропонованого алгоритму модулярного множення буде визначатися як співвідношення обчислювальних складностей

$$E3(n) = \begin{cases} \frac{n^2}{(\log_2 n)^2}, & \text{якщо } n < 256 \\ \frac{n^2}{n \cdot \log_2 n}, & \text{в інших випадках} \end{cases} \quad (\text{рис.2}).$$

Результати чисельного експерименту показують, що при розмірності чисел від 0 до 256 бітів ефективність стрімко зростає, за рахунок переходу від двовимірного базису Радемахера, складність операції модулярного множення в якому мають квадратичну залежність, до розмежованої системи числення Радемахера-Крестенсона з логарифмічною складністю. А в діапазоні від 256 до 1024 біт в розмежованій системі числення складність операції множення буде лінійно-логіфімічною, тому що при реалізації запропонованого алгоритму операція додавання чисел великої розрядності більше 256 біт, яка замінює операцію множення у відомих алгоритмах, здійснюється не за один такт, як при менших розрядах, а за декілька тактів.

Отже, використання базису Крестенсона суттєво збільшує перспективи щодо розробки систем з високим рівнем захисту інформаційних потоків та дозволяє пришвидшити час виконання алгоритму модулярного множення.



**Рис. 2.** Ефективність алгоритму модулярного множення розмірності  $n$ .

### Високопродуктивний алгоритм модулярного експоненціювання

Для модулярного експоненціювання  $a^x \bmod p$ , де  $x = x_{n-1}2^{n-1} + \dots + x_i2^i + \dots + x_12 + x_0$  (вважаємо, що  $x \leq \varphi(p)$ ,  $\varphi(p)$  — значення функції Ейлера від модуля  $p$ ) використаємо проміжну матрицю, представлену в таблиці 2. Її розмірність дорівнює розрядності  $n$  модуля  $p$ . В стовбцях матриці записано величини  $a^{2^i} \bmod p$  в базисі Радемахера, тобто  $a_{ij} = 0, 1$ . Тоді будь-який степінь  $x$  можна записати за степенями 2 і шуканий результат можна отримати, перемноживши відповідну кількість стовбців за допомогою таблиці 2, та виразу:

$$a^x \bmod p = \left( \prod_{k=1}^{n-1} \left( \sum_{i=1}^{n-1} \sum_{j=1}^{n-1} (a_i a_j 2^{i+j}) \bmod p \right)^{x_k 2^k} \right) \bmod p \quad (2)$$

Пропонований алгоритм піднесення до степеня двійкового числа будь-якої розрядності за модулем  $p$  дозволяє зменшити алгоритмічну складність за рахунок заміни операції множення операцією додавання, підвищити швидкість на 30–40% (рис. 3), для чисел розрядності менше 256 біт, а в діапазоні від 256 біт — на 10%. Чисельний експеримент показав, що запропонований алгоритм піднесення до степеня двійкового числа будь-якої розрядності за модулем  $p$  в базисі Радемахера–Крестенсона дозволяє



зменшити складність з  $O3 = \frac{n^3}{2}$  до  $O4(n) = \begin{cases} \log_2 n \cdot \left(\frac{n}{2} \cdot \log_2 n + 1\right), & \text{якщо } n < 256 \\ n \cdot \left(\frac{n}{2} \cdot \log_2 n + 1\right), & \text{в інших випадках.} \end{cases}$  в

$$E2(n) = \begin{cases} \frac{n}{(\log_2 n)^2 + 2 \cdot \log_2 n}, & n < 256 \\ \frac{n}{(\log_2 n) + 2 \cdot \log_2 n}, & 256 \leq n \leq 1024 \end{cases} \text{ разів, що показано на рисунку 4.}$$

Таблиця 2.

Матриця піднесення до степеня в базисі Радемахера–Крестенсона

|                 |     |               |     |               |               |
|-----------------|-----|---------------|-----|---------------|---------------|
| $a_{n-1 \ n-1}$ | ... | $a_{i \ n-1}$ |     | $a_{1 \ n-1}$ | $a_{0 \ n-1}$ |
| ...             | ... | ...           | ... | ...           | ...           |
| $a_{n-1 \ j}$   | ... | $a_{i \ j}$   | ... | $a_{1 \ j}$   | $a_{0 \ j}$   |
| ...             | ... | ...           | ... | ...           | ...           |
| $a_{n-1 \ 1}$   | ... | $a_{i \ 1}$   | ... | $a_{1 \ 1}$   | $a_{0 \ 1}$   |
| $a_{n-1 \ 0}$   | ... | $a_{i \ 0}$   | ... | $a_{1 \ 0}$   | $a_{0 \ 0}$   |
| $a^{2^{n-1}}$   | ... | $a^{2^i}$     | ... | $a^{2^1}$     | $a^{2^0}$     |

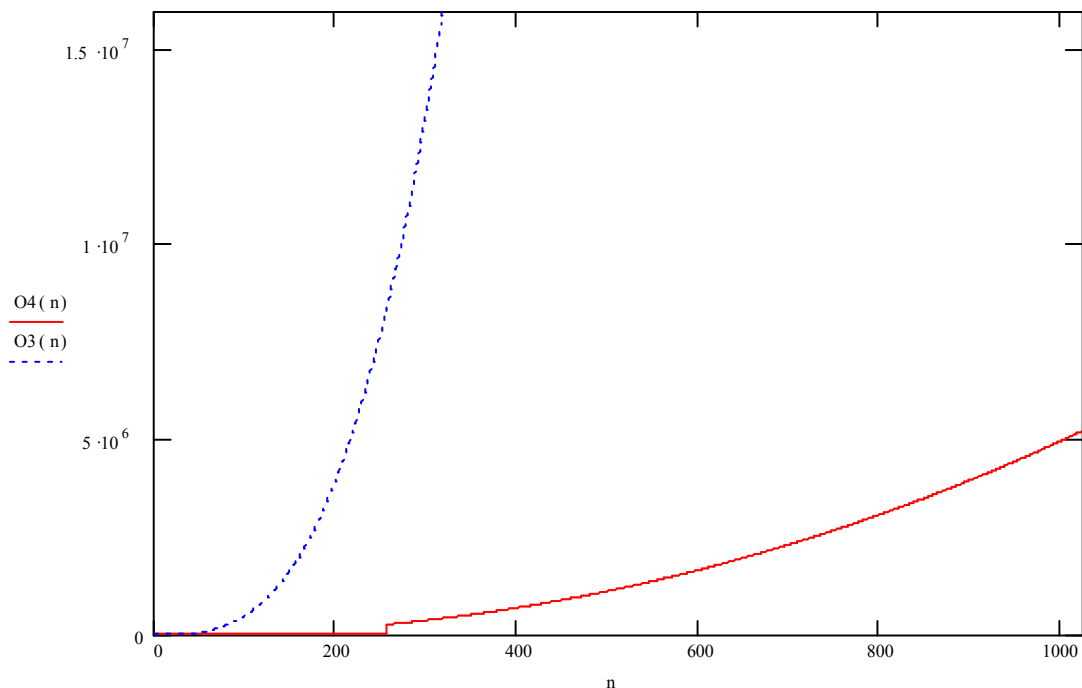
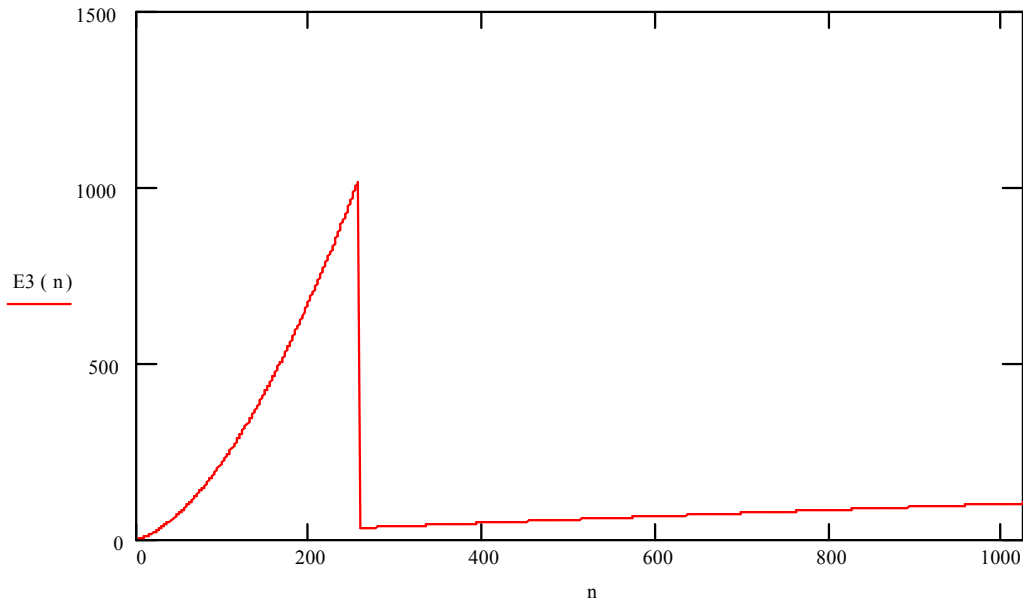


Рис. 3. Алгоритмічна складність операції модулярного піднесення до степеня

Отже, наведені дослідження показують, що запропонований алгоритм є ефективнішим для знаходження значення операції піднесення до степеня двійкового числа будь-якої розрядності за модулем  $p$ . Слід зазначити, що при збільшенні розрядності

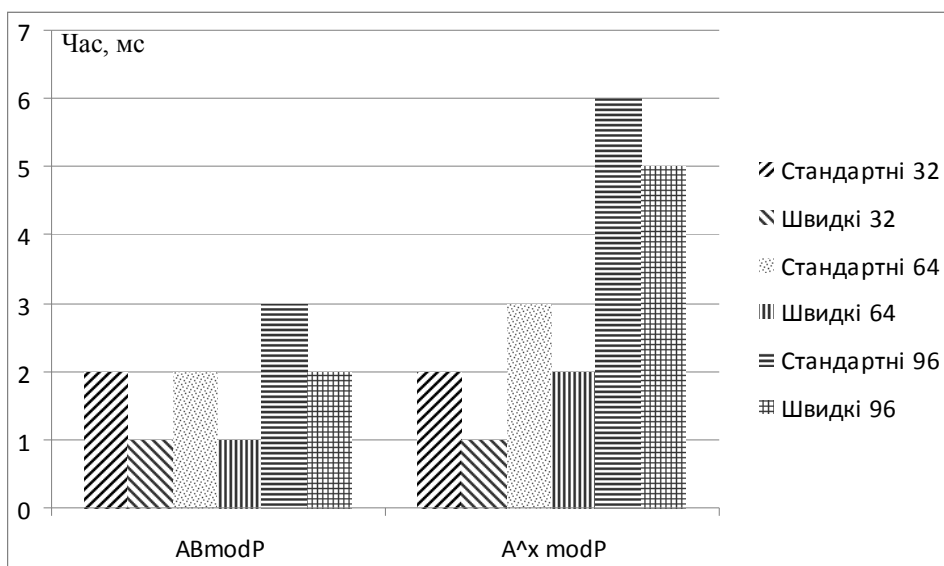
чисел зменшується ефективність (рисунок 4), бо частина ресурсу комп'ютера буде задіяна на обслуговування службової інформації, що значно збільшує складність і кількість операцій та зменшує швидкість.



**Рис. 4.** Ефективність запропонованого алгоритму

#### Експериментальне порівняння швидкодії стандартного та запропонованого алгоритмів

Експериментальні дослідження швидкодії стандартного та запропонованого алгоритмів для чисел різної розрядності (32, 64 та 96 біт) проводилися на комп'ютері з дво-ядерним процесором типу Intel з тактовою частотою 2,3 ГГц, оперативна пам'ять становила 2 Гбайт. Результати цих досліджень представлені на рисунку 5.



**Рис. 5.** Експериментальне порівняння швидкодії стандартного та запропонованого алгоритмів для чисел різної розрядності

Як видно з гістограми, запропоновані алгоритми потребують менше часу для виконання розглянутих операцій. При збільшенні розрядності ефективність алгоритму збільшується.

## Висновки

У роботі представлено теоретичні основи та нові ефективні алгоритми модулярного множення та експоненціювання в ТЧБ Радемахера–Крестенсона, що дозволило зменшити складність з поліноміально-експоненційної до лінійно–логарифмічної за рахунок заміни операції множення з наскрізними переносами на операцію додавання і, відповідно, збільшити швидкодію рішення задач даного класу.

## Список літератури

1. Романец Ю.В. Защита информации в компьютерных системах и сетях [Текст] : монография / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин ; под ред. В.Ф. Шаньгина. – М. : Радио и связь, 1999. – 328 с.
2. Kinakh I. Reliability of Schoof algorithm and its computational complexity / I. Kinakh, I. Iakymenko / The Experience of Designing and Application of CAD Systems in Microelectronics: Proceedings of the Xth International Conference – Lviv: Publishing House Vezha&Co, 2009. – p. 107.
3. Montgomery P.L. Modular multiplication without trial division // Mathematics of Computation. – 1985. – Vol.44, No.170. – PP. 519-521.
4. Задірака В.К. Комп'ютерна арифметика багаторозрядних чисел [Текст] / В.К. Задірака, О.С. Олексюк ; Ін-т кібернетики ім. В.М. Глушкова НАН України, Тернопільська академія народного господарства. – К. : Б.в., 2003. – 264 с.
5. Николайчук Я.М. Теоретичні основи базисних перетворень СЗК / Я.М. Николайчук, Ю.С. Федорович // Матеріали наукової конференції «Автоматика 2000». – Львів, 2000. – С. 120.
6. Yakymenko I. Matrix algorithms of processing of the information flow in computer systems based on theoretical and numerical Krestenson's basis / I. Yakymenko M. Kasyanchuk, Y. Nykolajchuk // TCSET'2010, February 23-27, 2010: Proceedings of Conference – Lviv-Slavske, Ukraine. – p. 241.
7. Николайчук Я.М. Теорія джерел інформації [Текст] : монографія / Я.М. Николайчук. – Вид. 2-е, випр. – Тернопіль : Терно-граф, 2010. – 536 с.

Я.Н. Николайчук, М.Н. Касянчук, И.З. Якименко, Т.Н. Долинюк  
ТЕОРЕТИЧЕСКИЕ ОСНОВАНИЯ ВЫПОЛНЕНИЯ МОДУЛЯРНЫХ ОПЕРАЦИЙ  
УМНОЖЕНИЯ И ЭКСПОНЕНЦИИРОВАНИЯ В ТЕОРЕТИКО–ЧИСЛОВОМ БАЗИСЕ  
РАДЕМАХЕРА–КРЕСТЕНСОНА

В данной статье изложены теоретические основания выполнения операций модулярного умножения и экспоненцирования при использовании теоретико-числовых базисов Радемахера и Крестенсона. Получены новые аналитические выражения вычислительной сложности предложенных высокопродуктивных алгоритмов.

**Ключевые слова:** система остаточных классов, теоретико-числовые базисы, базис Крестенсона, базис Радемахера, модулярное умножение, модулярное экспоненцирование

Ya. Nykolajchuk, M. Kasyanchuk, I. Yakymenko, T. Dolynyuk  
THEORETICAL BASES OF EXECUTION MODULAR MULTIPLICATION  
OPERATIONS AND EXPONENTIATION USING A THEORETICAL-NUMBERS BASES  
OF RADEMACHER-KRESTENSON

This article are shown theoretical bases of modular multiplication operations and exponentiation using a theoretical-numbers bases of Rademacher and Krestenson. It's authors created new analytical expressions calculation complexity of high speed algorithms.

**Keywords:** system of residual classes, theoretical-numbers bases, bases of Krestenson, bases of Rademacher, modular multiplication, modular exponentiation

# ВИРІШЕННЯ ПРОБЛЕМИ ЗМЕНШЕННЯ РІВНЯ СПОТВОРЕНЬ ВЕКТОРНИХ ЗОБРАЖЕНЬ ВНАСЛІДОК ВБУДОВУВАННЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ

В.В. Карпінець, Ю.Є. Яремчук

Вінницький національний технічний університет,  
вул. Хмельницьке шосе, 95, Вінниця, 21021, Україна; e-mail: yurevyar@gmail.com

У роботі розглянуто метод захисту векторних зображень цифровими водяними знаками (ЦВЗ) із забезпеченням зменшення впливу його вбудовування на якість зображення. Також розглянуто метод, який забезпечує вбудовування бітів ЦВЗ лише у ті матриці коефіцієнтів дискретного косинусного перетворення (ДКП), зміна яких не призводить до значних відхилень координат точок зображення. Було проведено аналіз стійкості запропонованого методу до найпоширеніших зловмисних атак, спрямованих на знищення чи підміну ЦВЗ, результати якого показали достатній рівень стійкості на рівні з відомими методами. У роботі також проведено аналіз обчислювальної складності запропонованого методу та порівняння з відомим методом.

**Ключові слова:** стеганографія, цифровий водяний знак, захист авторського права, дискретне косинус-перетворення, векторні зображення

## Вступ

На сьогодні в системах передавання інформації все більшого поширення отримують цифрові зображення векторного формату, що використовуються для проектування архітектурних об'єктів, інтер'єрів, розробки приладів, реклами, логотипів, створення шрифтів, географічних карт тощо, на створення яких витрачається багато часу та коштів. В зв'язку з цим виникає проблема, пов'язана з можливістю нелегального копіювання та розповсюдження векторних зображень, які мають свого правовласника.

Для вирішення задачі захисту авторських прав цифрових векторних зображень використовуються стеганографічні системи цифрових водяних знаків (ЦВЗ), що дають змогу маркувати об'єкти захисту для подальшого виявлення неправомірного використання зображення [1].

Залежно від того, яка інформація потрібна системі для того, щоб виявити ЦВЗ – оригінал зображення, ЦВЗ, секретний ключ чи додаткова інформація, вони поділяються на чотири типи: конфіденційні, напівконфіденційні, напіввідкриті та відкриті стеганосистеми [1]. Найбільш перспективними є відкриті стеганосистеми, які для своєї роботи, окрім секретного ключа, не вимагають ні знання оригінального зображення, ні вбудованого ЦВЗ, що полегшує процедуру підтвердження авторських прав.

Серед існуючих методів, що не потребують для витягнення ЦВЗ оригіналу зображення чи додаткової інформації, найбільшого поширення отримали методи, які базуються на частотних перетвореннях [2]. До таких методів відносяться методи Базіна-Барса-Маделана, Хе-Жу-Ванга, Солачідіса-Ніколаїдіса-Пітаса, Войт-Янга-Буша [3] та ін. Проте основною проблемою цих методів при вбудовуванні ЦВЗ є погіршення якості зображення, яка проявляється в зміні контурів об'єктів, чи їх положення внаслідок зміни координат точок. Причому для векторних зображень, що відображають реальні

об'єкти в масштабі (архітектурні споруди, механічні та електронні прилади, географічні карти тощо), ця проблема є дуже актуальною, бо суттєва зміна координат точок може спотворити інформацію про існуючі об'єкти чи вплинути на їх створення. Тому актуальними є дослідження, спрямовані на розробку методів, що для витягнення ЦВЗ не потребують оригіналу векторного зображення, в яких вирішувалась б указана проблема.

### Метод вбудовування ЦВЗ у векторні зображення зі зменшеним рівнем спотворень внаслідок вбудовування

У роботі [4] запропоновано стеганографічний метод вбудовування ЦВЗ у векторні зображення зі зменшенням рівня спотворень зображення внаслідок вбудовування ЦВЗ, який для витягування ЦВЗ не потребує оригіналу зображення чи самого ЦВЗ. Особливістю методу є використання двовимірного ДКП для матриць розміром  $8 \times 8$  та зміна в них високочастотних коефіцієнтів залежно від біту ЦВЗ та двох додаткових ВЧ-коефіцієнтів на середньоарифметичне значення цих коефіцієнтів збільшене або зменшене на величину  $P$ , яка забезпечує ідентифікацію бітів при витягуванні ЦВЗ.

Згідно з запропонованим методом зображення представляється у вигляді одновимірного масиву  $V$ , в якому елементами є точки векторного зображення  $V_l$ , де  $l = 1..N$ ,  $N$  – кількість точок в масиві.  $V_l = (X_l, Y_l)$ , де  $X_l, Y_l$  – значення координати точки  $V_l$  векторного зображення. Далі формуються матриці розміром  $8 \times 8$  з кожних 64 координат точок масиву  $V$ , які позначено, як  $C_i(x, y)$ , де  $i = 1..t$ ,  $t$  – кількість сформованих матриць,  $x, y$  – позиції координат в цій матриці. Для кожної матриці  $C_i(x, y)$  проводиться пряме двовимірне ДКП, в результаті чого отримуються матриці коефіцієнтів  $F(u, v)$ , де  $u, v$  – позиції цих коефіцієнтів в матриці.

Було запропоновано умови для вбудовування ЦВЗ, що дозволяють незначно змінювати координати точок зображення. При цьому для вбудовування одного біту ЦВЗ змінюється значення одного високочастотного (ВЧ) коефіцієнта  $F_i(u_1, v_1)$  матриці ДКП залежно від значень двох ВЧ-коефіцієнтів  $F_i(u_2, v_2)$  та  $F_i(u_3, v_3)$ . Вбудовування бітів ЦВЗ  $m_j$ , де  $i = 1..q$ ,  $q$  – кількість біт ЦВЗ, здійснюється таким чином. Якщо біт  $m_j = 0$ , то перевіряється умова:

$$F_i(u_1, v_1) < \frac{F_i(u_2, v_2) + F_i(u_3, v_3)}{2}. \quad (1)$$

Якщо умова (1) виконується, значення коефіцієнта  $F_i(u_1, v_1)$  залишається без змін, інакше значення коефіцієнта  $F_i(u_1, v_1)$  у матриці  $F_i(u, v)$  з вбудованим бітом ЦВЗ отримується таким чином:

$$F_i(u_1, v_1) = \frac{F_i(u_2, v_2) + F_i(u_3, v_3)}{2} - P. \quad (2)$$

Величина  $P$  використовується для забезпечення чіткої ідентифікації бітів ЦВЗ при витягуванні.

Якщо при вбудовуванні біт ЦВЗ  $m_j = 1$ , то перевіряється виконання такої умови:

$$F_i(u_1, v_1) > \frac{F_i(u_2, v_2) + F_i(u_3, v_3)}{2}. \quad (3)$$

Якщо умова (3) виконується, то коефіцієнт  $F_i(u_1, v_1)$  буде дорівнювати значенню коефіцієнта  $F_i(u_1, v_1)$ , інакше:

$$F_i(u_1, v_1) = \frac{F_i(u_2, v_2) + F_i(u_3, v_3)}{2} + P. \quad (4)$$

Після зміни коефіцієнтів проводиться обернене дискретне косинус-перетворення над матрицями змінених коефіцієнтів  $F'(u, v)$  і отримані змінені координати записуються у файл векторного зображення з вбудованим ЦВЗ.

Витягування ЦВЗ з векторного зображення проводиться без наявності оригіналу зображення чи самого ЦВЗ таким чином. Спочатку з масиву точок векторного зображення з вбудованим ЦВЗ  $V'$  формуються матриці  $C'_i(x, y)$  розміром  $8 \times 8$ , де  $i' = 1..t'$ ,  $t'$  – кількість сформованих матриць. Далі над матрицями  $C'(x, y)$  проводиться пряме двовимірне ДКП.

Після вибору позицій трьох ВЧ-коефіцієнтів  $F'_i(u'_1, v'_1)$ ,  $F'_i(u'_2, v'_2)$  та  $F'_i(u'_3, v'_3)$  перевіряється виконання умов та визначається відповідне значення біту ЦВЗ  $m'_{j'}$ :

$$\begin{cases} m'_{j'} = 0, & \text{якщо } F'_i(u'_1, v'_1) < \frac{F'_i(u'_2, v'_2) + F'_i(u'_3, v'_3)}{2} \\ m'_{j'} = 1, & \text{якщо } F'_i(u'_1, v'_1) > \frac{F'_i(u'_2, v'_2) + F'_i(u'_3, v'_3)}{2} \end{cases}. \quad (5)$$

Далі витягнуті біти  $m'_{j'}$ ,  $j' = 1..q'$ , перетворюються у формат представлення ЦВЗ.

Для запропонованого методу розроблено схему та алгоритми вбудовування і витягування ЦВЗ.

Проведений аналіз запропонованого методу з точки зору впливу ЦВЗ на якість зображення на прикладі векторної географічної карти показав, що використання двовимірного ДКП та умов зміни коефіцієнтів ДКП (1)-(4) вбудовування ЦВЗ забезпечує зменшення рівня спотворень векторних зображень внаслідок вбудовування ЦВЗ порівняно з існуючими методами, однак можливі випадки значних відхилень окремих точок [5].

Для усунення таких випадків у роботі [6] запропоновано метод відбору придатних для вбудовування ЦВЗ матриць коефіцієнтів ДКП, особливістю якого є те, що вбудовування бітів ЦВЗ пропонується здійснювати лише у ті матриці коефіцієнтів ДКП, зміна яких не призводить до значних відхилень координат точок зображення. При цьому визначення придатних для вбудовування матриць пропонується здійснювати на основі запропонованих умов їх відбору з використанням граничного значення  $P_h$  величини зміни коефіцієнтів внаслідок вбудовування ЦВЗ. Тобто, після проведення ДКП перевіряються такі умови:

$$|F_i(u_1, v_1) - F_i(u_2, v_2)| \leq P_h, \quad (6)$$

$$|F_i(u_1, v_1) - F_i(u_3, v_3)| \leq P_h. \quad (7)$$

Якщо хоч одна з умов (6)-(7) не буде виконуватись, вибрані коефіцієнти не будуть використовуватись для вбудовування, а відповідна їм матриця  $F_i(u, v)$  буде вважатися не придатною для вбудовування.

Проведений аналіз показав, що запропонований метод з використанням методу відбору придатних матриць ДКП забезпечує зменшення максимального відхилення значень координат точок векторних зображень внаслідок вбудовування ЦВЗ до 20 разів, а також їх рівномірне відхилення відносно точок оригіналу векторного зображення.

У випадку, коли кількість бітів ЦВЗ більша ніж кількість придатних для вбудовування матриць  $F_i(u, v)$ , то можна збільшити граничне значення  $P_h$ . Однак, в цьому випадку виникає необхідність передавання  $P_h$  разом з маркованим векторним зображенням, що потребує додаткових прихованих каналів передачі.

Для вирішення проблеми виникнення таких випадків вдосконалено запропонований метод вбудовування ЦВЗ забезпеченням придатності матриць шляхом зміни в кожній не більше двох коефіцієнтів, що приймають участь у вбудовуванні ЦВЗ, без зміни граничного значення  $P_h$ . При цьому величина зміни кожного коефіцієнта є не більшою ніж  $P_h$ , що дозволяє зберегти достатній рівень якості зображення. Для забезпечення придатності потрібно виконати перевірку та зміну коефіцієнтів за такими формулами:

$$\begin{aligned} &\text{Якщо } [P_h < |F_i(u_1, v_1) - F_i(u_2, v_2)| \leq 2P_h] \text{ та } [P_h < |F_i(u_1, v_1) - F_i(u_3, v_3)| \leq 2P_h], \text{ то,} \\ &\left\{ \begin{array}{l} \text{якщо } [F_i(u_1, v_1) > F_i(u_2, v_2)] \text{ та } [F_i(u_1, v_1) > F_i(u_3, v_3)], \text{ то зменшити } F_i(u_1, v_1) \text{ на } P_h; \\ \text{якщо } [F_i(u_1, v_1) < F_i(u_2, v_2)] \text{ та } [F_i(u_1, v_1) < F_i(u_3, v_3)], \text{ то збільшити } F_i(u_1, v_1) \text{ на } P_h; \\ \text{якщо } [F_i(u_1, v_1) > F_i(u_2, v_2)] \text{ та } [F_i(u_1, v_1) < F_i(u_3, v_3)], \text{ то збільшити } F_i(u_2, v_2) \text{ на } P_h \\ \hspace{15em} \text{та зменшити } F_i(u_3, v_3) \text{ на } P_h; \\ \text{якщо } [F_i(u_1, v_1) < F_i(u_2, v_2)] \text{ та } [F_i(u_1, v_1) > F_i(u_3, v_3)], \text{ то зменшити } F_i(u_2, v_2) \text{ на } P_h \\ \hspace{15em} \text{та збільшити } F_i(u_3, v_3) \text{ на } P_h. \end{array} \right. \end{aligned}$$

$$\begin{aligned} &\text{Якщо } [|F_i(u_1, v_1) - F_i(u_2, v_2)| \leq P_h] \text{ та } [P_h < |F_i(u_1, v_1) - F_i(u_3, v_3)| \leq 2P_h], \text{ то,} \\ &\left\{ \begin{array}{l} \text{якщо } [F_i(u_1, v_1) > F_i(u_3, v_3)], \text{ то збільшити } F_i(u_3, v_3) \text{ на } P_h; \\ \text{якщо } [F_i(u_1, v_1) < F_i(u_3, v_3)], \text{ то зменшити } F_i(u_3, v_3) \text{ на } P_h. \end{array} \right. \end{aligned}$$

$$\begin{aligned} &\text{Якщо } [P_h < |F_i(u_1, v_1) - F_i(u_2, v_2)| \leq 2P_h] \text{ та } [|F_i(u_1, v_1) - F_i(u_3, v_3)| \leq P_h], \text{ то,} \\ &\left\{ \begin{array}{l} \text{якщо } [F_i(u_1, v_1) > F_i(u_2, v_2)], \text{ то збільшити } F_i(u_2, v_2) \text{ на } P_h; \\ \text{якщо } [F_i(u_1, v_1) < F_i(u_2, v_2)], \text{ то зменшити } F_i(u_2, v_2) \text{ на } P_h. \end{array} \right. \end{aligned}$$

Таке вдосконалення не зменшує стеганографічну стійкість самого методу вбудовування ЦВЗ, при цьому зміна не більше двох коефіцієнтів забезпечує в цілому зменшення спотворення зображення.

### Аналіз запропонованого методу вбудовування ЦВЗ у векторні зображення щодо рівня спотворень векторних зображень

У роботі [7] проведено аналіз запропонованого методу вбудовування ЦВЗ у векторні зображення щодо рівня спотворення зображень внаслідок вбудовування ЦВЗ та порівняння його з відомим методом Войта-Янга-Буша, який базується на одновимірному



му ДКП. Аналіз проведено для декількох типів векторних географічних карт, різних ЦВЗ за розміром і форматом, який показав, що запропонований метод забезпечує середнє відхилення координат точок менше до 30 разів, а середню похибку відхилень координат точок до 4 разів порівняно з відомим методом.

Також проведено аналіз запропонованого методу для вбудовування ЦВЗ при використанні відбору придатних матриць коефіцієнтів ДКП та порівняння його, коли відбір придатних матриць не проводиться, а також у порівнянні з відомим методом Войта-Янга-Буша, результати якого наведені у таблиці 2. Аналіз показав, що використання умов відбору придатних матриць ДКП забезпечує зменшення максимального відхилення координат точок до 20 разів, ніж без використання, та до 70 разів порівняно з відомим методом Войта-Янга-Буша. При цьому сумарна похибка та середнє відхилення координат точок менші до 15 разів. Також отримано ряд показників відмінності та кореляційних показників, що використовуються для оцінювання стеганографічних методів, результати за основними з яких наведені у таблиці 1.

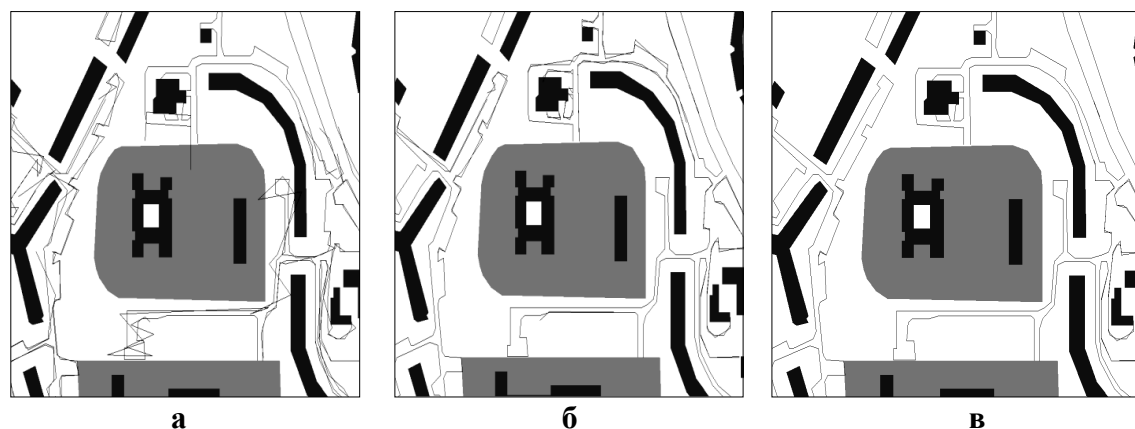
Таблиця 1.

Показники візуального спотворення зображення після вбудовування ЦВЗ

| Показники                                      | Оригінальне зображення |          | Метод Войта-Янга-Буша<br>$A_4 \dots A_6$ |                         | Запр. метод вбуд. ЦВЗ<br>$P = 0,00003$ |                         | Запр. метод вбуд. ЦВЗ з відбором придатних матриць<br>$P = 0,00003$<br>$P_h = 0,0005$ |                         |
|------------------------------------------------|------------------------|----------|------------------------------------------|-------------------------|----------------------------------------|-------------------------|---------------------------------------------------------------------------------------|-------------------------|
|                                                | Y                      | X        | Y                                        | X                       | Y                                      | X                       | Y                                                                                     | X                       |
| Максимальна відмінність, $MD$                  | 0                      | 0        | 0.078                                    | 0.11                    | 0.016                                  | 0.019                   | $2.316 \times 10^{-3}$                                                                | $2.657 \times 10^{-3}$  |
| Нормована середньо-квадратична помилка, $NMSE$ | 0                      | 0        | $3.25 \times 10^{-11}$                   | $1.735 \times 10^{-10}$ | $1.392 \times 10^{-12}$                | $5.441 \times 10^{-12}$ | $2.833 \times 10^{-14}$                                                               | $1.017 \times 10^{-13}$ |
| Відношення "сигнал-шум", $SNR$                 | $\infty$               | $\infty$ | $3.077 \times 10^{10}$                   | $5.764 \times 10^9$     | $7.183 \times 10^{11}$                 | $1.838 \times 10^{11}$  | $3.53 \times 10^{13}$                                                                 | $9.832 \times 10^{12}$  |
| Максимальне відношення "сигнал-шум", $PSNR$    | $\infty$               | $\infty$ | $3.081 \times 10^{10}$                   | $5.795 \times 10^9$     | $7.192 \times 10^{11}$                 | $1.848 \times 10^{11}$  | $3.534 \times 10^{13}$                                                                | $9.885 \times 10^{12}$  |
| Якість зображення, $IF$                        | 1                      | 1        | 0.99999999<br>99675032                   | 0.99999999<br>9826503   | 0.99999999<br>99986078                 | 0.99999999<br>9994559   | 0.99999999<br>99999717                                                                | 0.99999999<br>9999898   |
| Нормована взаємна кореляція, $NC$              | 1                      | 1        | 0.99999999<br>99941283                   | 0.99999999<br>99672231  | 0.99999999<br>99990318                 | 0.99999999<br>99965551  | 0.99999999<br>99999879                                                                | 0.99999999<br>99998924  |

З таблиці 1 видно, що запропонованому методу з використанням відбору придатних матриць відповідають найкращі показники відмінності порівняно з відомим методом Войта-Янга-Буша. Отримані кореляційні показники показують менші порушення кореляції між точками зображення внаслідок вбудовування ЦВЗ до 30 разів, що також показує підвищення стійкості запропонованого методу до зловмисних атак.

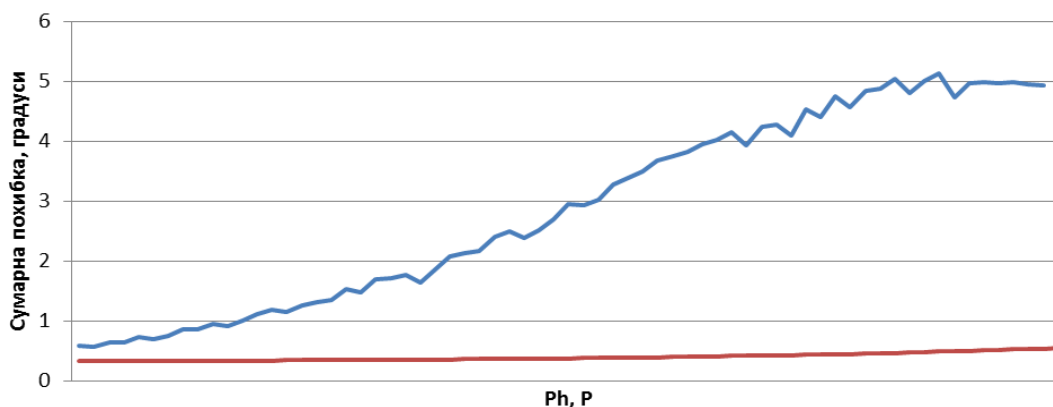
Також було проведено аналіз візуального рівня спотворення зображень на основі сумішених зображень оригіналу векторної карти та з вбудованим ЦВЗ згідно з запропонованим методом, з використанням відбору придатних матриць та методом Войта-Янга-Буша (рис. 1).



**Рис. 1.** Фрагменти векторних карт після вбудовування ЦВЗ суміщених з оригіналом за трьома методами: а – метод Войта-Янга-Буша; б – запропонований метод вбудовування ЦВЗ; в – запропонований метод вбудовування ЦВЗ з методом відбору придатних матриць

З рисунку 1 видно, що запропонований метод з використанням методу відбору придатних матриць забезпечує найменший рівень спотворення зображення серед розглянутих методів.

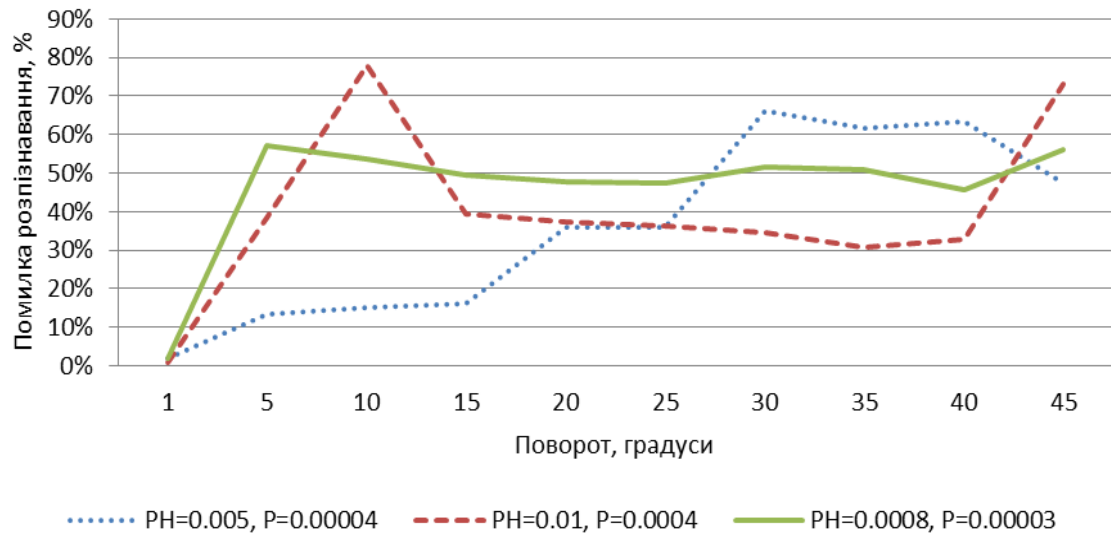
Проведено аналіз впливу величин  $P_h$  та  $P$  на спотворення зображення та розмір ЦВЗ, який показав, що при збільшенні величини  $P_h$  збільшується можливий для вбудовування розмір ЦВЗ, сумарна похибка та максимальне відхилення координат точок, а величина  $P$  незначно впливає на ці показники, оскільки згідно запропонованого методу її значення у десятки чи сотні разів менші від  $P_h$  (рис. 2).



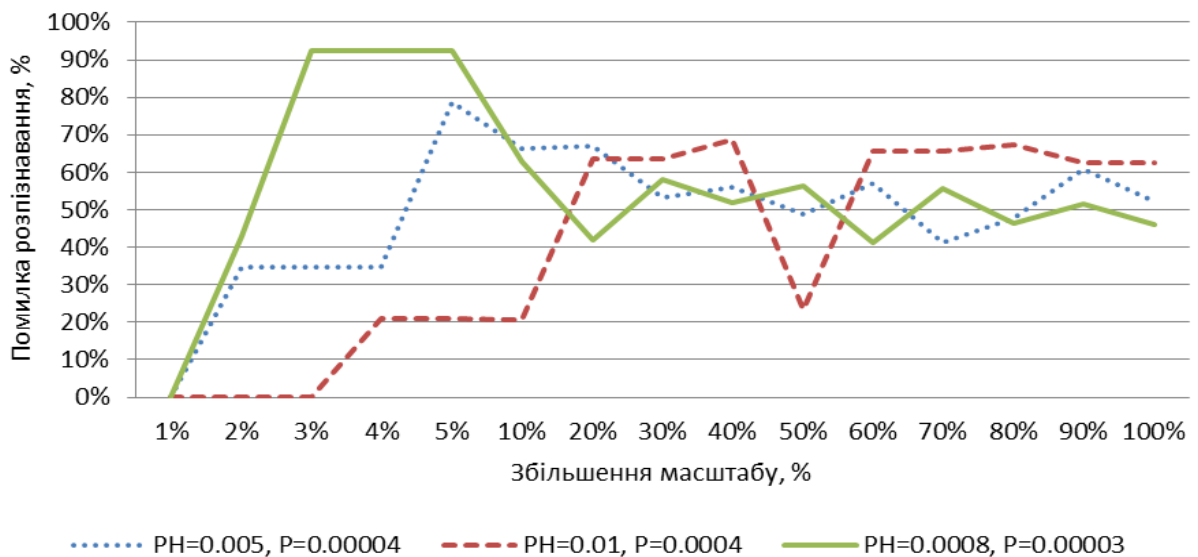
**Рис. 2.** Графік залежності сумарної похибки координат точок від  $P$  та  $P_h$

### Аналіз стійкості запропонованого методу вбудовування ЦВЗ до зловмисних активних та пасивних атак

Проведений аналіз стійкості запропонованого методу до активних зловмисних атак, спрямованих на ускладнення витягнення ЦВЗ правовласником, показав достатньо високий рівень стійкості методу, зокрема до повороту зображення (при повороті на 15 градусів похибка розпізнавання бітів склала 16%), до масштабування зображення (при масштабуванні на 3% і 100% помилка розпізнавання склала 0% та 55% бітів відповідно), а також абсолютну стійкість до зміщення векторного зображення (рис. 3,4).



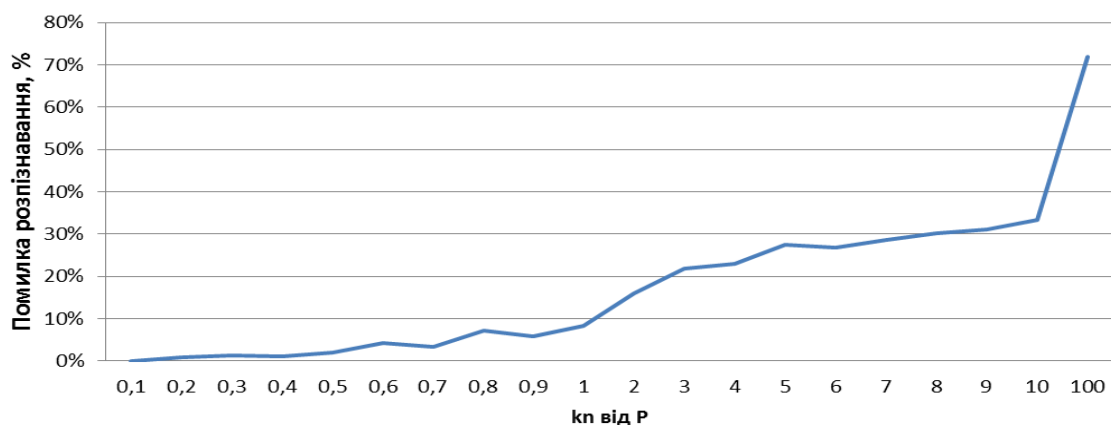
**Рис. 3.** Залежність помилок розпізнавання ЦВЗ від повороту зображення



**Рис. 4.** Залежність помилок розпізнавання ЦВЗ від масштабування зображення

Аналіз стійкості запропонованого методу до атаки внесення додаткового шуму показав, що при внесенні шуму зі збільшенням сумарної похибки відхилень координат від початкової у 5.7 разів (повна деградація зображення) помилка розпізнавання складає усього 33.46% неправильно розпізнаних бітів (рис. 5).

Стійкість до відсікання зображення може забезпечуватись шляхом вбудовування бітів ЦВЗ у певні блоки зображення із використанням точок інтересу POI.

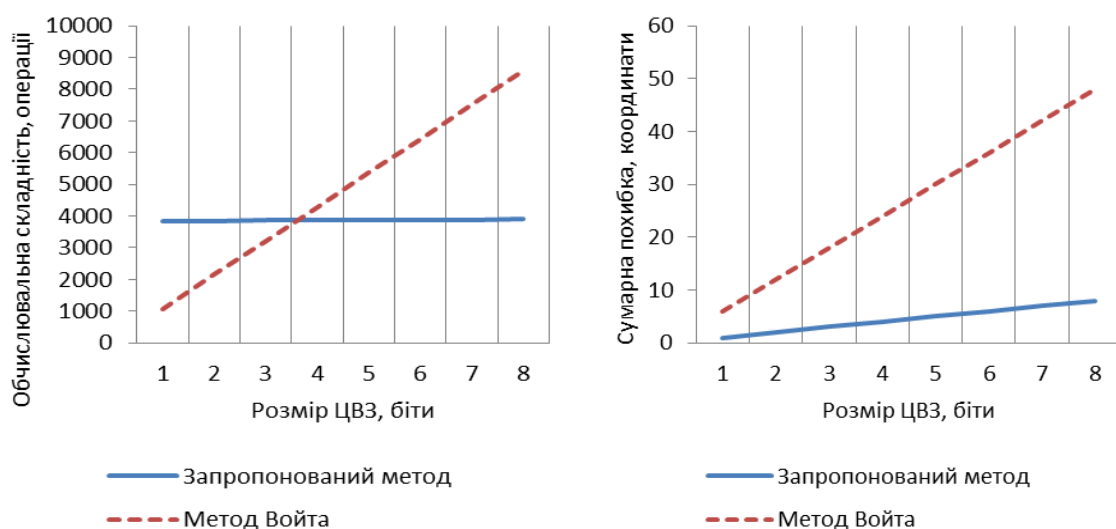


**Рис. 5.** Залежність помилок розпізнавання ЦВЗ від рівня шуму

### Аналіз обчислювальної складності запропонованого методу вбудовування ЦВЗ

Проведений аналіз обчислювальної складності запропонованого методу вбудовування ЦВЗ показав, що вбудовування ЦВЗ потребує у 2 рази більше арифметичних операцій ніж для витягування, що пояснюється необхідністю виконання за методом більше 90% операцій для проведення ДКП, яке при вбудовуванні виконується два рази, а при витягуванні ЦВЗ лише один.

Також було проведено порівняння обчислювальної складності з відомим методом Войта-Янга-Буша, результати якого показали, що запропонований метод має у 3 рази більшу обчислювальну складність процесу вбудовування та витягування ЦВЗ. Однак запропонований метод дає суттєві переваги, оскільки в ньому використовується двовимірне ДКП і 1 біт ЦВЗ вбудовується у блок з 64 коефіцієнтів, а це забезпечує менший рівень спотворень та кращу стійкість то пасивних атак шляхом статистичного дослідження. Крім того, якщо згідно запропонованого методу в одну матрицю ДКП вбудувати більшу кількість бітів ЦВЗ, то його обчислювальна складність буде незначно збільшуватись, в той час як складність методу Войта-Янга-Буша буде прямо пропорційно зростати кількості вбудовуваних ЦВЗ (рис.6).



**Рис. 6.** Залежність обчислювальної складності та сумарної похибки від кількості бітів для запропонованого методу та методу Войта-Янга-Буша

Так, зокрема при вбудовуванні 8 бітів ЦВЗ запропонований метод при достатньому рівні стійкості буде забезпечувати майже у 2 рази меншу обчислювальну складність ніж метод Войта-Янга-Буша і при цьому буде мати менший рівень спотворення зображення внаслідок вбудовування ЦВЗ.

## Висновки

В роботі розглянуто метод захисту векторних зображень цифровими водяними знаками із забезпеченням зменшення впливу його вбудовування на якість зображення. Особливістю методу є те, що використання в ньому двовимірного ДКП для матриць розміром  $8 \times 8$  та вбудовування бітів ЦВЗ шляхом незначної зміни в них високочастотних коефіцієнтів дозволяють забезпечити зменшення рівня спотворення зображення внаслідок вбудовування ЦВЗ порівняно з відомими методами.

Також розглянуто метод, який забезпечує вбудовування бітів ЦВЗ лише у ті матриці коефіцієнтів ДКП, зміна яких не призводить до значних відхилень координат точок зображення. Для визначення придатних для вбудовування матриць запропоновано умови відбору з використанням граничного значення величини зміни коефіцієнтів внаслідок вбудовування ЦВЗ. Також було розглянуто метод для збільшення кількості придатних матриць при однаковому граничному значенні. Метод дозволив збільшувати кількість придатних матриць зміною не більше двох коефіцієнтів, причому у більшості випадків лише одного.

Результати проведених досліджень рівня спотворення векторних зображень внаслідок вбудовування ЦВЗ показали, що запропонований метод забезпечує менші значення сумарної похибки відхилень координат точок, максимального відхилення координат точок, а також ряду показників відмінності та кореляційних показників у порівнянні з аналогами.

Проведено аналіз стійкості запропонованого методу до активних зловмисних атак, спрямованих на ускладнення витягнення ЦВЗ правовласником, зокрема до атак на основі афінних перетворень та атаки внесенням шуму. Результати дослідження показали, що запропонований метод забезпечує абсолютну стійкість до зміщення векторного зображення. Також метод забезпечує достатньо високий рівень стійкості до повороту та масштабування зображення. Аналіз стійкості запропонованого методу до атаки шляхом внесення додаткового шуму показав, що при внесенні шуму такого рівня, при якому сумарна похибка відхилень координат є більшою від початкової у 5,7 разів, що призводить до повної деградації зображення, помилка розпізнавання складає усього 33,46% неправильно розпізнаних бітів.

Проведено аналіз обчислювальної складності запропонованого методу та порівняння з відомим методом Войта-Янга-Буша. Результати аналізу показали, що у випадку, коли 1 біт ЦВЗ вбудовувати у матрицю коефіцієнтів розміром  $8 \times 8$  обчислювальна складність запропонованого методу є більшою у 3 рази, ніж вбудовування 1 біту ЦВЗ у один одновимірний масив з 8 коефіцієнтів ДКП згідно відомого методу. Однак при рівних умовах, якщо згідно запропонованого методу вбудовувати в одну двовимірну матрицю ДКП 8 бітів ЦВЗ, то його обчислювальна складність буде майже у 2 рази меншою ніж методу Войта-Янга-Буша, і при цьому запропонований метод буде забезпечувати менший рівень спотворення зображення внаслідок вбудовування ЦВЗ. Навіть у випадку, якщо вбудовувати лише 4 біти ЦВЗ в одну матрицю згідно запропонованого методу, то його обчислювальна складність та рівень спотворення будуть меншими порівняно з відомим методом.

## Список літератури

1. Хорошко В.О. Основи комп'ютерної стеганографії : Навчальний посібник / В.О. Хорошко, О.Д. Азаров, М.Є. Шелест, Ю.Є. Яремчук. – Вінниця: ВДТУ. – 2003. – 143 с.
2. Zheng L. Research on vector map digital watermarking technology / L. Zheng, Y. Jia, Q. Wang // Proceedings of the 2009 First International Workshop on Education Technology and Computer Science. – 2009. – PP. 303-307.
3. Voigt M. Reversible watermarking of 2D vector data / M. Voigt, B. Yang and C. Busch // ACM Multimedia and Security Workshop. – 2004. – PP. 160-165.
4. Карпинець В.В. Вирішення проблеми погіршення якості векторних зображень при вбудовуванні цифрових водяних знаків / В.В. Карпинець, Ю.Є. Яремчук // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2010. – № 1. – С. 73-83.
5. Карпинець В.В. Аналіз впливу цифрових водяних знаків на якість векторних зображень / В.В. Карпинець, Ю.Є. Яремчук // Сучасний захист інформації. – 2011. – №1. – С. 72-82.
6. Карпинець В.В. Зменшення відхилень координат точок внаслідок вбудовування цифрових водяних знаків у векторні зображення / В.В. Карпинець, Ю.Є. Яремчук // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2010. – № 2. – С. 69-78.
7. Карпинець В.В. Аналіз рівня спотворень векторних зображень внаслідок вбудовування цифрових водяних знаків / В.В. Карпинець, Ю.Є. Яремчук // Сучасний захист інформації. – 2011. – №2. – С. 94-99.

В.В. Карпинець, Ю.Є. Яремчук

### РЕШЕНИЕ ПРОБЛЕМЫ УМЕНЬШЕНИЯ УРОВНЯ ИСКАЖЕНИЙ ВЕКТОРНЫХ ИЗОБРАЖЕНИЙ В РЕЗУЛЬТАТЕ ВСТРАИВАНИЯ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ

В работе рассмотрен метод защиты векторных изображений цифровыми водяными знаками (ЦВЗ) с обеспечением уменьшения влияния его внедрения на качество изображения. Также рассмотрен метод, который обеспечивает внедрение битов ЦВЗ только в те матрицы коэффициентов дискретного косинусного преобразования (ДКП), изменение которых не приводит к значительным отклонениям координат точек изображения. Был проведен анализ устойчивости предложенного метода к распространенным вредоносным атакам, направленных на уничтожение или подмену ЦВЗ, результаты которого показали достаточный уровень устойчивости на уровне с известными методами. В работе также проведен анализ вычислительной сложности предложенного метода и сравнение с известным методом.

**Ключевые слова:** стеганография, цифровой водяной знак, защита авторского права, дискретное косинус-преобразование, векторные изображения

V. Karpinets, Y. Yaremchuk

### SOLUTION TO REDUCING DISTORTION VECTOR IMAGES DUE EMBEDDING DIGITAL WATERMARKS

In this work observed the method for vector graphics of digital watermarks ensuring mitigation of its embedding image quality. Also considered a method that provides embedded bits Manezh Central only those matrix coefficients of discrete cosine transform (DCT), a change which does not lead to significant deviations of coordinates of image points. It analyzed the stability of the proposed method to the most common malicious attacks aimed at the destruction or substitution digital watermark, the results of which showed a sufficient level of stability at the level of known methods. We also analyzed the computational complexity of the proposed method and comparison with the known method.

**Keywords:** steganography, digital watermark, copyright protection, discrete cosine transform, vector image

# THE SIGNIFICANCE OF GEODESIC MAPPINGS OF RIEMANNIAN SPACES IN GRAVITATION THEORY

Leonid V. Verozub

V.N. Karazin Kharkiv National University,  
Svobody Sq., 4, Kharkiv, 61022, Ukraine; e-mail: leonid.v.verozub@univer.kharkov.ua

In this paper we examine the consequences of the fact that many of the space-time metrics that are solutions of the Einstein equations are the geodesic (projective) equivalent to one-parameter set of other metrics, which generally are not solutions of these equations.

**Keywords:** geodesic mappings, Einstein equations, gravitation theory

## Introduction

The equations of motion of test bodies play a fundamental role in the classical field theory. They give evidence for the existence of the field and allow us to find its properties. The functions appearing in these equations are characteristics of the field.

In the case of gravity, the gravitational equations of motion of test particles are invariant under some group of transformations of the Christoffel symbols  $\Gamma_{\beta\gamma}^{\alpha}$  – of geodesic transformations [1]:

$$\bar{\Gamma}(x)_{\beta\gamma}^{\alpha} = \Gamma(x)_{\beta\gamma}^{\alpha} + \psi_{\beta}(x)\delta_{\gamma}^{\alpha} + \psi_{\gamma}(x)\delta_{\beta}^{\alpha}, \quad (1)$$

where  $\psi_{\alpha}(x)$  is an arbitrary gradient covector field. It is easiest to see it, if the coordinate  $t = x^0/c$  is used as a parameter in geodesic line:

$$\ddot{x}^{\alpha} + (\Gamma_{\beta\gamma}^{\alpha} - c^{-1}\Gamma_{\beta\gamma}^0 \dot{x}^{\alpha}) \dot{x}^{\beta} \dot{x}^{\gamma} = 0. \quad (2)$$

It seems obvious that the Christoffel symbols  $\bar{\Gamma}_{\beta\gamma}^{\alpha}(x)$  and  $\Gamma_{\beta\gamma}^{\alpha}(x)$  describe the same physical gravitational field, just as the 4-potentials in classical electro-dynamics, connected by a gauge transformation  $A_{\beta} \rightarrow A_{\beta} + \partial_{\beta}\phi(x)$ .

Such a gauge transformation of the Christoffel symbols induces a corresponding transformation of the metric tensor  $g_{\mu\nu}$ , the curvature tensor  $R_{\alpha\beta\gamma}^{\delta}$ , and the Ricci tensor  $R_{\alpha\beta}$ . So, all these objects in themselves have no more physical meaning than 4-potentials  $A_{\mu}$  in electrodynamics. Evidently due to this fact the equations of gravitational field, based on the hypothesis on free motion on geodesic lines, must be invariant under the geodesic (projective) transformations. It is well known that even vacuum Einstein's equations do not satisfy this condition [2].<sup>1</sup>

<sup>1</sup> We mean the original Einstein's equations, and not frequently considered its mathematical generalization

In Riemannian space-time, eqs.(1) are equivalent to the mappings of the space-time  $V$  with the metric tensor  $g(x)_{\alpha\beta}$  to the space-time  $\bar{V}$  with the metric tensor  $\bar{g}(x)_{\alpha\beta}$  defined by the following PDE:

$$\bar{g}(x)_{\alpha\beta;\gamma} = 2\psi(x)_{\gamma} \bar{g}_{\alpha\beta}(x) + \psi(x)_{\alpha} \bar{g}_{\gamma\beta}(x) + \psi(x)_{\beta} \bar{g}_{\alpha\gamma}(x), \quad (3)$$

where a semicolon denotes a covariant derivative with respect to  $x^{\alpha}$  in  $V$ . There exists extensive literature on the investigation of the possibility of geodesic mapping  $V \rightarrow \bar{V}$  based on these equations [4].

Consequently, every solution of Einstein's equations in any coordinate system gives in general only one of many physically equivalent metrics [5].

### FRW metric

It is recently this fact has been discovered independently in [6] for the case of the FRW metric. It was noted in this paper (and after that in [7]) that the line element of this cosmological model admits one-parameter transformations of the metric tensor that leaves unchanged non parameterized geodesics.

But the truth is that this is not a random fact. This is not a specifics of the FRW metric. The truth is that the metric, Christoffel symbols, or the curvature tensor define the gravity field only up to geodesic transformations, which should play the role of gauge transformations in any geometrical theory of gravitation [5].

Due to simplicity of the FRW metric, consideration of the consequences of such geodesic equivalence of metrics is especially simple.

Consider the line elements of a Riemannian space-time  $V$  :

$$ds^2 = b(t)dt^2 + a(t)\sigma_{ik}(x^1, x^2, x^3)dx^i dx^k. \quad (4)$$

It is known [3] that geodesics of such metric are the same as the ones of the space-time  $\bar{V}$  with the line element

$$\bar{ds}^2 = B(t)dt^2 + A(t)\sigma_{ik}(x^1, x^2, x^3)dx^i dx^k, \quad (5)$$

where

$$B(t) = \frac{b(t)}{[1 + qa(t)]^2}, \quad (6)$$

$$A(t) = \frac{a(t)}{1 + qa(t)}, \quad (7)$$

and  $q$  is an arbitrary constant.

Consider briefly the proof of this important fact.

Contracting (2) with respect to  $\alpha$  and  $\beta$ , we obtain  $\bar{\Gamma}_{\beta\gamma}^{\beta} = \Gamma_{\beta\gamma}^{\beta} + (n+1)\psi_{\beta}$ .

Consequently,



$$\psi_{\beta} = \frac{1}{2(n+1)} \frac{\partial}{\partial x^{\beta}} \left| \frac{\det \bar{g}}{\det g} \right|, \quad (8)$$

which shows that in the case under consideration only 0-component of  $\psi_{\alpha}$  is other than zero.

The useful for us components of the Christoffel symbols of  $V$  are:

$$\bar{\Gamma}_{00}^0 = b'(t)/2b, \quad \bar{\Gamma}_{11}^0 = a'(t)/2b(t), \quad \bar{\Gamma}_{10}^1 = a'(t)/2a(t),$$

and the same components of  $\bar{V}$ :

$$\bar{\Gamma}_{00}^0 = B'(t)/2B, \quad \bar{\Gamma}_{11}^0 = -A'(t)/2B(t), \quad \bar{\Gamma}_{10}^1 = A'(t)/2A(t). \quad (9)$$

Then eqs. (1) gives the following equations

$$\frac{A'(t)}{A(t)} - \frac{a'(t)}{a(t)} = 2\psi_0, \quad (10)$$

$$\frac{B'(t)}{B(t)} - \frac{b'(t)}{b(t)} = 4\psi_0, \quad (11)$$

$$\frac{A'(t)}{B(t)} - \frac{a'(t)}{b(t)} = 0. \quad (12)$$

Therefore,  $A/a = \exp(2 \int \psi(t)_0 dt)$ ,  $B/b = \exp(4 \int \psi(t)_0 dt)$  where the integration constants are equal to 1 because at  $\psi(t)_0 = 0$  the functions  $A(t) = a(t)$  and  $B(t) = b(t)$ . Consequently,  $B(t)/b(t) = (A(t)/a(t))^2$ , and with (12) we obtain the differential equations

$$A'(x) - A(t)^2 \frac{a'(t)}{a(t)} = 0, \quad (13)$$

which gives (7). Now from previous equation we obtain the function  $B(t)$  in the form (6).

On the contrary, if in eq. (1) to set  $\psi_i = 0$  for  $i = 1, 2, 3$ , and  $\psi_0 = -\frac{1}{2} \partial \ln(1 + qb(t)) / \partial t$ , then eqs. (10), (11), and (12) are satisfied. Thus, with this choice of the convector field  $\psi(x)_{\alpha}$ , the line element (4) at  $b = -1$  is equivalent to (5). In other words, the both line elements have the same equations of motion of test particles.

### Schwarzschild metric

As another example, we show here that a static centrally symmetric metric

$$ds^2 = b(r)dr^2 + r^2(d\theta^2 + \sin^2 \theta d\phi^2) - a(r)dr^2, \quad (14)$$

(in particular, Shvartsschild metric) is not unique. Namely, in a given coordinate system it has common geodesic lines with a metric of the form

$$\overline{ds}^2 = B(r)dr^2 + F(r)^2(d\theta^2 + \sin^2 \theta d\phi^2) - A(r)dt^2, \quad (15)$$

where  $A(x); B(x)$  and  $F(x)$  are functions of  $r$ , depending on a continuous parameter.

The Christoffel symbols for (14) is given by

$$\Gamma_{rr}^r = \frac{1}{2} \frac{b'(r)}{b(r)}, \quad \Gamma_{r\theta}^\theta = \frac{1}{r}, \quad \Gamma_{r\phi}^\phi = \frac{1}{r}, \quad \Gamma_{rt}^t = \frac{1}{2} \frac{a'(r)}{a(r)}, \quad \Gamma_{\theta\theta}^r = \frac{r}{b(r)}, \quad (16)$$

$$\Gamma_{\theta\phi}^\phi = \frac{\cos \theta}{\sin \theta}, \quad \Gamma_{\phi\phi}^r = -\frac{r \sin^2 \theta}{b(r)}, \quad \Gamma_{\phi\phi}^\theta = -\sin \theta \cos \theta, \quad \Gamma_{tt}^r = \frac{1}{2} \frac{a'(r)}{b(r)}. \quad (17)$$

The Christoffel symbols for 15 are:

$$\overline{\Gamma}_{rr}^r = \frac{1}{2} \frac{B'(r)}{B(r)}, \quad \overline{\Gamma}_{r\theta}^\theta = \frac{F'(r)}{F(r)}, \quad \overline{\Gamma}_{r\phi}^\phi = \frac{F'(r)}{F(r)}, \quad \overline{\Gamma}_{rt}^t = \frac{1}{2} \frac{A'(r)}{A(r)}, \quad \overline{\Gamma}_{\theta\theta}^r = -\frac{F(r)F'(r)}{B(r)}, \quad (18)$$

$$\overline{\Gamma}_{\theta\phi}^\phi = \frac{\cos \theta}{\sin \theta}, \quad \overline{\Gamma}_{\phi\phi}^r = -\frac{F(r)F'(r)\sin^2 \theta}{B(r)}, \quad \overline{\Gamma}_{\phi\phi}^\theta = -\sin \theta \cos \theta, \quad \overline{\Gamma}_{tt}^r = \frac{1}{2} \frac{A'(r)}{B(r)}, \quad (19)$$

where a prime here and later denotes a derivative with respect to  $r$ .

In view of this, Levi-Civita equations (1) yield:

$$\frac{B'(r)}{B(r)} - \frac{b'(r)}{b(r)} = 4\psi_r(r), \quad F(r)F'(r)b(r) - rB(r) = 0, \quad A'(r)b(r) - a'(r)B(r) = 0, \quad (20)$$

$$\frac{F'(r)}{F(r)} - \frac{1}{r} = \psi_r(r), \quad \frac{A'(r)}{A(r)} - \frac{a'(r)}{a(r)} = 2\psi_r(r), \quad \psi_\theta(r) = \psi_\phi(r) = \psi_t(r) = 0. \quad (21)$$

According to (8) the function  $\psi_r(r)$  can be written as

$$\psi_r = \partial \ln \chi / \partial r,$$

where

$$\chi(r) = \left( \frac{\overline{g}}{g} \right)^{1/2(n+1)}.$$

Consequently,

$$B = b\chi^4; \quad A = a\chi^2; \quad F = \chi;$$

$$A = a'\chi^4; \quad (F^2)' = 2r\chi^4.$$

Formulas for the function  $F(r)$  are compatible only if the functions  $\chi(r)$  are the solution of the differential equations

$$r\chi'(r) + \chi(r) - \chi(r)^3 = 0$$

which yields

$$\chi(r) = (1 + kr^2)^{1/2},$$

where  $k$  is an arbitrary constant.

As a result, formulas which express the  $A(x)$ ;  $B(x)$  and  $F(x)$  by  $a(r)$  and  $b(r)$  are given by

$$A(r) = \frac{a(r)}{1 + kr^2}, \quad B(r) = \frac{b(r)}{(1 + kr^2)^2}, \quad F(r) = \frac{r}{(1 + kr^2)^{1/2}}, \quad (22)$$

where  $k$  is a constant satisfying appropriate physical conditions.

## Discussion

It is obvious that the geodesics (projective) mappings of Riemannian spaces should be considered as gauge transformations of the differential equation, which is used to determine the geometrical characteristics of gravity in any theory based on Einstein's hypothesis of the motion of test bodies along geodesics of Riemannian space.

The fact that the connection coefficients and the metric tensor are determined up to an arbitrary geodesic mapping, does not mean that our physical space-time has a projective symmetry. No doubt the physical space-time is locally pseudo-Euclidean and the notion of length has a physical sense. This fact means that the geometric characteristics of the physical space-time (the coefficient of the connection or metric tensor) can not be directly identified with the characteristics of the gravitational field, they are not observable variables of the field. Such variables must be geodesically invariant.

However, the possibility to define observable variables of gravitational field exists. For example, although Christoffel symbols are not be viewed as the observable characteristics of gravity, there are symbols of Thomas, which are geodesically invariant objects. They are not tensors. However, in the presence of a flat background metric, a tensor object from the symbols of Thomas can be formed [5].

As for metrics, there are two possibilities to compare such theory with observations.

Firstly, we can use solution of the field equations at some selected gauge condition, just as we do it with solutions of the Einstein equations at a selected coordinate conditions.<sup>2</sup> (It is used in [5]).

Secondly, there is an object that is geodesically invariant generalization of the metric tensor  $g_{\alpha\beta}$  if we consider the metric tensor as the 4-components of some 5-dimensional tensor in the spirit of a 5-dimensional interpretation of geodetic maps dating back to Thomas [9] and Veblen [12].

Let  $X^A$  ( $A = 0 \div 4$ ) be homogeneous coordinates of points in the tangent space of the space-time manifold with an arbitrary factor, which is conveniently labeled as  $\exp(x^4)$ . Then, in addition to coordinate transformations

$$\bar{x}^\alpha = \bar{x}^\alpha(x^0, x^1, x^2, x^3) \quad (23)$$

<sup>2</sup> From a fundamental point of view, the problem of observables in general relativity has not been solved.

we must also take into account the change of this factor by transformation of the fifth coordinate

$$\bar{x}^4 = x^4 + \log \rho, \quad (24)$$

where  $\rho$  is an arbitrary function of  $x^\alpha$ . In this auxiliary five-dimensional manifold, we can define the geometric objects, which are transformed through (23) and (24). In particular, a tensor transforms as follows

$$\bar{Q}_{AB} = Q_{CD} \frac{\partial x^C}{\partial \bar{x}^A} \frac{\partial x^D}{\partial \bar{x}^B},$$

where capital letters range from 0 to 4.

The equation

$$G_{AB} X^A X^B = 0$$

defines the quadric for which the equation of light cone  $g_{\alpha\beta} dx^\alpha dx^\beta = 0$  is an asymptotic. Tensor  $G_{AB}$  determines a metric. In this case,  $g_{AB} = G_{AB}/G_{44}$  is a projective tensor, such that  $g_{44} = 1$ . If we define  $f_A = g_{A0}$ , it follows from the transformation law of  $G_{AB}$ , that  $f_A$  is a covariant projective vector which transforms under pure 4-transformation of coordinates as

$$\bar{f}_4 = f_4; \quad \bar{f}_\alpha = f_\beta \frac{\partial x^\beta}{\partial \bar{x}^\alpha},$$

and under pure transformation of 5-coordinate (i.e under projective transformations) as

$$\bar{f}_4 = f_4, \quad \bar{f}_\alpha = f_\alpha - \frac{\partial \log \varsigma}{\partial x^\alpha}.$$

The tensor  $g_{AB}$  is of the form

$$g_{AB} = \begin{pmatrix} 1 & f_\alpha \\ f_\beta & g_{\alpha\beta} \end{pmatrix} \quad (25)$$

where  $g_{\alpha\beta}$  is an affine tensor which can be identified with the metric tensor of space-time. It follows from the transformation law (23) and (24) that the object

$$\bar{g}_{\alpha\beta} = g_{\alpha\beta} - f_\alpha f_\beta \quad (26)$$

is invariant under the transformation of the fifth coordinate, and hence is invariant under the geodesic (projective) maps of space-time.

What is a field of  $f_\alpha(x)$ ? It follows from the transformation properties of the vector  $f_\alpha$  with respect to the transformation of 5-th coordinate that it can be a kind of a gradient invariant physical field similar to the 4-potential of electromagnetic field which was used in the Kaluza-Klein model. However, this vector can also be formed from the components of the metric tensor, since the Christoffel symbols  $\Gamma_\beta = \Gamma_{\alpha\beta}^\alpha$  have the same transformation law under the transformation of 5-th coordinate. This possibility was used in paper [11].

From this point of view Einstein's equation is very similar to some gauge-invariant equations that describe gravity in a fixed gauge.

The simplest projective-invariant equation which do not contradict the available observations (in particular, in cosmology) are proposed in [5].

## References

1. Eisenhart L.P. Riemannian Geometry. – Princeton, N.J.: Princeton University Press, 1926. – 262 p.
2. Petrov A.Z. Einstein Spaces. – Oxford: Pergamon Press, 1969. – 411 p.
3. Mikeš J. Geodesic mappings of affine-connected and Riemannian spaces // Journal of Mathematical Sciences. – 1996. – Vol.78, No.3. – PP. 311-333.
4. Mikeš J., Kiosak V., Vanšurová A. Geodesic mappings of manifolds with affine connection. – Olomouc: Palacký University, 2008. – 220 p.
5. Verozub L. Geodesic-invariant equations of gravitation // Annalen der Physik. – 2008. – Vol.17, Iss.1. – PP. 28-51.
6. Neurowsky P. Is dark energy meaningless? // Rend. Sem. Mat. Univ. Politec. Torino. – 2010. – Vol.68, No.4. – PP. 361-367.
7. Gibbons G.W., Warnick C.M. Dark energy and projective symmetry // Physics Letters B. – 2010. – Vol.688, Iss.4-5. – PP. 337-340.
8. Thomas T.Y. On the Projective and Equi-Projective Geometries of Paths // Proceedings of the National Academy of Sciences of the United States of America. – 1925. – Vol.11, No.4. – PP. 199-203.
9. Veblen O. A generalization of the quadratic differential form // The Quarterly Journal of Mathematics. – 1930. – No.1. – PP. 66-76.
10. Verozub L.V., Kochetov A.Y. Testing of the Metric-Field Equation // Gravitation and Cosmology. – 2000. – Vol.6, No.3. – PP. 246-250.

Л.В. Верозуб

## О ЗНАЧЕНИИ ГЕОДЕЗИЧЕСКИХ ОТОБРАЖЕНИЙ РИМАНОВЫХ ПРОСТРАНСТВ В ТЕОРИИ ТЯГОТЕНИЯ

В статье рассмотрены следствия того факта, что многие метрики пространства-времени, являющиеся решением уравнений тяготения Эйнштейна, являются геодезически (проективно) эквивалентными однопараметрическому множеству других метрик, которые, вообще говоря, не являются решением этих уравнений.

**Ключевые слова:** геодезические отображения, уравнения тяготения Эйнштейна, теория гравитации

Л.В. Верозуб

## ПРО ЗНАЧЕННЯ ГЕОДЕЗИЧНИХ ВІДОБРАЖЕНЬ РИМАНОВИХ ПРОСТОРІВ В ТЕОРІЇ ТЯЖІННЯ

У статті розглянуті наслідки того факту, що велика кількість метрик простору-часу, що є рішеннями рівнянь тяжіння Ейнштейна, є геодезично (проективно) еквівалентними однопараметричній множині інших метрик, які, взагалі кажучи, не є рішенням цих рівнянь.

**Ключові слова:** геодезичні відображення, рівняння тяжіння Ейнштейна, теорія гравітації

## ОПРЕДЕЛЕНИЕ ОПТИМАЛЬНОЙ ПЕРИОДИЧНОСТИ ФОРМ ОБСЛУЖИВАНИЯ В СЛОЖНОЙ СИСТЕМЕ

В.А. Хорошко, Ф.И. Егоров, Е.О. Тискина

Государственный университет информационно-коммуникационных технологий,  
ул. Соломенская, 7, Киев, 03110, Украина; e-mail: professor\_va@ukr.net

Рассматривается восстанавливаемая сложная система с возможными нарушениями. При заданных интенсивностях появления нарушений отказа системы, ее восстановления, продолжительность рабочего периода и времени обслуживания устанавливаются удобные для инженерных расчетов приближенные зависимости коэффициента использования от безразмерных параметров.

**Ключевые слова:** сложная система, отказоустойчивость, цикл функционирования, техническое обслуживание

### Введение

В настоящее время большое значение имеет разработка методик отыскания оптимального режима технического обслуживания (ТО) сложных систем. Обоснование существующих методик содержится в работах [1-3]. Как правило, методики предполагают восстановление отказавшей системы, что отвечает узкому понятию «отказ». Поскольку понятие «отказ» предполагает восстановление отказавших систем, то должны быть найдены оптимальные периодичности и объемы ТО системы с возможными нарушениями в условиях реального понимания отказа.

Устранение накопившихся нарушений производится при проведении различных форм обслуживания. Если при этом устраняются все накопившиеся к началу обслуживания нарушения, то такая форма обслуживания называется полной. Очевидно, что при условии возможности в сложной системе многих нарушений с отличающимися интенсивностями появления полной формы обслуживания может быть невыгодной. Целесообразно увеличить частоту проведения обслуживаний по нарушениям с большими интенсивностями появления. Такая форма, при которой во время обслуживания устраняются нарушения только определенного типа, называются неполной. Если же происходит чередования в определенной последовательности полных и неполных обслуживаний, то такой режим называется смешанным.

### Постановка задачи

Рассмотрим случай проведения полной формы обслуживания. Показателем эффективности организации ТО, как и в [1-3] будем принимать коэффициент технического использования

$$q = T_p / T_k, \quad (1)$$

где  $T_k$  – календарное время;  $T_p$  – среднее время работы системы за календарное время с учетом ее ненадежности и затрат времени на проведение обслуживаний.

## Основная часть

Исходным пунктом общей методики определения оптимальной периодичности ТО восстанавливаемой системы является анализ случая возможности в ней лишь одного нарушения. При этом система может находиться в трех состояниях: исправном, функционирования с нарушением и отказа. Интенсивности появления нарушения, отказа системы с нарушениями и восстановления системы обозначим соответственно  $\lambda$ ,  $\mu$ ,  $\alpha$ . Предположим, что во время обслуживания исправная сложная система не отказывает и отказавшая не восстанавливается.

Если  $P_i(t)$  (где  $i = \overline{1,3}$ ) – вероятность  $i$ -го состояния системы в момент  $t$ , то при работе системы (между техническими обслуживаниями) эти вероятности связаны уравнениями

$$\begin{aligned} P_1'(t) &= -\lambda P_1(t) + \alpha P_3(t), \\ P_2'(t) &= -\mu P_2(t) + \lambda P_1(t), \\ P_3'(t) &= -\alpha P_3(t) + \mu P_2(t). \end{aligned} \quad (2)$$

Считаем, что при  $t = 0$  система исправна, т.е.  $P_1(0) = 1$ ,  $P_2(0) = 0$ ,  $P_3(0) = 0$ .

Цикл функционирования системы состоит из периода работы и периода ТО. С ростом номера цикла закон изменения вероятностей состояний во времени становится более стабильным пока, начиная с некоторого номера, практически полностью стабилизуется – наступает установившийся режим изменений вероятности состояний системы по циклам.

При продолжительном времени работы сложной системы, включающем много циклов с установившимся режимом изменения вероятностей ее состояний, определение коэффициента использования с достаточной точностью может осуществляться не по всему этому времени, а по времени ее функционирования в одном установившемся цикле.

Так как среднее время функционирования в пределах установившегося цикла с продолжительностью рабочего периода  $t_p$  определяется формулой, то

$$t_c = \int_0^{t_p} [P_1^w(r) + P_2^w(r)] dr, \quad (3)$$

где  $P_1^w(r)$ ,  $P_2^w(r)$  – зависимость вероятностей исправного состояния системы и ее состояния с нарушением от времени с нового начала ее отсчета – начала цикла. Поэтому коэффициент использования системы можно записать как

$$q = \frac{\int_0^{t_p} [P_1^w(r) + P_2^w(r)] dr}{t_p + t_n}, \quad (4)$$

где  $t_n$  – средняя продолжительность ТО.

Решив уравнения (2) при начальных условиях  $P_1(0) = A$ ,  $P_2(0) = 0$ ,  $P_3(0) = 1 - A$ , где  $A$  – неопределенная величина, получим

$$\begin{aligned}
 P_1^w(t) &= \frac{\alpha\mu}{\beta_1\beta_2} - \frac{(\mu - \beta_1)(\alpha - A\beta_1)}{\beta_1(\beta_2 - \beta_1)} e^{-\beta_1 t} + \frac{(\mu - \beta_2)(\alpha - A\beta_2)}{\beta_2(\beta_2 - \beta_1)} e^{-\beta_2 t}, \\
 P_2^w(t) &= \frac{\alpha\lambda}{\beta_1\beta_2} - \frac{\lambda(\alpha - A\beta_1)}{\beta_1(\beta_2 - \beta_1)} e^{-\beta_1 t} + \frac{\lambda(\alpha - A\beta_2)}{\beta_2(\beta_2 - \beta_1)} e^{-\beta_2 t},
 \end{aligned}
 \tag{5}$$

где  $\beta_1, \beta_2$  – величины, связанные с интенсивностями  $\lambda, \mu, \alpha$  соотношениями

$$\beta_1 + \beta_2 = \alpha + \lambda + \mu,$$

$$\beta_1\beta_2 = \alpha\lambda + \alpha\mu + \lambda\mu.$$

Подставив в (5)  $t = t_p$ , а результат в соотношение

$$P_1(t_p) + P_2(t_p) = P_1(0) = A,$$

характерное для установившегося режима, найдем

$$A = M(t_p) / N(t_p), \tag{6}$$

где

$$\begin{aligned}
 M(t_p) &= \frac{\lambda(\mu + \lambda)}{\beta_1\beta_2} - \frac{\alpha(\mu + \lambda - \beta_1)}{\beta_1(\beta_2 - \beta_1)} e^{-\beta_1 t_p} + \frac{\alpha(\mu + \lambda - \beta_2)}{\beta_2(\beta_2 - \beta_1)} e^{-\beta_2 t_p}, \\
 N(t_p) &= 1 - \frac{\mu + \lambda - \beta_1}{\beta_2 - \beta_1} e^{-\beta_1 t_p} + \frac{\mu + \lambda - \beta_2}{\beta_2 - \beta_1} e^{-\beta_2 t_p}.
 \end{aligned}$$

Цель организации обслуживания сложной системы – поддержания ее высокой надежности и живучести, поэтому продолжительность рабочего периода, как правило, устанавливается такой, что величины  $\lambda t_p, \mu t_p, \alpha t_p$ , определяющее вероятность отказа системы в течении рабочего периода, малы. Соответственно, вместо точной формулы (6), определяющей начальное условие «установившегося» цикла обслуживания, можем использовать приближенную, предусматривающую разложение функций  $M(t_p), N(t_p)$  в ряд Маклорона относительно аргумента  $t_p$  и учет членов этого разложения до второго порядка малости. Выполнив это, получим

$$A = \left( 1 + \frac{\lambda t_p}{1 - \frac{\alpha t_p}{2}} \right)^{-1}, \tag{7}$$

где

$$\beta = \frac{\mu\lambda}{2\alpha}.$$



Подставив соотношение(5) в равенство (3), произведя интегрирование и разложив результат в ряд Маклорона относительно аргумента  $t_p$  с той же степенью точности, получим

$$\int_0^{t_p} [P_1^w(\tau) + P_2^n(\tau)] d\tau = At_p + (1-A)\frac{t_p^2}{2}.$$

Соответственно, согласно (4) и (7)

$$q = \frac{\mu[1-w(1-\mu)]}{(\mu+v)(1+\mu-w)}, \quad (8)$$

где

$$\mu = \beta t_p; \quad v = \beta t_n; \quad w = \frac{\alpha t_p}{2}.$$

Построив согласно (8) графики зависимости  $q(\mu, v, w)$  при параметрах  $v$  и  $w$ , можно по ним при известных  $\lambda$ ,  $\mu$ ,  $t_p$  и  $t_n$  определять коэффициент технического использования системы.

Формула (8) применима и в общем случае полной формы обслуживания для  $n$  последовательно соединенных элементов, но величина  $\beta$  вычисляется согласно формуле:

$$\beta = \sum_{i=1}^n \mu_i \lambda_i / 2\alpha,$$

где  $\mu_i$  и  $\lambda_i$  – соответственно интенсивности появления нарушения и отказа с нарушением в  $i$ -м элементе;  $t_n = t_{n_1} + \dots + t_{n_n}$ , где  $t_{n_i}$  – среднее время ТО  $i$ -го элемента.

Общая задача определения оптимальной периодичности ТО восстанавливаемой сложной системы с возможными нарушениями предполагает определение оптимального числа форм ТО и объем каждой формы. В настоящей работе решается часть этой задачи: определение периодичности ТО при заданной его структуре. Рассмотрим определение оптимальной периодичности смешанной формы ТО восстанавливаемой системы с возможными нарушениями.

Задача решается в предположении, что систему можно представить как  $n$  последовательно соединенных элементов, каждый из которых может находиться в одном из трех состояний: исправном, функционирования с нарушением и отказа. Естественно, что при этом отказ любого элемента приводит к отказу всей системы в целом.

Как и в случае полной формы ТО, показателем эффективности организации технического обслуживания принимается коэффициент использования  $\eta$ . Интенсивность появления нарушения в  $i$ -м элементе системы обозначим через  $\lambda_i$ , а интенсивность возникновения его отказа при наличии нарушения –  $\mu_i$ , интенсивность восстановления отказавшей системы –  $\alpha$ .

Пусть полная форма обслуживания осуществляется через время  $t_p$ , а величина  $r_i$  показывает, сколько раз проводится обслуживание  $i$ -го элемента за период  $t_p$ .

Для каждого элемента системы справедливого приближенное выражение функции живучести  $F_i(t)$ , учитывающее члены расположения до третьего порядка малости

$$F_i(t) = \left[ A_i 1 + \frac{1 - A_i}{A_i} \left( 1 - \frac{t}{t_p} \right) \alpha t \right],$$

где

$$A_i \left( 1 + \frac{\beta_i t_p}{t - \frac{\alpha t_p}{2r_i}} \right)^{-1}, \quad (9)$$

$$\beta_i = \frac{\mu_i \lambda_i}{2\alpha r_i}. \quad (10)$$

Тогда функция живучести последовательного соединения элементов –

$$F(t) = \prod_{i=1}^n F_i(t),$$

или с учетом членов до третьего порядка малости –

$$F(t) = \left[ 1 + \frac{1 - A}{A} - \left( \frac{t}{t_p} \right) \alpha t \right], \quad (11)$$

где

$$A = \prod_{i=1}^n A_i \approx 1 + \frac{\beta t_p}{\left( 1 - \frac{\alpha t_p}{2} \sum_{i=1}^n \frac{1}{r_i} \right)^{-1}}, \quad (12)$$

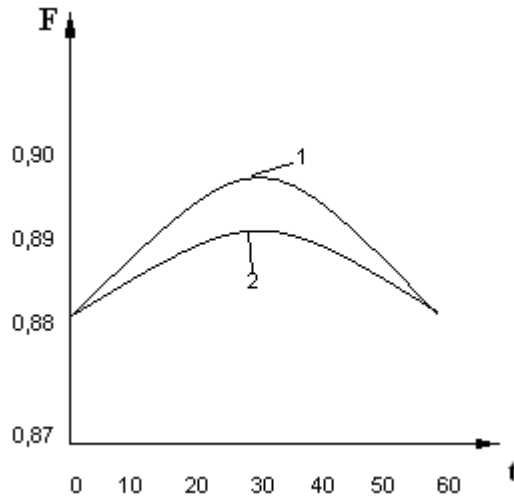
$$\beta = \sum_{i=1}^n \beta_i.$$

Подставив (9) и (12) в (11), получим приближенное выражение функции живучести всего соединения

$$F(t) = A + \alpha(1 - A)t_p - \alpha(1 - A)\frac{t^2}{t_p}. \quad (13)$$

### Анализ результатов

Как видно (рис. 1), отличие кривой, соответствующей точному выражению функции живучести, от кривой, построенной по приближенной формуле (13), незначительно, поэтому сделанное приближение существенной ошибки не дает.



**Рис. 1.** Зависимость функции живучести  $F$  от времени  $t$ : 1 - точное выражение функции живучести; 2 - с использованием формулы (13)

При установившемся режиме работы системы

$$T_p = \int_0^{t_p} F(t) dt; \quad T_k = t_p + t_n.$$

Тогда исходя из (1),

$$q = \frac{\int_0^{t_p} F(t) dt}{t_p + t_n}. \quad (14)$$

Соответственно, используя (13) и (14), получим

$$\eta = \frac{\mu \left[ 1 - w \left( \sum_{i=1}^n \frac{1}{r_i} - \frac{u}{j} \right) \right]}{\left( 1 + u - w \sum_{i=1}^n \frac{1}{r_i} \right) (u + v)}, \quad (15)$$

где

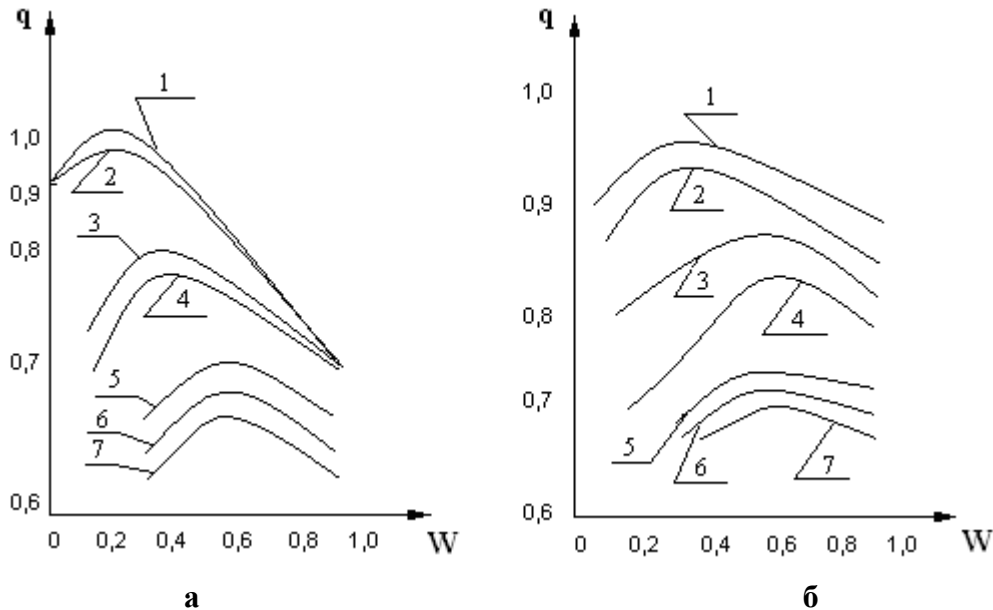
$$u = \beta t_p; \quad v = \beta t_n; \quad w = \frac{\alpha t_p}{2}. \quad (16)$$

Определить оптимальную продолжительность рабочего периода по графикам вида  $\eta = \eta(u, v, w)$ , при заданных величинах  $\alpha$ ,  $\mu$ ,  $\lambda$ ,  $t_n$  неудобно, так как от  $t_p$  зависят два безразмерных параметра  $u$  и  $w$ . Поэтому при решении такой задачи необходимо

использовать не один график  $\eta(u, v, w)$ , а их систему. Рациональнее, введя новый безразмерный параметр

$$W_1 = u/w = 2\beta/\alpha,$$

не зависящий от  $t_p$ , построить графики зависимостей  $\eta = \eta(u, v, w)$  для различных  $v, w_1$ , не связанных с продолжительностью рабочего периода  $t_p$ . Соответственно определение оптимальной периодичности рабочего периода «установившегося» цикла обслуживания сводится к отысканию максимального из таких графиков.



**Рис. 2.** Зависимость коэффициента  $q$  использования системы от параметра  $w$ :

а –  $w_1 = 0.2$ , б –  $w_1 = 0.3$ ;  $\lambda/10^{-3}$ ; 1 – 0.05, 2 – 0.1, 3 – 0.3, 4 – 0.5, 5 – 1.0, 6 – 1.5, 7 – 2.0

При проведении эксперимента по точному и приближенному значению коэффициента использования находилась ошибка вычислений. Точное значение коэффициента использования вычислялось на ЭВМ, а приближенное – по формуле (15). Погрешность расчетов в диапазонах  $0.2 \leq w_1 \leq 0.5$ ;  $0 \leq u \leq 0.1$ ;  $0.0005 \leq v \leq 0.015$  не превышает 5%, что явно говорит в пользу предлагаемой оценки.

### Список литературы

1. Капустян М.В. Оценка эффективности функционирования сложных систем / М.В. Капустян, В.А. Хорошко // Інформаційна безпека. – 2011. – №1 (5). – С. 5-8.
2. Одияненко Е.В. Оценка эффективности тестовой диагностики в запрещенных сетях связи / Е.В. Одияненко, Н.В. Пискун, В.А. Хорошко // Системи обробки інформації. – 2011. – Вип. 3 (93). – С. 134-137.
3. Капустян М.В. Математическая модель контроля качества функционирования систем защиты информации / М.В. Капустян, В.А. Хорошко // Захист інформації. – 2011. – №2. – С. 51-56.

В.О. Хорошко, Ф.І. Єгоров, О.О. Тіскіна

## ВИЗНАЧЕННЯ ОПТИМАЛЬНОЇ ПЕРІОДИЧНОСТІ ФОРМ ОБСЛУГОВУВАННЯ В СКЛАДНІЙ СИСТЕМІ

Розглядається відновлювана складна система з можливими порушеннями. При заданих інтенсивностях появи порушень відмови системи, її відновлення, тривалість робочого періоду і часу обслуговування встановлюються зручні для інженерних розрахунків наближені залежності коефіцієнта використання від безрозмірних параметрів.

**Ключові слова:** складна система, відмовостійкість, цикл функціонування, технічне обслуговування

V. Khoroshko, F. Egorov, O. Tiskina

## DETERMINATION OF THE OPTIMAL FREQUENCY OF SERVICE FORM IN COMPLEX SYSTEMS

We consider the complex system being restored with possible violations. At a given intensity of rejection of recovery from a system failure, working time and service time are set convenient for engineering calculations of the approximate dependence of the use of dimensionless parameters.

**Keywords:** complex systems, fault-tolerance, cycle of functioning, technical service

# НЕЙРОСЕТЕВОЙ ПОДХОД К ОБНАРУЖЕНИЮ СЕТЕВЫХ АТАК НА КОМПЬЮТЕРНЫЕ СИСТЕМЫ

М.П. Комар<sup>1</sup>, И.О. Палий<sup>1</sup>, Р.П. Шевчук<sup>1</sup>, Т.Б. Федысив<sup>2</sup>

<sup>1</sup> Тернопольский национальный экономический университет,  
ул. Львовская, 11, Тернополь, 46020, Украина; e-mail: mko@tneu.edu.ua

<sup>2</sup> Государственное высшее учебное заведение «Дрогобычский механико-технологический колледж»,  
ул. Раневицкая, 12, 82100, Дрогобыч, Украина; e-mail: f\_taras2006@ukr.net

В работе произведен выбор нейронной сети для обнаружения сетевых атак. Предложен способ формирования обучающей выборки для обучения нейросетевого детектора. Представлено применение метода главных компонент для сокращения размера данных для анализа сетевого трафика. Представлены результаты экспериментальных исследований.

**Ключевые слова:** нейронная сеть, сетевая атака, нейросетевой детектор, метод главных компонент, сетевой трафик

## Введение

Произведенный анализ методов и средств защиты компьютерных систем от сетевых атак показывает, что нейросетевые методы продолжают стремительно развиваться, причем основная тенденция – применение комбинаций нейронных сетей с другими методами.

Благодаря своим особенностям, таким как высокая степень параллелизма обработки информации, способность к обобщению, адаптация к изменениям окружающей среды, распознавание зашумленных образов, низкий уровень ресурсоемкости и т.д., нейронные сети позволяют достичь хороших результатов в решении таких сложных инженерных задач как распознавание образов, классификация, прогнозирование, системы контроля и т.д. В связи со способностью искусственных нейронных сетей в процессе обучения выявлять сложные зависимости между входными и выходными данными, которые отсутствовали в обучающей выборке, и, способностью корректно классифицировать зашумленные образы, они являются привлекательным инструментом для решения сложных разнообразных задач защиты компьютерной информации.

Все это послужило базой для выбора искусственных нейронных сетей в качестве основного инструмента обнаружения компьютерных атак.

В работе исследуются разнообразные архитектуры нейронных сетей с целью выбора нейронной сети для обнаружения сетевых атак, предложен способ формирования обучающей выборки для обучения нейросетевого детектора, представлено применение метода главных компонент для сокращения размера данных для анализа сетевого трафика и представлены результаты экспериментальных исследований.

## Выбор архитектуры нейронной сети для обнаружения компьютерных атак

Существует большое количество нейронных сетей, применяемых для решения тех или иных сложных инженерных задач. Так многослойные персептроны (*multilayer*

*perceptron* – MLP) [1] характеризується прямим розповсюдженням входного сигналу від шару до шару і складається з множини входних нейронних елементів, одного або декількох прихованих шарів нейронних елементів, і вихідного шару. Одним з головних переваг таких мереж є можливість вирішувати алгоритмічно нерозв'язні задачі або задачі, для яких алгоритмічне рішення невідоме, але для яких можливо скласти репрезентативний набір прикладів з відомими рішеннями. MLP при навчанні, за рахунок свого внутрішнього будови, виявляє закономірності в зв'язі входних і вихідних образів і тим самим узагальнює отриманий на навчальній вибірці досвід.

Рекуррентні нейронні мережі [1] мають зворотні зв'язки між шарами нейронів, тобто виходи нейронних елементів наступних шарів пов'язані з нейронами попередніх шарів. Таким чином, відбувається врахування результатів перетворення нейронною мережею інформації на попередньому етапі для обробки входного вектора на наступному етапі функціонування мережі. Рекуррентні мережі можуть використовуватися для вирішення задач прогнозування і управління.

Рециркуляційні нейронні мережі (*recirculation neural networks* – RNN) [1] призначені для стиснення (пряме перетворення) і відновлення (зворотне перетворення) вихідної інформації і характеризуються як прямим так і зворотним перетворенням інформації.

Нейронні мережі з радіально-базисною функцією активації (*radial basis function networks* – RBF) [1] застосовуються для вирішення задач прогнозування, апроксимації функцій, розпізнавання образів і т.д.

Нейронні мережі Кохонена дозволяють в результаті навчання здійснювати топологічно неперервне відображення  $F$ -входного  $n$ -вимірного простору в вихідне  $m$ -вимірне простору. Структура такої нейронної мережі представляє собою мережу з прямим розповсюдженням сигналу. В якості методу навчання використовується конкурентне навчання. По мірі надходження входних образів на таку мережу за допомогою навчання відбувається розбиття  $n$ -вимірного входного простору на різні області рішень, кожній з яких відповідає окремий нейрон.

Нейронні мережі для векторного квантування (LVQ) використовуються для стиснення даних і ґрунтовані на ідеї порівняння входного вектора з еталоном. В процесі надходження еталонних векторів на мережу вона навчається так, що утворюються кластери різних еталонів, кожному з яких відповідає свій нейрон. При надходженні на вхід такої нейронної мережі невідомого образу, він ідентифікується в відповідності з мірою близькості до еталонних векторів і кодується на виході мережі номером нейрона.

До системи виявлення вторгнень пред'являється ряд жорстких вимог, одним з яких є функціонування в режимі реального часу. В результаті, необхідно мінімізувати часові витрати, пов'язані з навчанням нейронної мережі. В результаті, необхідно вибрати таку архітектуру, яка б характеризувалася мінімальним часом навчання, а, відповідно, і мінімальним розміром навчальної вибірки. Розглянемо характеристики MLP [1, 2]. Многослойні перцептрони навчаються при використанні алгоритму зворотного розповсюдження помилки (*back-propagation algorithm*) [1, 2] і успішно застосовуються для вирішення багатьох складних задач класифікації, розпізнавання і др. В [2] сказано, що на здатність нейронної мережі до правильного узагальнення впливають розмір навчальної вибірки і архітектура нейронної мережі. В нашому випадку кількість входних нейронів повинно дорівнювати кількості атрибутів мережевого трафіка, тобто  $n = 41$ . Кількість прихованих нейронів згідно з проведеними експериментами повинно дорівнювати  $m = 10$ . Кількість вихідних нейронів дорівнює  $k = 2$ , тобто кожен з вихідних нейронів відображає той або інший клас входного образу.

Для правильного навчання нейронної мережі достатньо, щоб розмір навчальної

выборки  $L$  удовлетворял следующему соотношению [2]:

$$L = O(W / \varepsilon), \quad (1)$$

где  $W$  – общее количество настраиваемых параметров (весовых коэффициентов и пороговых значений);  $\varepsilon$  – допустимая точность ошибки классификации;  $O(\dots)$  – порядок величины, т.е., например, для ошибки в 5% количество примеров обучения должно в 5 раз превосходить количество свободных параметров сети  $W$ .

Общее количество настраиваемых параметров вычисляется согласно следующему выражению:

$$W = m(n + 3) + 2. \quad (2)$$

В результате, в случае применения MLP в качестве детектора для обнаружения сетевых атак обучающая выборка для обучения нейронной сети с допустимой ошибкой классификации  $\varepsilon = 0.1$  должна состоять, согласно выражениям (1) и (2) из 4420 образцов.

Проведем аналогичный анализ для RBF сетей [1, 2]. Сети на основе радиальных базисных функций также являются многослойными нейронными сетями. Первый слой таких сетей является входным слоем и обеспечивает связь сети с внешней средой. Второй слой – скрытый слой, выполняет нелинейное преобразование входное пространство образов в скрытое пространство, зачастую имеющее существенно более высокую размерность, чем входное. Третий слой – выходной, он состоит из линейных нейронов. В [2] сказано, что формулы (1) и (2) в общем случае применимы и для сетей RBF, т.е. для корректного обучения детектора на основе RBF сети нам также необходимо, чтобы размер обучающей выборки был равным 4420 образцов. Более того, известно, что чем выше число скрытых нейронов сети RBF тем выше качество классификации в определенных задачах. Так, например, в [2] показано, что при увеличении количества центров с 20 до 100, качество классификации увеличивается примерно на 4.5%. Таким образом, для повышения качества распознавания сетевых атак на основе RBF сети необходима обучающая выборка большего размера.

Теперь рассмотрим сеть встречного распространения [1, 2] с идентичным количеством нейронов в каждом из слоев. В скрытом слое такой сети будем использовать нейронные элементы Кохонена [1-3]. Для обучения такой сети достаточно, чтобы размер обучающей выборки был равным согласно следующему выражению [2]:

$$L \geq 2m. \quad (3)$$

Таким образом, для обучения сети встречного распространения с нейронами Кохонена в скрытом слое необходимо иметь обучающую выборку с размерностью равной минимум 82 образам. В результате, основываясь на выдвинутых ранее требованиях к системе обнаружения вторжений, выберем данную нейронную сеть в качестве основы нейросетевого детектора.

### Формирование обучающей выборки

Структура нейросетевого детектора для обнаружения сетевых атак и метод обучения многослойной нейронной сети с входным слоем, одним скрытым слоем, состоящим из нейронов Кохонена [1, 3], и выходным слоем представлены в [4-6].

В качестве входных данных для нейросетевых детекторов использовались данные, взятые из базы данных KDD Cup1999 Data [7].

Для обучения предложенного нейросетевого детектора используется обучающая



выборка, состоящая из 80% соединений одного из типов атак и 20% нормального соединения, т.е. соотношение атак к нормальным соединениям равняется четыре к одному.

Такое соотношение было получено экспериментальным путем и показало наилучшие результаты классификации сетевого трафика (результаты экспериментов представлены в таблице 1).

**Таблица 1.**

Результаты обнаружения DoS-атак

| Тип атаки | 5/1   | 4/1   | 3/1   | 2/1   | 1/1   |
|-----------|-------|-------|-------|-------|-------|
| DoS       | 95.7% | 98.0% | 97.5% | 96.4% | 96.0% |
| Probe     | 59.2% | 65.1% | 63.9% | 62.1% | 61.5% |
| R2L       | 32.4% | 36.9% | 34.8% | 33.9% | 33.0% |
| U2R       | 16.8% | 20.8% | 19.0% | 18.7% | 17.1% |

Было проведено 5 экспериментов. В каждом эксперименте генерировались 20 нейросетевых детекторов. В первом эксперименте для обучения нейронной сети использовалась такая обучающая выборка, в которой соотношение нормальных сетевых соединений к атакам составляло пять к одному. Во втором эксперименте соотношение классов сетевых соединений равнялось четыре к одному, в третьем – три к одному, в четвертом – два к одному. В последнем эксперименте обучающая выборка состояла из 50% нормального трафика и 50% сетевых атак. Сгенерированные детекторы обучались и классифицировали неизвестные образы. Результаты классификации представлены в таблице 1. Как видно из таблицы 1, наилучший результат показали те детекторы, для обучения которых использовалась выборка, состоящая из 80% сетевых атак и 20% нормальных сетевых соединений.

Исходя из того, что классы сетевого трафика распределены в обучающей выборке в соотношении 80% сетевых атак и 20% нормальных соединений, то это налагает определенные требования на распределение нейронов Кохонена в скрытом слое нейросетевого детектора. Для корректного функционирования выбранной нейронной сети необходимо, чтобы соотношение между количеством нейронов в слое Кохонена, характеризующие различные классы, должно быть кратным соотношению четыре к одному.

Таким образом, соотношение нейронов в скрытом слое должно быть равным

$$f/1 = 4/1, \quad (4)$$

где  $f$  – первые нейроны слоя Кохонена, активность которых характеризует сетевую атаку; 1 – последние нейроны слоя Кохонена, активность которых характеризует нормальное сетевое соединение.

В результате, если количество нейронов Кохонена в скрытом слое равняется десяти, то количество нейронов, отвечающих за сетевую атаку, будет равным  $f = 8$ , а количество нейронов, отвечающих за нормальное соединение, будет равным  $1 = 2$ .

### Применение метода главных компонент

Для сокращения размера данных при обучении и анализе сетевого трафика предлагается использовать метод главных компонент [8].

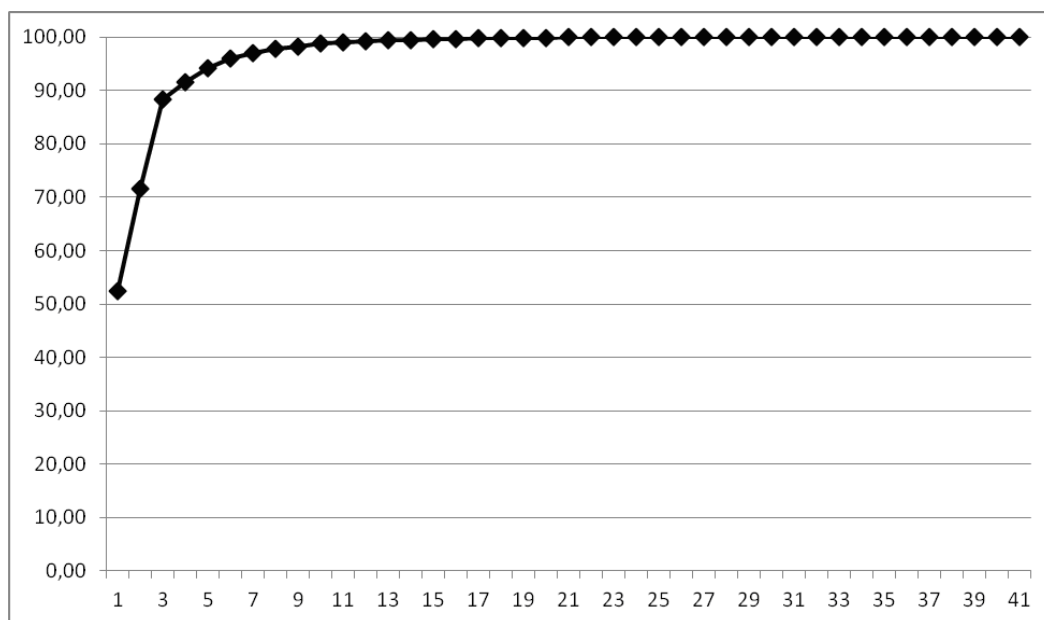
В общем виде метод главных компонент можно представить в виде следующей формулы:

$$X = TP^T + E, \quad (5)$$

где  $X$  – матрица данных, каждая строка которой является вектором преобработанных данных. Матрицу данных можно представить в следующем виде:  $X = \{x_1, \dots, x_m\}^T$ , где  $m$  – число векторов данных,  $n$  – размерность пространства данных;  $P$  – матрица нагрузок, в которой каждый столбец отображает вектор главных компонент. Матрицу нагрузок можно представить в следующем виде:  $P = \{a_1, \dots, a_k\}$ , где  $k$  – количество векторов главных компонент, выбранных для проецирования;  $T$  – матрица счетов, в которой каждая строка представляет собой проекцию вектора данных на  $k$  главных компонент. Матрицу счетов можно представить в виде  $T = [t_{ij}]$ , где  $t_{ij} = (x_i, a_j)$ ;  $E$  – матрица ошибок, вычисляемая по формуле  $E = X - TP^T$ .

Анализируя распределение количества информации, содержащейся в каждой последующей главной компоненте, можно определить число компонент, которые целесообразно использовать для дальнейшего анализа.

На рис. 1 представлена зависимость количества информации от числа главных компонент.

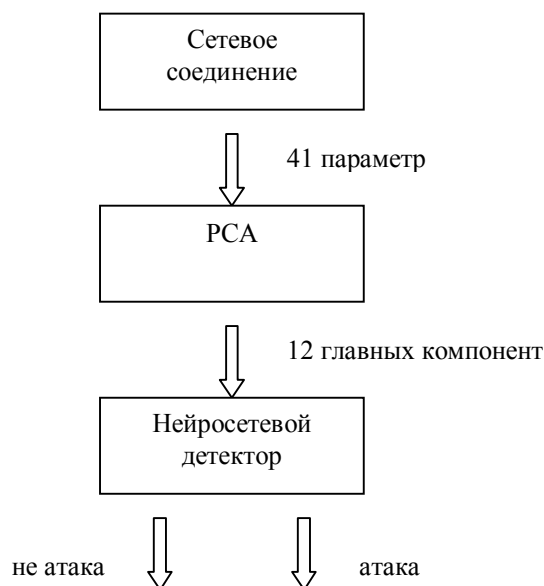


**Рис. 1.** Зависимость количества информации от числа главных компонент

Как видно из рис. 1 первых главных компонент содержат 99% информации о сетевом трафике. В остальных 30 компонентах содержится только 1% информации, и из соображения целесообразности их можно исключить из анализа.

Использование метода главных компонент выявило тот факт, что для успешного анализа сетевого трафика достаточно использовать 12 первых главных компонент, в которых содержится 99% информации о сетевом соединении, а не 41 параметр. Это позволит существенно ускорить как процесс обучения нейросетевого детектора, так и процесс анализа сетевого трафика. Для этого, к выделенным из сетевого трафика применяем сначала метод главных компонент, а затем, подаем полученные данные на вход нейронной сети.

Схематически данный процесс изображен на рис. 2.



**Рис. 2.** Взаимодействие связки PCA и нейросетевой детектор

При таком подходе, количество  $n$  входных нейронов используемой нейронной сети в качестве детектора равняется 12. Подаваемая информация – двенадцать первых главных компонент, подаются на скрытый слой детектора, где и происходит его определение к классу сетевой атаки или к классу легитимного соединения.

Сравнительный анализ результатов обнаружения сетевых атак с применением метода главных компонент и без PCA представлены в таблицах 2–5.

**Таблица 2.**  
Сравнительный анализ результатов обнаружения DoS-атак

|           | Back,<br>% | Land,<br>% | Neptune,<br>% | Pod,<br>% | Smurf,<br>% | Teardrop,<br>% | Среднее по<br>атакам, % |
|-----------|------------|------------|---------------|-----------|-------------|----------------|-------------------------|
| PCA       | 99.5       | 100.0      | 100.0         | 98.1      | 100.0       | 100.0          | 99.6                    |
| без PCA   | 99.5       | 90.5       | 100.0         | 98.1      | 100.0       | 100.0          | 98.0                    |
| Улучшение | 0          | 9.5        | 0.0           | 0.0       | 0.0         | 0.0            | 1.6                     |

**Таблица 3.**  
Сравнительный анализ результатов обнаружения Probe-атак

|           | Ipsweep, % | Nmap, % | Portswweep, % | Satan, % | Среднее по атакам, % |
|-----------|------------|---------|---------------|----------|----------------------|
| PCA       | 65.2       | 100.0   | 99.9          | 99.3     | 91.1                 |
| без PCA   | 7.1        | 54.5    | 99.6          | 99.3     | 65.1                 |
| Улучшение | 58.1       | 45.5    | 0.3           | 0.0      | 26.0                 |

Таблица 4.

Сравнительный анализ результатов обнаружения R2L-атак

|           | Ftp_write, % | Guess_passwd, % | Imap, % | Multihop, % | Phf, % | Spy, % | Warezclient, % | Warezmaster, % | Среднее по атакам, % |
|-----------|--------------|-----------------|---------|-------------|--------|--------|----------------|----------------|----------------------|
| PCA       | 100.0        | 94.3            | 83.3    | 57.1        | 100.0  | 100.0  | 65.0           | 90.0           | 86.2                 |
| без PCA   | 25.0         | 0.0             | 50.0    | 28.6        | 100.0  | 0.0    | 32.0           | 80.0           | 36.9                 |
| Улучшение | 75.0         | 94.3            | 33.3    | 28.5        | 0.0    | 100.0  | 33.0           | 10.0           | 49.3                 |

Таблица 5.

Сравнительный анализ результатов обнаружения U2R-атак

|           | Buffer_overflow, % | Loadmodule, % | Perl, % | Rootkit, % | Среднее по атакам, % |
|-----------|--------------------|---------------|---------|------------|----------------------|
| PCA       | 83.3               | 100.0         | 33.3    | 30.0       | 61.7                 |
| без PCA   | 63.3               | 0.0           | 0.0     | 20.0       | 20.8                 |
| Улучшение | 20.0               | 100.0         | 33.3    | 10.0       | 40.9                 |

Как видно из полученных результатов, качество обнаружения удалось значительно увеличить благодаря применению метода главных компонент к параметрам сетевого трафика. Так прирост в качестве обнаружения в среднем для DoS-атак составил 1.6 %, для Probe-атак составил 26.0%, для R2L-атак составил 49.3%, для U2R-атак составил 40.9%.

Следует отметить, что процент возникновения ложного обнаружения составляет менее 1.7%.

Также, за счет того, что для анализа сетевого трафика теперь используются не все 41 параметр, а 12 главных компонент, удалось значительно повысить быстродействие системы в целом, что является важным критерием для систем защиты информации.

## Заключение

В данной работе в качестве нейросетевого детектора для обнаружения сетевых атак выбрана многослойная нейронная сеть с входным слоем, одним скрытым слоем, состоящим из нейронов Кохонена, и выходным слоем. Для обучения нейросетевого детектора используется обучающая выборка, состоящая из 80% соединений, относящихся к сетевым атакам, и 20% соединений, относящихся к нормальным соединениям.

Также, представлено применение метода главных компонент для сокращения размера данных для анализа сетевого трафика с целью выявления компьютерных атак. Применение PCA позволило повысить качество обнаружения сетевых атак на компьютерные системы, а также повысить быстродействие системы за счет сокращения анализируемых данных. Однако, некоторые типы атак, такие как ipsweep, multihop, warezclient, perl и rootkit, недостаточно хорошо обнаруживаются. Для преодоления этого недостатка предлагается применить метод искусственных иммунных систем.

## Список литературы

1. Головкин В.А. Нейронные сети: обучение, организация, применение / В.А. Головкин // Нейрокомпьютеры и их применение: учеб. пособие / В.А. Головкин. – М.: Радиоэлектроника, 2001 – 256 с.

2. Хайкин С. Нейронные сети: полный курс [Текст] : пер. с англ. / под ред. д.т.н. Н.Н. Куссуль. – 2-е изд., испр. – М. : ООО «И. Д. Вильямс», 2006. – 1104 с.
3. Kohonen T. Self-organized formation of topologically correct feature maps / T. Kohonen // *Biological Cybernetics*. – 1982. – Vol.43, No.1. – PP. 59-69.
4. Комар М.П. Система анализа сетевого трафика для обнаружения компьютерных атак / М.П. Комар // *Вестник Брестского государственного технического университета: (Серия: физика, математика и информатика)*. – 2010. – №5. – С. 14-16.
5. Комар М. Методы искусственных нейронных сетей для обнаружения сетевых вторжений / М. Комар // *Сборник тезисов седьмой международной научно-технической конференции «Интернет – Образование – Наука» (ИОН-2010)* – Винница: Винницкий национальный технический университет, 2010. – С. 410-413.
6. Комар М.П. Интеллектуализированная информационная технология обнаружения компьютерных атак / М.П. Комар, Д.И. Боднар, А.А. Саченко // *Измерительная и вычислительная техника в технологических процессах*. – 2010. – № 2. – С. 133-137.
7. KDD Cup 1999 Data [Электронный ресурс]. – Режим доступа: <http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html>.
8. Jolliffe I.T. *Principal Component Analysis* / I.T. Jolliffe. – New York: Springer, 2010. – 516 p.

М.П. Комар, І.О. Палій, Р.П. Шевчук, Т.Б. Федисів  
 НЕЙРОМЕРЕЖЕВИЙ ПІДХІД ДО ВИЯВЛЕННЯ МЕРЕЖЕВИХ АТАК НА  
 КОМП'ЮТЕРНІ СИСТЕМИ

Зроблено вибір нейронної мережі для виявлення мережеских атак. Запропоновано спосіб формування навчальної вибірки для навчання нейромережевого детектора. Представлено застосування методу головних компонент для скорочення розміру даних для аналізу мережевого трафіку. Представлені результати експериментальних досліджень.

**Ключові слова:** нейронна мережа, комп'ютерна атака, нейромережевий детектор, метод головних компонент, мережевий трафік

M. Komar, I. Paliy, R. Shevchuk, T. Fedysiv  
 NEURAL NETWORK APPROACH FOR DETECTION OF NETWORK ATTACKS ON  
 COMPUTER SYSTEMS

We made the choice of a neural network to detect network attacks. The method that forms the training set for neural network detector training. Is proposed the use of principal component analysis to reduce the size of data for analyzation of network traffic is presented. The results of experimental studies are presented.

**Keywords:** neural network, network attack, neural network detector, method of principal components analysis, network traffic

## К ВОПРОСУ О РАНЖИРОВАНИИ КРИТЕРИЕВ ОПАСНОСТИ ГАЛОГЕНОУГЛЕВОДОРОДОВ

О.И. Бодюл, И.В. Дубро, Е.С. Бодюл, А.В. Шаталов

Одесская государственная академия холода,  
ул. Дворянская, 1/3, Одесса, 65026, Украина; e-mail: olga\_bodyul@ukr.net

Рассматриваются различные модели определения весовых коэффициентов критериев опасности на основе экспертизы. Предлагается метод оценки экологической опасности галогеноуглеводородов в различных информационных ситуациях, базирующийся на использовании аддитивных функций. Приведены результаты определения экологической опасности галогеноуглеводородов.

**Ключевые слова:** галогеноуглеводороды, экологическая опасность, информационная ситуация, функция неопределенности

### Введение

Выбор экологически безопасного галогеноуглеводородного хладагента представляет собой задачу принятия решения в условиях противоречивых целей при отсутствии строгой упорядоченности по принятым критериям выбора [1, 2]. Хорошие возможности учета при принятии решения ранга экологических целей (как глобального, так и локального уровня), а также изменяющихся приоритетов позволяет применение аддитивных функций и априорно-апостериорных процедур [2-4]. Преимущества использования аддитивных функций связаны с возможностью привлечения результатов экспертизы. Информационная ситуация при оценке экологической опасности хладагентов может быть представлена следующим образом: имеется  $n$  сравниваемых между собой альтернативных веществ ( $R_j$ ) экологические последствия применения которых могут быть оценены по совокупности критериев опасности. Однако точная количественная оценка последствий в большинстве случаев затруднительна. Ниже рассматривается интерпретация общих методологических принципов оценки экологических ситуаций согласно [5-7], применительно к задаче анализа предпочтений на основе экспертизы при выборе экологически безопасных хладагентов.

### Основная часть

Последствия принятия решения о выборе галогеноуглеводородного хладагента по совокупности критериев опасности определяются на основе мнений групп опрошенных экспертов (последующее обращение оценок экспертов в критерий риска включает операцию определения вероятности, как меры субъективных мнений [7]). Чем ниже значения рангов  $\zeta_{ij}$ , тем выше ущерб при использовании хладагента с позиции учета  $i$ -го критерия опасности

Предпочтительность  $\xi_j$   $j$ -го хладагента с точки зрения экологических последствий заранее неизвестна. Осуществить ранжирование экологических целей можно с использованием критерия Байеса [6, 7]

$$W_i = \sum_{j=1}^m \varsigma_{ij} \xi_j. \quad (1)$$

Весовые коэффициенты критериев экологической опасности могут быть определены, как

$$\lambda_i = W_i^{-1} / \sum_{i=1}^n W_i^{-1}, \quad (2)$$

а значение функции экологической опасности галогенуглеводорода, согласно [2, 4] по соотношению:

$$U(R) = \sum_{i=1}^n \lambda_i u_i^*(R_i), \quad (3)$$

где  $u_i^*(R)$  – нормированное значение  $i$ -го критерия экологической опасности.

Упорядочение последствий ранговых последовательностей экспертных оценок  $\varsigma_{ij}$  решения о выборе хладагента целесообразно осуществлять с учетом их максимального и минимального значений по соотношению:

$$\Delta_j = \max \varsigma_{ij} - \min \varsigma_{ij}; \quad 1 \leq \Delta_j \leq m. \quad (4)$$

Соотношения для определения коэффициентов  $\xi_j$  могут быть получены, согласно рекомендациям, приведенным в работах [6, 7], из условий максимизации функции неопределенности второго рода или энтропии Шеннона с использованием метода множителей Лагранжа:

$$H_2(\xi) = \prod_{j=1}^f \xi_j^{(m-j+1)k_j} \rightarrow \max_{\xi_j}; \quad (5)$$

$$\sum_{j=1}^f k_j \xi_j = 1,$$

где  $f = m - \sum_{j=1}^m (k_j - 1)$ .

$$L = \prod_{j=1}^f \xi_j^{(m-j+1)k_j} + l \left( 1 - \sum_{j=1}^f k_j \xi_j \right), \quad (6)$$

$$\frac{\partial L}{\partial \xi_j} = (m-j+1)k_j \xi_j^{(m-j+1)k_j-1} \prod_{\substack{g=1 \\ g \neq j}}^f \xi_g^{(m-g+1)k_g} - lk_j = 0, \quad (7)$$

$$l \sum_{j=1}^f k_j \xi_j = H_2(\xi) \sum_{j=1}^f k_j (m-j+1), \quad (8)$$

или

$$l = H_2(\xi) \sum_{j=1}^f k_j (m - j + 1), \quad (9)$$

откуда

$$\xi_j = (m - j + 1) / \left( \sum_{j=1}^f k_j (m - j + 1) \right). \quad (10)$$

Соотношение (10) представляет собой обобщение оценок Фишборна [9] на случай кратности ранговых последовательностей  $\varsigma_{ij}$ .

$$H = - \sum_{j=1}^m \xi_j \ln \xi_j \rightarrow \max_{\xi_j}, \quad (11)$$

где  $H$  – энтропия Шеннона.

Задача (11) решается при выполнении условий нормировки  $\sum_{j=1}^m \xi_j = 1$  и постоянства среднегеометрического значения  $\Delta_i: \prod_{j=1}^m \Delta_j^{\xi_j} = \text{const}$ .

Используя метод множителей Лагранжа

$$L = - \sum_{j=1}^m \xi_j \ln \xi_j + l_1 \left( \sum_{j=1}^m \xi_j - 1 \right) + l_2 \left( \sum_{j=1}^m \xi_j \ln \Delta_j - c \right), \quad (12)$$

$$\frac{\partial L}{\partial \xi_j} = - \ln \xi_j - 1 + l_1 + l_2 \ln \Delta_j = 0, \quad (13)$$

можно получить соотношения для весовых коэффициентов  $\xi_j$  в виде потенциальных распределений

$$\xi_j = \Delta_j / \sum_{j=1}^m \Delta_j. \quad (14)$$

Нами была выполнена оценка экологической опасности галогеноуглеводородных холодильных агентов в различных информационных ситуациях на основе соотношений (1) – (14) с использованием результатов анкетирования, которое проводилась среди специалистов Одесской государственной академии холода и Производственно-коммерческой фирмы «Инжмаш Сервис» (Украина), а также IG Samson Enterprises (Vernon, Connecticut, USA).

## Результаты исследования

Фрагмент результатов анкетирования – ранговые последовательности экспертных оценок последствий замены R13, R13B1 и R503 на современные хладагенты в холодильном оборудовании, предназначенном для промышленного охлаждения и замораживания, приведены в табл. 1.



Таблиця 1.

Оценка ситуаций при выборе заменителей R13, R13B1 и R503 в холодильном оборудовании, предназначенном для промышленного охлаждения и замораживания

|                   | CFC 13<br>CClF3 | Halon 13B1<br>CBrF3 | CHF 23<br>CHF3 | R503<br>CHF3/CClF3<br>40,1%/59,9% | R508A<br>CHF3/CF3CF3<br>39%/61% | R403B<br>C3H8/CHClF2<br>/C3F8<br>5/75/20 | R170 (C2H6) | R744 (CO2) |
|-------------------|-----------------|---------------------|----------------|-----------------------------------|---------------------------------|------------------------------------------|-------------|------------|
| q, кДж/кг         | 4               | 6                   | 5              | 4                                 | 4                               | 4                                        | 4           | 4          |
| $l_{ad}$ , кДж/кг | 4               | 4                   | 3              | 4                                 | 4                               | 4                                        | 4           | 4          |
| $\varepsilon_o$   | 4               | 4                   | 4              | 5                                 | 4                               | 4                                        | 4           | 4          |
| ODP               | 1               | 1                   | 1              | 3                                 | 1                               | 4                                        | 4           | 4          |
| GWP               | 2               | 2                   | 2              | 2                                 | 2                               | 2                                        | 2           | 2          |
| TEWI              | 4               | 4                   | 4              | 4                                 | 4                               | 4                                        | 4           | 4          |
| $T_{at}$ лет      | 7               | 7                   | 7              | 8                                 | 9                               | 9                                        | 9           | 9          |
| LFL, %            | 3               | 3                   | 3              | 3                                 | 3                               | 3                                        | 3           | 3          |
| НОС, МДж/кг       | 3               | 3                   | 3              | 3                                 | 3                               | 3                                        | 3           | 3          |
| Flam              | 9               | 9                   | 9              | 9                                 | 9                               | 9                                        | 3           | 9          |
| ПДК               | 6               | 6                   | 6              | 6                                 | 6                               | 8                                        | 8           | 8          |
| TDC               | 4               | 4                   | 4              | 4                                 | 4                               | 4                                        | 4           | 8          |
| LC 50             | 8               | 8                   | 8              | 9                                 | 9                               | 9                                        | 6           | 10         |
| TLV-TWA           | 4               | 4                   | 4              | 4                                 | 4                               | 4                                        | 4           | 4          |
| STEL              | 8               | 8                   | 8              | 9                                 | 9                               | 9                                        | 6           | 10         |
| WEEL              | 8               | 8                   | 8              | 9                                 | 9                               | 9                                        | 6           | 10         |
| IDLH              | 8               | 8                   | 8              | 9                                 | 9                               | 9                                        | 6           | 10         |
| LOEL              | 8               | 8                   | 8              | 9                                 | 9                               | 9                                        | 6           | 10         |
| EC 50             | 8               | 8                   | 8              | 9                                 | 9                               | 9                                        | 6           | 10         |
| RD 50             | 8               | 8                   | 8              | 9                                 | 9                               | 9                                        | 6           | 10         |
| Std 34            | 5               | 5                   | 5              | 5                                 | 5                               | 5                                        | 5           | 5          |

где *ODP* – потенциал истощения озона (Ozone Depletion Potential); *GWP<sub>100</sub>* – потенциал глобального потепления за 100 лет (Global Warming Potential); *TEWI* – полный эквивалент глобального потепления (Total Equivalent Warming Impact); *T<sub>at</sub>* – атмосферное время жизни (Atmospheric Lifetime), лет; *LFL* – предел воспламеняемости в воздухе (Lower flammability limit); *НОС* – теплота сгорания (Heat of combustion); *Flam* – горючесть хладагента (Flammability); *ПДК* – предельно допустимая концентрация, мг/м<sup>3</sup>; *TDC* – коэффициент токсической опасности (Toxic Danger Coefficient); *LC<sub>50</sub>* – средняя смертельная доза для 50% тестируемых животных (Lethal Concentration) ppm; *TLV-TWA* – допустимое пороговое значение (Threshold Limit Value-Time Weighted Average), ppm; *STEL* – предельное кратковременное воздействие (Short-Term Exposure Limit), ppm; *WEEL* – допустимое содержание паров в рабочем помещении (Workplace Environmental Exposure), восьмичасовой день/средний вес; *IDLH* – непосредственная опасность для жизни и здоровья (Immediately Dangerous to Life and Health), ppm; *LOEL* – индекс снижения сердечной сенсibilизации (Lowest-Observed Effect Level), ppm; *EC50* – индекс наркотическое воздействие (Anesthetic Effective Concentration), ppm; *RD50* – индекс снижение частоты дыхания (Concentration Decrease of Respiratory Rate), ppm; *Std 34* – класс безопасности, с учетом токсичности и пожароопасности (Safety Classification – Std 34).

Согласно данным табл. 1:

$$\Delta_5 = \Delta_8 > \Delta_1 = \Delta_2 = \Delta_3 = \Delta_4 = \Delta_6 > \Delta_7, \quad (15)$$

а упорядочение ранговых последовательностей, отражающее систему предпочтений экспертов, имеет вид:

$$\xi_5 = \xi_8 \succ \xi_1 = \xi_2 = \xi_3 = \xi_4 = \xi_6 \succ \xi_7. \quad (16)$$

Сравнение результатов расчета мер неопределенности (табл. 2), отвечающих общим требованиям [9], показывает, что во всех случаях мера неопределенности, соответствующая модели (14) оказывается меньше мер, соответствующих модели (10). Следовательно, модель (14) добавляет меньше субъективной информации к имеющейся и в данном случае является более предпочтительной.

**Таблица 2.**

Энтропия Шеннона и другие меры неопределенности для законов распределений (10) и (14) при выборе заменителей R13, R13B1 и R503 в холодильном оборудовании для промышленного охлаждения и замораживания.

| Мера неопределенности                           | Модель (7)              | Модель (8)              |
|-------------------------------------------------|-------------------------|-------------------------|
| $H = -\sum_{j=1}^m \xi_j \ln \xi_j$             | 2.0748                  | 2.06832                 |
| $H_2(\xi) = \prod_{j=1}^f \xi_j^{(m-j+1)k_j}$   | $0.13400 \cdot 10^{-7}$ | $0.29222 \cdot 10^{-8}$ |
| $H_3 = 1 - \max \xi_j$                          | 0.86                    | 0.8432                  |
| $H_4 = \min \xi_j$                              | 0.105                   | 0.0784                  |
| $H_5 = \prod_{j=1}^m \xi_j^2$                   | $0.3297 \cdot 10^{-13}$ | $0.87 \cdot 10^{-14}$   |
| $H_6 = 1 - \sum_{j=1}^m \xi_j^2$                | 0.94224                 | 0.85057;                |
| $H_7 = \prod_{j=1}^m \xi_j^m$                   | $1.47 \cdot 10^{-8}$    | $1.43 \cdot 10^{-9}$    |
| $H_8 = \sum_{j=1}^m \xi_j (1 - e^{-(1-\xi_j)})$ | 0.58226                 | 0.56259                 |

Результаты определения величин  $\Delta_j$  и  $\xi_j$  при выборе заменителей R13, R13B1 и R503 в холодильном оборудовании для промышленного охлаждения и замораживания приведены в табл. 3.

Таблиця 3.

Значения весовых коэффициентов  $\xi_j$  ранговых последовательностей экспертных оценок важности критериев  $u_i(r)$  выбора хладагента при замене R13, R13B1 и R503 в холодильном оборудовании для промышленного охлаждения и замораживания

| № | Вещество                              | $\Delta_j$ | $\xi_j$     | $\xi_j$     |
|---|---------------------------------------|------------|-------------|-------------|
|   |                                       |            | Модель (10) | Модель (14) |
| 1 | CFC 13                                | 7          | 0.1228      | 0.1372      |
| 2 | Halon 13B1                            | 7          | 0.1228      | 0.1372      |
| 3 | CHF 23                                | 7          | 0.1228      | 0.1372      |
| 4 | R503                                  | 7          | 0.1228      | 0.1372      |
| 5 | R508A                                 | 8          | 0.14        | 0.1568      |
| 6 | R403B                                 | 7          | 0.1228      | 0.1372      |
| 7 | R170 (C <sub>2</sub> H <sub>6</sub> ) | 4          | 0.105       | 0.0784      |
| 8 | R744 (CO <sub>2</sub> )               | 8          | 0.14        | 0.1568      |

Определение весовых коэффициентов  $\xi_j$  ранговых последовательностей позволяет выполнить последующий расчет критерия  $W_i$ , осуществить ранжирование экологических целей и определить весовые коэффициенты  $\lambda_i$  соответствующих критериев  $u_i(R)$  экологической опасности галогеноуглеводородов.

В таблице 4 приведены результаты определения критерия Байеса и весовых коэффициентов  $\lambda_i$  функций опасности  $U(R)$  согласно данным таблицы 1. Сопоставление полученных нами результатов расчета по приведенным выше моделям в различных расчетных случаях выбора хладагента свидетельствует о незначительном отличии значений «весов»  $\lambda_i$  критериев  $u_i(r)$ . Таким образом, полученные результаты можно считать статистически устойчивыми.

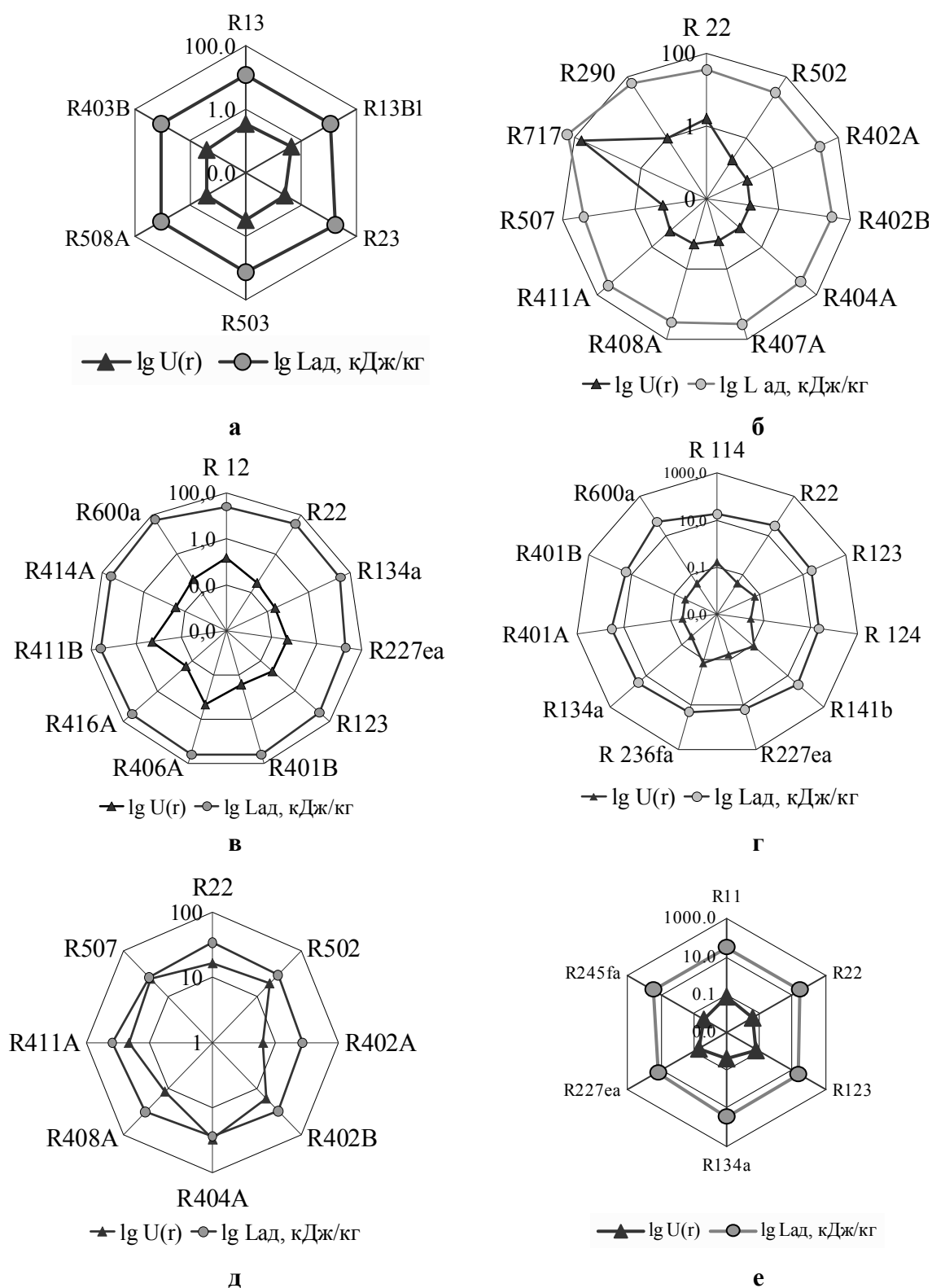
Согласно данным табл. 4, наиболее существенными для принятия решения являются критерии, имеющие высокие значения весовых коэффициентов  $\lambda_i$ . Согласно полученным результатам такими критериями являются  $l_{ad}$ , ODP, GWP,  $T_{at}$ , LFL, TDC. Как показано в [2, 4] величина  $l_{ad}$  является мерой негативного воздействия, причиняемого косвенными выбросами в атмосферу токсичных, озonoактивных и парниковых газов, сопровождающего производство энергии, потребляемой холодильным оборудованием. Экологическая опасность эмиссии в атмосферу этих веществ оценивается на основе критериев ODP, GWP,  $T_{at}$ , TDC, LFL. Величина GWP определяется с учетом атмосферного времени жизни вещества  $T_{at}$ . Таким образом, согласно результатам экспертизы, оценка экологической опасности и выбор хладагентов могут быть осуществлены на основе следующих независимых показателей ODP, GWP, TDC, LFL.

Таблица 4.

Весовые коэффициенты  $\lambda_i$  критериев  $u_i(r)$  при выборе заменителей R13, R13B1 и R503 в холодильном оборудовании для промышленного охлаждения и замораживания

| $u_i(r)$ | Критерий Байеса | Весовой коэффициент | Критерий Байеса | Весовой коэффициент |
|----------|-----------------|---------------------|-----------------|---------------------|
|          | Модель (13)     |                     | Модель (17)     |                     |
|          | $W_i$           | $\lambda_i$         | $W_i$           | $\lambda_i$         |
| $q_v$    | 4.36            | 0.0612              | 4.7236          | 0.0536              |
| $l_{ад}$ | 3.86            | 0.0691              | 4.1748          | 0.0606              |
| ODP      | 2.344           | 0.1144              | 2.4696          | 0.1025              |
| GWP      | 1.998           | 0.1337              | 2.156           | 0.1174              |
| $T_{at}$ | 8.1314          | 0.0328              | 8.7416          | 0.0289              |
| LFL      | 2.997           | 0.0891              | 3.234           | 0.0782              |
| HOC      | 2.997           | 0.0891              | 3.234           | 0.0782              |
| Flam     | 8.151           | 0.0327              | 8.7612          | 0.0288              |
| ПДК      | 6.7296          | 0.0397              | 7.2128          | 0.0350              |
| TDC      | 4.416           | 0.0605              | 4.6256          | 0.0547              |
| LC50     | 8.3076          | 0.0322              | 7.1736          | 0.0353              |
| TLV-TWA  | 3.996           | 0.0667              | 0.1394          | 0.0723              |
| STEL     | 8.3076          | 0.0322              | 7.3304          | 0.0345              |
| WEEL     | 8.3076          | 0.0322              | 7.3304          | 0.0345              |
| IDLH     | 8.3076          | 0.0322              | 7.3304          | 0.0345              |
| LOEL     | 8.3076          | 0.0322              | 7.3304          | 0.0345              |
| EC50     | 8.3076          | 0.0322              | 7.3304          | 0.0345              |
| RD50     | 8.3076          | 0.0322              | 7.3304          | 0.0345              |
| Std 34   | 3.767           | 0.0709              | 5.39            | 0.0469              |

В табл. 5 приведены результаты определения критерия Байеса и весовых коэффициентов  $\lambda_i$  критериев  $u_i(r)$  для выбора хладагента на основе четырех наиболее важных критериев в различных информационных ситуациях. Результаты определения экологической опасности галогеноуглеводородов в рассмотренных в табл. 5 ситуациях выбора приведены на рис. 1. Представление результатов в координатах « $U(r) - l_{ao}$ » позволяет принимать решение на основе как экологических, так и термодинамических показателей хладагента. Поскольку величина  $l_{ao}$  является мерой косвенного (в части производства потребляемой энергии) экологического ущерба, то выбор хладагента осуществляется при более широком охвате факторов опасности. Согласно выполненным расчетам, предпочтительными согласно обобщенным экологическим показателям с учетом мнений экспертов в рассмотренных информационных ситуациях являются следующие хладагенты: R23, R403B (ситуация 1, рис. 1, а); R22, R407A (ситуация 2, рис. 1, б); R134a, R401B, R414A, R416A (ситуация 3, рис. 1, в), R124, R134a, R401A/B (ситуация 4, рис. 1, г); R402A/B, R22, (ситуация 5 рис. 1, д), R245fa, R134a (ситуация 6, рис. 1, е). Окончательный выбор может быть осуществлен исходя из требуемых эксплуатационных и физико-химических показателей хладагента в зависимости от конкретных условий работы охлаждающей системы и ее назначения [1].



**Рис. 1.** Результаты оценки опасности холодильных агентов в различных информационных ситуациях

Таблица 5.

Весовые коэффициенты  $\lambda_i$  критериев  $u_i(r)$ 

| $u_i(r)$ | Критерий Байеса                                                                                             | Весовой коэффициент | Критерий Байеса                                                                              | Весовой коэффициент |
|----------|-------------------------------------------------------------------------------------------------------------|---------------------|----------------------------------------------------------------------------------------------|---------------------|
|          | $W_i$                                                                                                       | $\lambda_i$         | $W_i$                                                                                        | $\lambda_i$         |
|          | Решение о замене R13, R13B1 и R503 в холодильном оборудовании для промышленного охлаждения и замораживания. |                     | Решение о замене R502 в холодильном оборудовании для охлаждения торговых складов             |                     |
| ODP      | 2.4696                                                                                                      | 0.2904              | 5.3337                                                                                       | 0.2165              |
| GWP      | 2.1560                                                                                                      | 0.3326              | 4.5773                                                                                       | 0.2523              |
| LFL      | 3.2340                                                                                                      | 0.2217              | 3.6798                                                                                       | 0.3139              |
| TDC      | 4.6256                                                                                                      | 0.1551              | 5.3168                                                                                       | 0.2171              |
| $u_i(r)$ | Решение о замене R12 в бытовых и транспортных холодильниках и кондиционерах                                 |                     | Решение о замене R114 и R12B1 в оборудовании для производственного кондиционирования воздуха |                     |
| ODP      | 4.6914                                                                                                      | 0.2049              | 1.8352                                                                                       | 0.2183              |
| GWP      | 5.1378                                                                                                      | 0.1853              | 1.8352                                                                                       | 0.2183              |
| LFL      | 2.8058                                                                                                      | 0.3395              | 1.7998                                                                                       | 0.2235              |
| TDC      | 3.5003                                                                                                      | 0.2720              | 1.1881                                                                                       | 0.3370              |
| $u_i(r)$ | Решение о замене R502 в бытовых холодильниках и морозильниках.                                              |                     | Решение о замене R11 в холодильном оборудовании для охлаждения воды.                         |                     |
| ODP      | 3.45472                                                                                                     | 0.2317              | 2.5296                                                                                       | 0.1782              |
| GWP      | 3.5239                                                                                                      | 0.2272              | 2.5296                                                                                       | 0.1782              |
| LFL      | 2.2912                                                                                                      | 0.3494              | 1.5708                                                                                       | 0.2799              |
| TDC      | 4.1774                                                                                                      | 0.1916              | 1.2648                                                                                       | 0.3564              |

## Выводы

1. На основании математической обработки результатов экспертизы наиболее существенными независимыми показателями для экологической оценки хладагентов являются ODP, GWP, TDC, LFL.

2. Сопоставление результатов расчета по различным моделям в каждом из рассмотренных расчетных случаев выбора хладагента свидетельствует о незначительном отличии значений «весов»  $\lambda_i$  критериев  $u_i(r)$ . Таким образом, полученные результаты можно считать статистически устойчивыми.

3. Согласно результатам оценки экологической опасности современных галогеноуглеводородных хладагентов в рассмотренных информационных ситуациях предпочтительными являются R22, R23, R124, R134a, R245fa, R401A/B, R402A/B, R403B, R407A, R414A, R416A.

## Список литературы

1. Mazur V. Optimum refrigerant selection for low temperature engineering // Low Temperature and Cryogenic Refrigeration / V. Mazur. – Kluwer Academic Publishers, 2003. – PP. 101-118.
2. Bodyul O.I., Dubro I.V. An Ecological Approach to a Problem of Risk Evaluation of Halocarbons // Proc. of 21<sup>st</sup> International Congress of Refrigeration – Serving the Needs of Mankind, August 17-22, 2003. – Washington D.C., USA. – CD-ROM ISBN 2913149324 – 8 p.
3. Suter G.W. Uncertainty in environmental risk assessment // Acting under Uncertainty: Multidisciplinary Conceptions / G.W. Suter. – Kluwer Academic Publishers, 1990. – PP. 203-230.
4. Bodyul O.I., Dubro I.V., Vinogradova Ye.I., An ecological risk assessment of the halocarbons // Proc. of 11<sup>th</sup> international symposium “Loss prevention and safety promotion in the process industries – Loss prevention 2004”, May 31 - June 3, Praha (Czech Republic). – CD-ROM ISBN 80-02-01574-6. – 8 p.
5. Morgan M.G., Henrion M. and Morris S.C. Expert Judgments for Policy Analysis, report of an invitational workshop held at Brookhaven National Laboratory, July 8-11 1979. Brookhaven National Laboratory, BNL 51358, 1980.

6. Ивченко Б.П. Информационная экология : монография / Б.П. Ивченко, Л.А. Мартыщенко. – СПб: Нордмед-Издат, 1998 – .  
Ч. 1 : Оценка риска техногенных аварий и катастроф. Статистическая интерпретация экологического мониторинга. Моделирование и прогнозирование экологических ситуаций. – 1998. – 201 с. – ISBN 5-86581-023-6
7. Хеттманспенгер Т. Статистические выводы, основанные на рангах / Т. Хеттманспенгер ; пер. с англ. Д.С. Шмерлинга ; [редкол.: А.Г. Аганбегян и др.]. – М.: Финансы и статистика, 1987. – 334 с.
8. Фишберн П. Теория полезности для принятия решений / П. Фишберн. – М.: Наука, 1978. – 352 с.
9. Боровков А.А. Курс теории вероятности. – М.: Наука, 1972. – 288 с.

О.І. Бодюл, І.В. Дубро, О.С. Бодюл, О.В. Шаталов  
ДО ПИТАННЯ ЩОДО РАНЖУВАННЯ КРИТЕРІЇВ НЕБЕЗПЕКИ  
ГАЛОГЕНВУГЛЕВОДНІВ

Розглядаються різні моделі визначення вагових коефіцієнтів критеріїв небезпеки на основі експертизи. Пропонується метод оцінки екологічної небезпеки галогенвуглеводнів в різних інформаційних ситуаціях, що базується на використанні адитивних функцій. Приведені результати визначення екологічної небезпеки галогенвуглеводнів.

**Ключові слова:** галогенвуглеводні, екологічна небезпека, інформаційна ситуація, функція невизначеності

O. Bodyul, I. Dubro, E. Bodyul, A. Shatalov  
HAZARD RANKING SYSTEM CRITERIA FOR HALOCARBONS

The method of ecological danger evaluations of halocarbons is offered. This method use additive functions and definition of danger criteria weight factors on the basis of expert's opinions. Results of ecological danger definition of halocarbons are presented.

**Keywords:** halocarbons, ecological danger, information situation, function of uncertainty

# КОМБИНИРОВАННЫЙ АЛГОРИТМ ПОВЫШЕНИЯ ВЕРОЯТНОСТИ РАСПОЗНАВАНИЯ ДВУМЕРНЫХ ИЗОБРАЖЕНИЙ

В.С. Ситников, Д.М. Шатохин

Одесский национальный политехнический университет,  
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: sitnvs@mail.ru

Предложен комбинированный алгоритм распознавания, объединяющий линейные и нелинейные признаки. Для получения признаков и первоначального понижения размерности пространства используется линейный и нелинейный метод главных компонент. Признаки объединяются в комплексное число, и далее производится распознавание по алгоритму Fisherfaces. Рассмотрено влияние коэффициентов нелинейного метода, а также метрик для определения принадлежности к определенному классу.

**Ключевые слова:** статистический метод, метод главных компонент, линейный дискриминантный анализ, комбинированный метод, «ядерные» методы

## Введение

При создании современного автомобиля на одно из первых мест выходят вопросы безопасности. Существующие электронные системы позволяют оптимизировать работу агрегатов и облегчить водителю вождение автомобилем, однако, при разработке новых систем, большое внимание уделяют системам, которые бы, анализируя ситуацию в автомобиле и вокруг него, выступали в роли советчика при принятии решения водителем [1].

При движении в сложных погодных условиях такие системы могли бы предупреждать водителя о состоянии дороги, о движении впереди идущей машины, о дорожных знаках, установленных на дороге и т.п. Повышение производительности вычислительной техники позволяет активно использовать системы технического зрения для распознавания двумерных образов. Например, системы распознавания дорожных знаков (СРДЗ) могут предупредить водителя во время движения о действующих ограничениях или иных ситуациях за счет считывания дорожных знаков [2].

В области обработки изображений сложился общепринятый подход к обработке двумерных изображений в виде последовательности алгоритмов [3]:

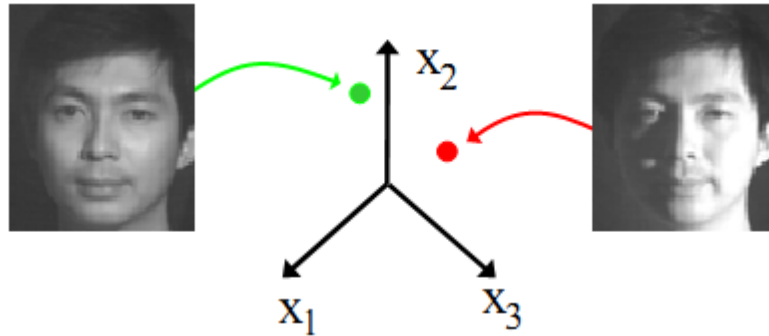
- алгоритм локализации знака на видеоизображении;
- алгоритм определения формы и цвета, позволяющий произвести первичную классификацию изображения;
- алгоритм распознавания изображений;
- алгоритм формирования решений.

Одним из наиболее сложных алгоритмов является алгоритм распознавания изображения. Широко используемыми методами для решения подобных задач (в частности распознавание лиц) являются статистические методы. Семейство статистических методов предполагает наличие обучающей выборки, по которой строятся все возможные варианты и предположения о распознаваемых объектах. Для удобства описания обработки вводится понятие многомерного пространства за счет разворачивания изо-



бражения в вектор  $\vec{T} = n \times m$ , где  $n$  и  $m$  ширина и высота изображения. Тогда, каждое изображение  $x$  есть точка в многомерном пространстве  $R$  размерностью  $N$ ,  $x \in R^N$  (рис. 1).

В каждом методе имеются свои правила выбора базиса для проектирования, но общим является то, что они позволяют уменьшить размерность базиса, оставив только наиболее значимые компоненты. Поэтому для каждого изображения выбирается вектор характерных признаков в выбранном базисе.



**Рис.1.** Понятие многомерного пространства

При распознавании широкое распространение получили линейные и нелинейные методы. Используя их или их сочетание, можно повысить степень распознавания изображений. К линейным методам следует отнести алгоритмы *Eigenfaces* (на основе метода главных компонент – PCA) и *Fisherfaces* (на основе линейного дискриминантного анализа – LDA) [4]. Применяя к этим алгоритмам нелинейные ядра, получим ядерный метод главных компонент (Kernel PCA или KPCA) и ядерный дискриминант Фишера (KFD или KLDA). На их основе созданы алгоритмы *Kernel Eigenfaces* и *Kernel Fisherfaces* [5, 6].

Рассмотрим задачу повышения распознавания изображений на основе линейных и нелинейных статистических методов.

### Метод главных компонент

Пусть  $M$  набор образцов  $x_1, x_2, \dots, x_M$  в  $R^n$ , тогда общая ковариационная матрица набора будет определяться как

$$C = \frac{1}{M} \sum_{j=1}^M (x_j - \bar{x})(x_j - \bar{x})^T, \quad (1)$$

где  $\bar{x}$  – вектор средних значений по всем образцам.

Ортонормированный вектор собственных значений  $w_1, w_2, \dots, w_m$  матрицы  $C$ , соответствующий  $m$  наибольшим собственным значениям, позволяет выбрать их как оси проекции. В общем случае он может быть вычислен непосредственно. Однако, при распознавании образов размерность образца (вектора изображения) всегда велика (например, для изображения 50x50 это 2500 пикселей) и его вычисление занимает много времени. Для сокращения времени вычислений собственных векторов воспользуемся сингулярным разложением.

Пусть  $Q = [x_1 - \bar{x}, \dots, x_M - \bar{x}]$ , тогда ковариационная матрица представится в виде

$$C = \frac{1}{M} Q Q^T,$$

а матрица  $R = Q^T Q$  будет размером  $M \times M$ . Так как число образцов много меньше числа пикселей в изображении образца, то размерность матрицы  $R$  много меньше размерности матрицы  $C$ , поэтому вычислить ее собственный вектор будет проще. В соответствии с сингулярным разложением можно записать [7]

$$w_j = \frac{1}{\sqrt{\lambda_j}} Q u_j, j = 1, \dots, m, \quad (2)$$

где  $u_1, u_2, \dots, u_m$  собственные вектора в порядке соответствия  $m$  наибольшим собственным значениям  $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_m$  матрицы  $R$ .

Тогда для проекции образца на вычисленный нами базис собственных векторов  $w_j$  получим

$$y_j = w_j^T x = \frac{1}{\sqrt{\lambda_j}} Q^T u_j^T x, j = 1, \dots, m. \quad (3)$$

Вычисленные признаки каждого изображения  $y_1, y_2, \dots, y_m$  формируют вектор-столбец линейных (РСА) признаков  $Y = (y_1, y_2, \dots, y_m)^T$  для образца  $x$ .

### Ядерный метод главных компонент

Если нелинейное преобразование  $\Phi$  (ядро) проецирует пространство входных данных  $R^n$  в пространство признаков  $\mathfrak{Z}$

$$\begin{aligned} \Phi : R^n &\rightarrow \mathfrak{Z} \\ x &\rightarrow \Phi(x) \end{aligned}, \quad (4)$$

то идея ядерного преобразования (КРСА) позволяет выполнить алгоритм РСА в пространстве признаков  $\mathfrak{Z}$ , в которое данные проецируются по нелинейному закону  $\Phi$ .

Таким образом, в пространстве  $\mathfrak{Z}$  матрица ковариации будет выглядеть как

$$C = \frac{1}{M} \sum_{j=1}^M (\Phi(x_j) - \bar{\Phi})(\Phi(x_j) - \bar{\Phi})^T, \quad (5)$$

где  $\bar{\Phi} = \frac{1}{M} \sum_{j=1}^M \Phi(x_j)$ .

Однако, центрировать данные в пространстве признаков  $\mathfrak{Z}$  из-за большого объема вычислений сложно. Поэтому рассмотрим не центрированную матрицу ковариации

$$\tilde{C} = \frac{1}{M} \sum_{j=1}^M \Phi(x_j) \Phi(x_j)^T, \quad (6)$$

В алгоритме КРСА вводится понятие ядра, что позволяет избежать сложных вычислений скалярного произведения [3]

$$k(x, y) = (\Phi(x_i) \cdot \Phi(x_j)). \quad (7)$$

Тогда, если  $Q = [\Phi(x_1), \dots, \Phi(x_M)]$ , то выражение (6) можно представить в виде

$$\tilde{C} = \frac{1}{M} Q Q^T.$$

Сформируем матрицу  $\tilde{R} = Q^T Q$ , используя выражение (7)

$$\tilde{R} = \Phi(x_j)^T \cdot \Phi(x_j) = (\Phi(x_i) \cdot \Phi(x_j)) = k(x_i, y_j). \quad (8)$$

Вычисляя собственные значения  $u_1, u_2, \dots, u_m$  собственных векторов в порядке соответствия  $m$  наибольшим собственным значениям  $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_m$  матрицы  $\tilde{R}$  можно показать, что собственные вектора матрицы  $\tilde{C}$  на основе сингулярного разложениям будут иметь вид

$$w_j = \frac{1}{\sqrt{\lambda_j}} Q u_j, j = 1, \dots, m, \quad (9)$$

где  $w_1, w_2, \dots, w_m$  – собственные вектора  $\tilde{C}$ .

Для вычисления собственных значений и вектора матрицы ковариации  $C$  (5), на основе матрицы  $\tilde{R}$ , необходимо ее центрировать и произвести расчет в соответствии с (9). Для центрирования воспользуемся выражением

$$R = \tilde{R} - 1_M \tilde{R} - \tilde{R} 1_M + 1_M \tilde{R} 1_M, \quad (10)$$

где  $1_M$  – матрица, состоящая из единиц.

Тогда для проекции образа на вычисленный базис собственных векторов  $w_j$  запишем

$$y_j = w_j^T \Phi(x) = \frac{1}{\sqrt{\lambda_j}} Q^T u_j^T \Phi(x) = \frac{1}{\sqrt{\lambda_j}} u_j^T [k(x_1, x), k(x_2, x), \dots, k(x_M, x)], \quad (11)$$

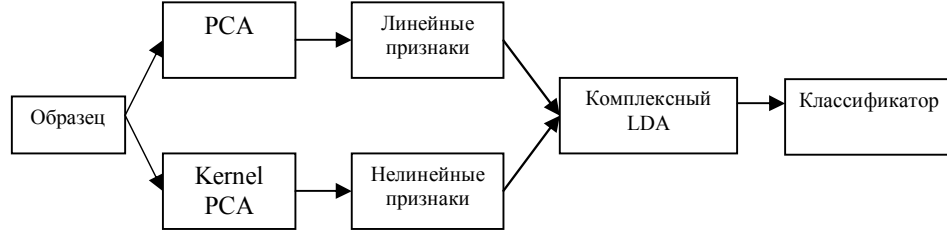
$$j = 1, \dots, m$$

Вычисленные признаки каждого изображения  $y_1, y_2, \dots, y_m$  формируют вектор–столбец нелинейных признаков  $Y = (y_1, y_2, \dots, y_m)^T$  для образа  $x$ .

### Комплексный LDA

В результате проведенных преобразований получено два пространства признаков – линейное (РСА) и нелинейное (КРСА), обозначим их соответственно как  $A$  и  $B$ . Пусть наши образцы принадлежат пространству  $\Omega$ . Получив их разложения на линейном наборе признаков  $\alpha \in A$  и нелинейном наборе признаков  $\beta \in B$ , объединим их в

некоторый комплексный вектор  $\gamma = \alpha + i\beta \in C$ . Вектора  $\alpha$  и  $\beta$  должны быть одинаковой размерности, либо должны быть приведены к этому, рисунок 2.



**Рис.2.** Комбинированный алгоритм

Таким образом, в новом пространстве между классовая, внутри классовая и общая матрицы разброса будут иметь следующий вид

$$S_b = \sum_{i=1}^c N_i (m_i - m_0)(m_i - m_0)^H, \quad (12)$$

$$S_w = \sum_{i=1}^c \{ \sum (X - m_0)(X - m_0)^H | w_i \}, \quad (13)$$

$$S_t = S_b + S_w = \sum (X - m_0)(X - m_0)^H, \quad (14)$$

где  $N_i$  – число образцов класса  $i$ ,  $m_i$  – среднее значение по классу  $i$ ,  $m_0$  – среднее значение по всей выборке.

Из выражений (12)-(14) следует, что все три матрицы  $S_b, S_w$  и  $S_t$  являются положительно определёнными эрмитовыми матрицами. Кроме того, матрицы  $S_w$  и  $S_t$  являются положительно определёнными в случае если  $S_w$  несингулярна. Пусть матрица  $S_w$  несингулярна.

Функцию дискриминантного критерия Фишера объявим как:

$$J(\varphi) = \frac{\varphi^H S_b \varphi}{\varphi^H S_w \varphi}, \quad (15)$$

где  $\varphi$  –  $n$ -размерный ненулевой вектор.

Для положительно определённой матрицы  $S_w$  и полуположительно определённой матрицы  $S_b$ , для любого  $\varphi$ , имеем  $\varphi^H S_b \varphi \geq 0$  и  $\varphi^H S_w \varphi > 0$ . Это означает что значения дискриминантного критерия  $J(\varphi)$  являются неотрицательными действительными числами. В физическом понимании это означает, что критерий Фишера в комплексном пространстве аналогичен критерию в евклидовом пространстве.

Вектор  $\varphi^*$ , соответствующий максимальному значению критерия  $J(\varphi)$ , называют оптимальным направлением проекции. При проекции образцов в  $\varphi^*$  отношение между классового и внутри классового рассеивания будет максимальным. Вектор  $\varphi^*$  можно выбрать как обобщенный вектор собственных значений выражения  $S_b X = \lambda S_w X$ , соответствующий максимальным обобщенным собственным значениям.

Как показано в [4] оптимальное число осей  $\mathbf{P} = (\varphi_1, \varphi_2, \dots, \varphi_d)$  выбирается из соотношения  $d \leq c - 1$ , где  $c$  – число классов. Далее базис  $\mathbf{P}$  используется для проецирования в комплексное пространство признаков. Для вычисления признаков по комплексному алгоритму LDA используется формула

$$Z = P^H Y, \quad (16)$$

где  $Y$  – проекция исходного образца в комплексное пространство,  $Z$  – вектор признаков по методу LDA.

### Постановка эксперимента и анализ результатов

Для проверки работоспособности комбинированного алгоритма распознавания проведено тестирование, для которой создана база изображений знаков ограничения скорости от 5, 10, 20 и далее до 120 км/ч, всего 13 классов знаков. Обучающую выборку для каждого класса составляют 10 изображений, которые сделаны фронтально, под углом слева и справа, сверху и снизу и в их комбинациях. Кроме того одно изображение с ухудшенным освещением, рисунок 3. Каждое изображение обрезано по размеру знака и приведено к разрешению  $50 \times 50$  пикселей. Над каждым изображением проведено автоматическое контрастирование. Аналогичные преобразования выполнены для тестовых изображений, которые были сняты с произвольных позиций.



Рис. 3. Обучающая выборка для одного класса

Каждое изображение сохранено в формате JPEG и ему присвоено название в соответствии с маской <класс>-<номер>.jpg (например, 80-2541.jpg), что в дальнейшем позволило провести проверку правильности, путем сравнения классов.

При тестировании комбинированный метод сравнивался с методом *Eigenfaces*, *Fisherfaces*, *Kernel Eigenfaces*. На первом этапе тестирования использовалось 100 главных компонент (для *Eigenfaces* и *Kernel Eigenfaces*), в комбинированном методе и методе *Fisherfaces* количество компонент ограничено числом классов и равно  $d = c - 1 = 12$ . Для метода *Kernel Eigenfaces* использовалось полиномиальное ядро вида  $k(x, y) = (x \cdot y + 1)^q$ , которое давало наилучшие результаты [5].

Оценим оптимальную степень полиномиального ядра  $q$ . Воспользуемся для этого метрика Евклидова расстояния и косинуса угла между двумя векторами

$$g_i(Z) = \sqrt{(Z - \mu_i)^H (Z - \mu_i)}, \quad (17)$$

$$d_l(Z) = -\frac{Z \cdot Y}{\|Z\| \|Y\|}, \quad (18)$$

где  $Z$  – тестовый образец,  $\mu_l$  – вектор среднего по классу  $l$ ,  $Y$  – образец в обучающей выборке.

При этом, если для образца  $Z$

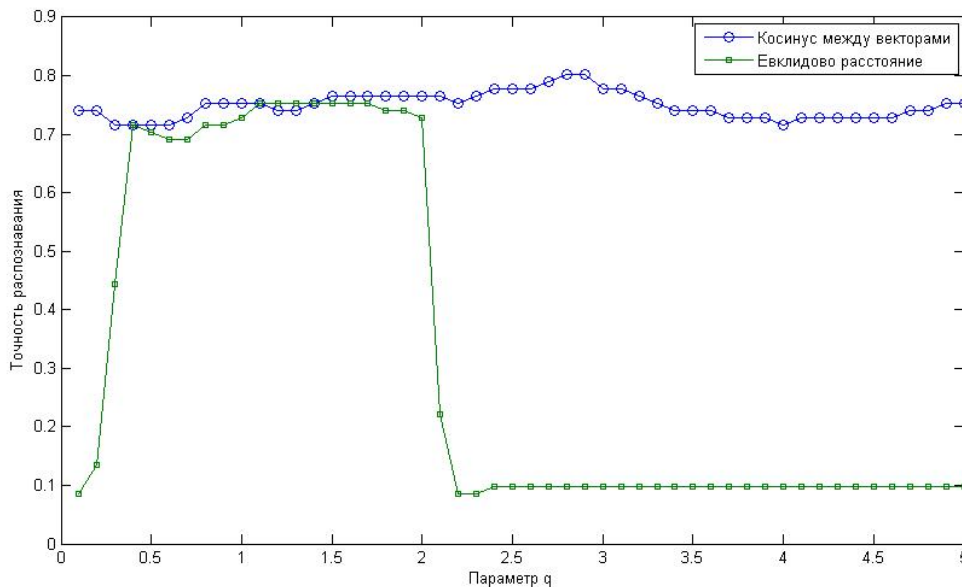
$$g_k(Z) = \min_l (g_l(Z)) \text{ или } d_k(Z) = \min_l (d_l(Z)),$$

то образец  $Z$  принадлежит классу  $k$ .

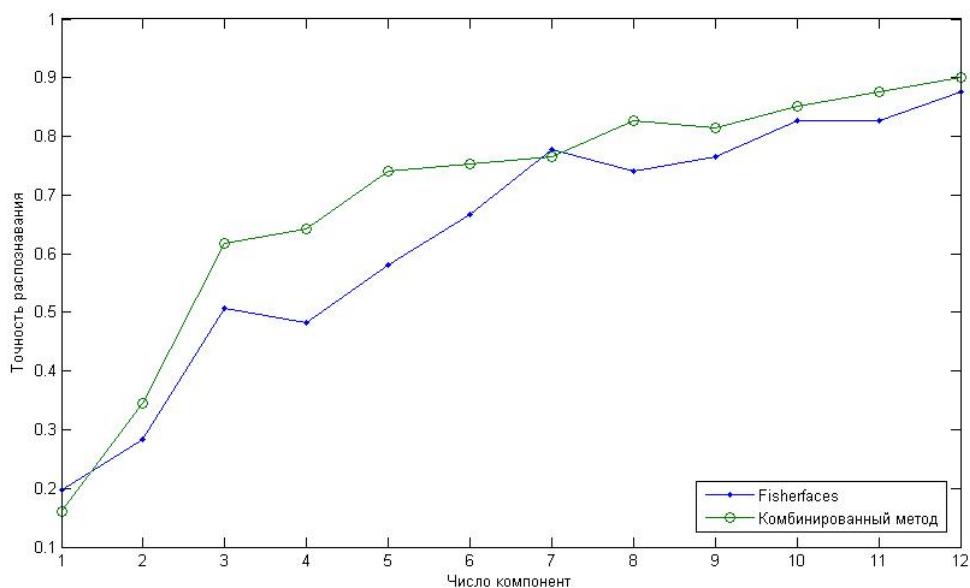
Результаты оценивания степени полиномиального ядра  $q$ , приведены на рисунке 4. Лучшие результаты получены по формуле (18) при параметре  $q = 2.8$ . Для евклидового расстояния оптимальное значение  $q = 1.8$ . В дальнейшем во всех исследованиях использовалась метрика по косинусу угла.

Анализ вероятности распознавания изображений показал, что чем больше число используемых компонент, тем выше точность распознавания. В общем зависимость точности распознавания от числа компонентов близка к экспоненциальной и при большом числе компонентов она стабилизируется, что нельзя сказать о алгоритме *Fisherfaces*, рисунок 5.

Результаты тестирования вероятности распознавания изображений приведены в таблице. Следует отметить, что комбинированный алгоритм дает прирост вероятности распознаваний изображений на 2.5%.



**Рис 4.** Сравнение метрик для метода *Kernel Eigenfaces* в зависимости от параметра  $q$  полиномиального ядра



**Рис 5.** Сравнение предложенного метода и метода *Fisherfaces* в зависимости от числа компонент

**Таблица 1.**  
Результаты тестирования вероятности распознавания изображений (%)

| <i>Eigenfaces</i> | <i>Kernel Eigenfaces</i> | <i>Fisherfaces</i> | Комбинированный алгоритм |
|-------------------|--------------------------|--------------------|--------------------------|
| 62.96             | 72.84                    | 87.65              | 90.12                    |

Предложенный комбинированный алгоритм распознавания изображений можно рекомендовать для использования в системе технического зрения распознавания дорожных знаков.

### Список литературы

1. Fang C.Y. et al. An automatic road sign recognition system based on a computational model of human recognition processing // Computer Vision and Image Understanding. – 2004. – Vol.96, Iss.2. – PP. 237-268.
2. Система распознавания дорожных знаков [Электронный ресурс] / Системы современного автомобиля. – Режим доступа: [http://systemsauto.ru/active/traffic\\_sign\\_recognition.html](http://systemsauto.ru/active/traffic_sign_recognition.html)
3. Escalera S. et al. Traffic-Sign Recognition System // SpringerBriefs in Computer Science 2011. – Springer, 2011. – 96 p., 34 illus.
4. Belhumeur P.N., Hespanha J.P., Kriegman D.J. Eigenfaces vs. Fisherfaces: Recognition using class specific linear projection // Proc. of the 4<sup>th</sup> European Conference on Computer Vision. – Cambridge, UK. – 1996. – PP. 45-58.
5. Yang M.H. Kernel Eigenfaces vs. Kernel Fisherfaces: Face Recognition Using Kernel Methods // Proc. of the 5<sup>th</sup> IEEE International Conference on Automatic Face and Gesture Recognition. – Washington D.C., USA. – 2002. – PP. 215-220.
6. Schölkopf B., Smola A., Müller K.-R. Nonlinear component analysis as a kernel eigenvalue problem // Neural Computation. – 1998. – Vol.10, No.5. – PP. 1299-1319.
7. Голуб Дж. Матричные вычисления / Голуб Дж., Ван Лоун Ч. – М.: Мир, 1999. – 548 с.

В.С. Ситніков, Д.М. Шатохін

## КОМБІНОВАНИЙ АЛГОРИТМ ПІДВИЩЕННЯ ВІРОГІДНОСТІ РОЗПІЗНАВАННЯ ДВОВИМІРНИХ ЗОБРАЖЕНЬ

Запропоновано комбінований метод розпізнавання двовимірних образів на основі лінійних і нелінійних статистичних методів. Для отримання ознак і початкового зниження розмірності простору використовується лінійний та нелінійний метод головних компонент. Ознаки об'єднуються в комплексне число, і далі проводиться розпізнавання за алгоритмом Fisherfaces. Розглянуто вплив коефіцієнтів нелінійного методу, а також метрик для визначення належності до певного класу.

**Ключові слова:** статистичний метод, метод головних компонент, лінійний дискримінантний аналіз, комбінований метод, «ядерні» методи

V. Sitnikov, D. Shatokhin

## COMBINED ALGORITHM FOR INCREASING THE RECOGNITION RATE OF RECOGNITION OF TWO-DIMENSIONAL IMAGES

Proposed combined recognition algorithm combining linear and nonlinear features. To obtain the original features and dimension reduction used linear and nonlinear principal component analysis. The features are combined into a complex number, and then made recognition algorithm Fisherfaces. Considered influence of coefficients of nonlinear method, and metrics for metrics for determining the belonging to the particular class.

**Keywords:** statistical techniques, principal component analysis, linear discriminant analysis, combined method, kernel methods



# НОВИЙ ПІДХІД ДО ПРОБЛЕМИ СТЕГАНОАНАЛІЗУ

А.А. Кобозєва

Одеський національний політехнічний університет,  
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: alla\_kobozeva@ukr.net

Робота присвячена створенню принципово нового підходу до проблеми рішення задач стеганоаналізу на основі адаптації розробленого автором раніше загального підходу до аналізу стану й технології функціонування інформаційних систем. Основним результатом є отримання якісних характерних рис сингулярних спектрів матриць зображень, що дозволяють відокремити контейнер від стеганоповідомлення, сформованого на основі цифрового зображення, збереженого у форматі з втратами.

**Ключові слова:** стеганоаналіз, контейнер, стеганоповідомлення, збурення, сингулярні числа

## Вступ

Активізація в даний момент наукової діяльності в галузі стеганографії, де приховується сам факт існування таємного повідомлення, що викликана заборонаю шифрування на законодавчому рівні в багатьох країнах світу, привела до зростання можливостей використання отримуваних нових розробок різними терористичними структурами [1]. Завдяки цьому надзвичайно актуальним у даний момент є рішення питань, пов'язаних з підвищенням ефективності стеганоаналізу (СА) [2]. При всіх різноманітності наявних стеганоаналітичних методів [1, 3-5] загального підходу до проблеми СА (у сенсі виявлення проведеної вбудови секретної, або додаткової, інформації (ДІ) у деякий об'єкт – основне повідомлення (ОП), або контейнер, чи висновку про відсутність такої вбудови) до теперішнього часу не існує.

Не обмежуючи спільності міркування, далі у якості ОП для спрощення викладу матеріалу розглядається цифрове зображення (ЦЗ). Процес вбудови ДІ в контейнер будемо називати стеганоперетворенням (СПР), а результат цієї вбудови – стеганоповідомленням (СП).

В [6-8] був розроблений новий загальний математичний підхід до аналізу стану й технології функціонування інформаційних систем (ЗПАІС), основна ідея якого полягає в наступному.

Довільна інформаційна система, зокрема, стеганографічна система (або окремо взятий контейнер, СП), формалізується у вигляді двовимірної  $m \times n$ -матриці  $F$  (скінченної множини таких матриць), що дозволяє звести аналіз стану системи до аналізу відповідних матриць. Не обмежуючи спільності міркувань [6], скрізь далі для представлення довільної інформаційної системи використовується одна матриця.

Результат будь-яких дій над системою у загальному випадку формально можна представити у вигляді:

$$\bar{F} = F + \Delta F, \quad (1)$$

де  $\Delta F = f(F)$  – збурення матриці  $F$ , при цьому  $\Delta F$  є деякою функцією  $F$ ,  $\bar{F}$  – матриця перетвореної системи. Як набір формальних параметрів, що однозначно визначають і всебічно характеризують інформаційну систему, використовується множина син-

гулярних чисел (СНЧ) і сингулярних векторів (СНВ), отриманих за допомогою нормального сингулярного розкладання матриці [8], що відповідає розглянутій системі. Будь-яке перетворення інформаційної системи, у тому числі й СПР, представляється у вигляді сукупності збурень СНЧ і (або) СНВ, що дозволяє звести задачу аналізу процесу перетворення (а тому потенційно й СА) і підсумкового стану системи до аналізу цих збурень. Враховуючи це,

Метою автора є розробка нового загального теоретичного підходу до рішення проблеми СА шляхом адаптації ЗПАІС в галузь стеганографії, на основі якого згодом можуть бути побудовані ефективні стеганоаналітичні методи й алгоритми.

Основними математичними інструментами виступають теорія збурень і матричний аналіз.

При рішенні задач СА не може не враховуватися той факт, що в теперішній час зберігання й передача інформації по каналах телекомунікацій у зв'язку зі значним збільшенням її об'ємів здійснюється в стисненому виді. Тому як контейнери нижче розглядаються ЦЗ, збережені з втратами. У зв'язку з цим у рамках досягнення поставленої мети необхідно розв'язати наступні задачі:

1. Виявити якісні характерні риси формальних параметрів, що визначають ЦЗ, збережені у форматах з втратами, до й після СПР. Ці особливості згодом дозволять відокремити ОП від СП, сформованого на основі ЦЗ, збереженого у форматі з втратами. Складовими частинами рішення цієї задачі є наступні:
2. Визначити формальні параметри ЦЗ, збурення яких будуть однаковими, незалежно від області аналізу ЦЗ (просторової, частотної) – універсальні параметри (УП). Рішення даної задачі забезпечить універсальність розроблювальних згодом методів СА з погляду можливості їх ефективної роботи як у просторовій, так і в частотній області (залежно від зручності й специфіки конкретної задачі);
3. Визначити й обґрунтувати якісні відмінності УП ЦЗ, збереженого без втрат, від УП ЦЗ, коефіцієнти якого зазнали операцію квантування;
4. Виявити якісну залежність збурень УП матриць ЦЗ від об'єму інформації, що вбудовується (ОВІ);
5. Визначити й обґрунтувати якісні відмінності множини УП СП, сформованого на базі контейнера, збереженого у форматі з втратами, від множини УП контейнера.

Загальна схема стиснення (з втратами) для ЦЗ складається із трьох основних кроків (після попередньої стандартної розбивки матриці зображення на блоки  $8 \times 8$ ): відображення в частотну область, квантування отриманих коефіцієнтів, ентропійне кодування [7]. Тому, ніяк не обмежуючи область міркувань, нижче розглядається один з найпоширеніших форматів з втратами для ЦЗ – формат JPEG (заснований на дискретному косінусному перетворенні (ДКП), хоча це не має принципового значення).

### Якісні характеристики універсальних параметрів матриць зображень при різних способах їх зберігання

Стан як ОП, так і СП, згідно з ЗПАІС визначається набором СНЧ і СНВ відповідних матриць. Говорячи про СПР, будемо припускати, що результуюче збурення матриці контейнера є малим. Таке обмеження викликане вимогою забезпечення надійності сприйняття СП, що є обов'язковим при роботі будь-якого стеганографічного методу [7].

Аналіз стану контейнера (СП) доцільно звести до аналізу тільки СНЧ, які відповідно до співвідношення [6]

$$\max_{1 \leq j \leq n} |\sigma_j(F) - \sigma_j(F + \Delta F)| \leq \|\Delta F\|_2, \quad (2)$$

де  $\sigma_j(F)$ ,  $\sigma_j(F + \Delta F)$  – СНЧ матриць  $F$ ,  $F + \Delta F$  відповідно,  $\|\Delta F\|_2$  – спектральна норма матриці збурення, є нечутливими до збурних дій (інакше – добре обумовленими), оскільки реакція СНВ на збурні дії різна, а в деяких випадках – об’єктивно непередбачена [6, 7]. Відмітимо, що вибір такого набору формальних параметрів розв’язує задачу 2, оскільки, як показано в [9], СНЧ (збурення СНЧ) матриці яскравості (просторова область) і матриці коефіцієнтів ДКП (частотна область) ЦЗ однакові. Таким чином, як набір УП виступає множина СНЧ матриць (матриць) ОП (СП).

Квантування коефіцієнтів, отриманих у частотній області, що відбувається в процесі стиску ЦЗ, є необоротною процедурою й приводить до деяких закономірних відмінностей СНЧ блоків зображень, збережених з втратами й без втрат. Для останніх у середньому менш, ніж 3% загального числа блоків (ЗЧБ) мають нульові СНЧ [6-8]. Даний факт не є випадковим. Ранг будь-якої матриці визначається кількістю її ненульових СНЧ [6]. Для довільного ЦЗ імовірність того, що рядки (стовпці) чергового блоку відповідної матриці виявляться лінійно залежними, невелика. Найчастіше це виникає у випадку колінеарності (або просто співпадіння) векторів, яка для реального ЦЗ, збереженого без втрат, зустрічається рідко, що й підтверджується обчислювальним експериментом.

Далі, говорячи про відновлення ЦЗ після стиску, будемо розглядати два можливі способи: часткове відновлення (ЧВ) після «повернення» матричних коефіцієнтів із частотної області в просторову не припускає їх округлення на відміну від повного відновлення (ПВ).

Нехай для зберігання ЦЗ використовується схема JPEG з ЧВ. В отриманих матриць у середньому більш, ніж 95% блоків від ЗЧБ містять нульові СНЧ [7]: після квантування й округлення багато з коефіцієнтів ДКП, що відповідають високим і середнім частотам, стануть нульовими, залишаючись нулями після ЧВ, що відповідно до [7] приведе до того, що нульовими виявляться найменші (а можливо й середні за значенням) СНЧ матриць блоків.

Нехай вхідне ЦЗ, що зазнало JPEG-стиску, відновлюється повністю. Ця дія збурить матрицю ЦЗ, отриману після ЧВ, змінить кількість нульових СНЧ у блоках. У тих блоках, де після ЧВ не було елементів, значно менших 0 або більших 255 (як показує обчислювальний експеримент, таких блоків більшість), збурення матриці буде малим, а оскільки СНЧ відповідно до (2) є нечутливими до збурних дій, у цьому випадку – до округлень, їх збурення також будуть незначними [6, 7]. Нульові СНЧ блоків матриці ЧВ ЦЗ хоч і стануть ненулями після ПВ, але їх значення будуть порівнянні з похибкою округлення й між собою, а швидкість зміни близька до нуля, що не є характерним для блоків ЦЗ, збереженого без втрат. Така якісна особливість, яка повністю підтверджується результатами обчислювального експерименту, дає можливість розрізняти блоки ЦЗ, ПВ після стиску, і ЦЗ, збереженого у форматі, що не передбачає квантування коефіцієнтів, і розв’язує задачу 3. Для практичного використання цієї знайденої особливості необхідне встановлення порогу для значення швидкості зміни найменших СНЧ блоків ЦЗ, збережених у різних форматах.

Зіставлення властивостей СНЧ блоків зображень, збережених без втрат і в стисненому стані, дає можливість передбачити характер змін властивостей СНЧ JPEG-контейнера в ході СПР. Виходячи з вищесказаного, очікуваним результатом СПР є зменшення кількості нульових СНЧ в блоках, причому це зменшення буде тим більше, чим більшим буде ОВІ.

## Аналіз результатів роботи стеганографічного методу модифікації найменшого значущого біта

Відповідно до (1), довільне СПР можна представити у вигляді аддитивної вбудови деякої інформації в просторовій області, при цьому  $F$  розглядається як матриця контейнера, а  $\bar{F}$  – матриця СП. ДІ представляється у вигляді випадково сформованої бінарної послідовності.

Для рішення задач 4,5 розглянемо докладно роботу стеганографічного методу модифікації найменшого значущого біта (LSB) [2]. Даний метод обраний автором, головним чином, тому, що СПР тут, з урахуванням випадкового характеру формування стеганошляху [2] і відмінностей в об'ємах ДІ, може приводити до дуже незначних і випадкових збурень  $\Delta F$  матриці контейнера. Можливість виявлення результатів такої збуреної дії дасть для розроблювального автором стеганоаналітичного методу реальну перспективу його ефективної роботи з виявлення «слідів» застосування інших стеганографічних методів. Крім того, LSB є одним з найпоширеніших і широко використовуваних стеганографічних методів на сьогоднішній день. Результат його роботи представляється відповідно до (1), при цьому матриця збурення  $\Delta F$  має елементи, значення яких належать множині  $\{-1,0,1\}$ . При вбудові ДІ надалі будемо враховувати лише ті її біти, які збурюють відповідні пікселі ОП. Так, будемо казати, що ОВІ становить, наприклад, 20%, якщо при вбудові цієї ДІ п'ята частина загального числа пікселів ОП зазнала збурень. Під час роботи LSB-метода, як правило [1, 3-5], вбудовується ДІ, для якої ОВІ приймає значення від 10% до 100%.

Проаналізуємо й оцінимо кількісно збурення СНЧ матриці (блоку матриці) JPEG-контейнера, що виникають внаслідок вбудови ДІ.

Нехай ОВІ дорівнює 10%. Позначимо  $F_B$   $8 \times 8$ -матрицю довільного блоку контейнера. При зроблених вище припущеннях відповідний  $8 \times 8$ -блок  $\Delta F_B$  матриці  $\Delta F$ , яка є матрицею збурення для  $F_B$ , буде мати в середньому 6-7 ненульових значень, які дорівнюють 1 або (-1). Оцінка норми Фробеніуса  $\|\Delta F_B\|_F$  не викликає труднощів й не вимагає додаткових обчислювальних витрат:

$$\|\Delta F_B\|_F \approx \sqrt{6} \approx 2.45.$$

Однак оцінка (2) збурення СНЧ блоку контейнера припускає знання спектральної матричної норми  $\|\Delta F_B\|_2$ . Відповідно до [10]:

$$\|A\|_2 \leq \|A\|_F,$$

з урахуванням чого оцінка (2) для блоку  $F_B$  при ОВІ 10% здобуває вид:

$$|\sigma_j(F_B) - \sigma_j(F_B + \Delta F_B)| \leq 2.45, \quad j = \overline{1,8}. \quad (3)$$

Оскільки найменші СНЧ блоків, як правило, мають значення, порівнянні з одиницею, виходячи з (3), можна було б сподіватися на явні кількісні відмінності в сингулярних спектрах блоків зображення до й після СПР, принаймні, у частині, що містить найменші СНЧ. Однак на практиці абсолютні похибки СНЧ блоків у переважній більшості випадків виявляються набагато менше зазначеної верхньої межі в (3), а тому її використання для розпізнавання ОП і СП викликає труднощі.

Незважаючи на те, що абсолютні похибки СНЧ – збурення, що виникають за рахунок СПР, для всіх СНЧ обмежені зверху однаково, для відносних похибок картина

буде принципово іншою. Для ілюстрації цього в таблиці 1 наведена частина типових результатів обчислювального експерименту для п'яти обраних випадково тестових JPEG-ЦЗ.

**Таблиця 1.**

Відносні похибки СНЧ блоків ЦЗ-контейнера, які виникають під час стеганоперетворення LSB-методом при OBI 10%

| № ЦЗ | Відносні похибки СНЧ блоків ЦЗ-контейнера при СПР LSB-методом для OBI 10% (%) |        |         |         |         |         |          |         |
|------|-------------------------------------------------------------------------------|--------|---------|---------|---------|---------|----------|---------|
|      | Номер СНЧ                                                                     |        |         |         |         |         |          |         |
|      | 1                                                                             | 2      | 3       | 4       | 5       | 6       | 7        | 8       |
| 1    | 0.0605                                                                        | 1.9531 | 1.4846  | 17.2256 | 5.2750  | 19.2736 | 137.1945 | 12.4750 |
| 2    | 0.0274                                                                        | 0.0831 | 0.1253  | 0.7436  | 2.4138  | 8.3467  | 11.3690  | 26.1539 |
| 3    | 0.0203                                                                        | 0.1300 | 1.3231  | 1.9764  | 9.2759  | 9.4315  | 35.1892  | 33.4940 |
| 4    | 0.2488                                                                        | 2.2687 | 20.5072 | 41.0460 | 26.3921 | 6.4525  | 10.8207  | 0.4913  |
| 5    | 0.1943                                                                        | 1.8031 | 1.4811  | 3.3200  | 49.6878 | 38.8003 | 76.4647  | 91.1596 |

Очевидно, що в результаті СПР найбільше «страждають» найменші СНЧ. До того ж для переважної більшості блоків ЦЗ абсолютне значення швидкості зміни двох найменших СНЧ після СПР зростає (частина типових результатів для ілюстрації сказаного наведена в таблиці 2). Це явище є теоретично очікуваним і пояснюється наступним чином. Після ПВ ЦЗ, як вже було відзначено вище, найменші СНЧ, що були нульовими після ЧВ, стають порівнянними між собою (і незначно відрізняються від 0), тобто швидкість їх зміни близька до нуля. Тому навіть мала збурна дія у таких блоках приведе до збільшення відокремленості [6] найменших СНЧ і, як наслідок, до зростання швидкості зміни. Кількісна картина для ЦЗ №4 у табл. 1, відповідає блокам, які вже після ЧВ не мали (або мали малу кількість) нульових СНЧ (такі блоки на зображенні відповідають областям, що містять контури), і ніяк не суперечить очікуваним результатам.

**Таблиця 2.**

Зміна швидкості зростання (спадання) найменших СНЧ у блоках ЦЗ-контейнера після стеганоперетворення з OBI 10%

| № ЦЗ                                                                                    | Кількість блоків (%), для яких швидкість зміни двох найменших СНЧ після СПР |         | № ЦЗ | Кількість блоків (%), для яких швидкість зміни двох найменших СНЧ після СПР |                                                                                     | № ЦЗ | Кількість блоків (%), для яких швидкість зміни двох найменших СНЧ після СПР |         |
|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|---------|------|-----------------------------------------------------------------------------|-------------------------------------------------------------------------------------|------|-----------------------------------------------------------------------------|---------|
|                                                                                         | Зменшується                                                                 | зростає |      | Зменшується                                                                 | зростає                                                                             |      | Зменшується                                                                 | зростає |
| 1                                                                                       | 35.3                                                                        | 64.7    | 4    | 28.8                                                                        | 71.1                                                                                | 7    | 22.1                                                                        | 77.9    |
| 2                                                                                       | 40.6                                                                        | 59.3    | 5    | 24.7                                                                        | 75.2                                                                                | 8    | 31.5                                                                        | 68.5    |
| 3                                                                                       | 30.0                                                                        | 69.9    | 6    | 24.0                                                                        | 76.0                                                                                | 9    | 38.0                                                                        | 62.0    |
| Середнє значення (тестувалися більш 500 ЦЗ)                                             |                                                                             |         |      |                                                                             |                                                                                     |      |                                                                             |         |
| Кількість блоків (%), для яких швидкість зміни двох найменших СНЧ після СПР зменшується |                                                                             |         |      |                                                                             | Кількість блоків (%), для яких швидкість зміни двох найменших СНЧ після СПР зростає |      |                                                                             |         |
| 32                                                                                      |                                                                             |         |      |                                                                             | 68                                                                                  |      |                                                                             |         |

Збурення, які зазнають СНЧ при навіть дуже малому OBI, очевидно приведуть до зміни якісної картини наявності нульових СНЧ у блоках при стандартній розбивці матриці ЦЗ, про що вже говорилося вище. Оскільки виродженість блоків визначається лінійною залежністю стовпців (рядків) відповідних матриць, а вбудова ДІ, змінюючи значення елементів стовпців (рядків), з великою ймовірністю приведе до «руйнування» цієї лінійної залежності (а тому до зростання рангу матриці блоку СП), висувається гі-

потеза: кількість вироджених блоків JPEG-ОП після СПР повинна значно поменшатися, кількість невироджених блоків буде тим більше, чим більше ОВІ.

Для перевірки цієї гіпотези в середовищі Matlab був проведений обчислювальний експеримент, у якому тестувалося більш 500 різних ЦЗ, збережених у форматі JPEG. Ді, як і раніше, представлялася у вигляді випадково сформованої бінарної послідовності. При цьому при СПР мінімально ОВІ склав 10%. Збереження СП проводилося у форматі без втрат (TIF, BMP). В результаті для 100% тестуємих ЦЗ було отримано строге монотонне зростання кількості блоків, що не містять нульових СНЧ, разом з зростанням ОВІ, до того ж, коли ОВІ був більше 60%, практично всі блоки матриці виявлялися невиродженими (у всіх тестуємих зображеннях більш 99% ЗЧБ), тобто СП, сформоване на базі JPEG-контейнера, якісно поводить себе в цьому випадку, як ЦЗ, збережене без втрат.

В ході проведеного обчислювального експерименту були отримані наступні результати, корисні для використання в СА:

1) В результаті вбудови ДІ (навіть у випадку, коли ОВІ дорівнює 10%) матриця СП не містить блоків, які б мали 7, 8 нульових СНЧ. Разом з збільшенням ОВІ в матриці СП послідовно зникають блоки з великою кількістю нульових СНЧ (у табл. 3 наведений типовий приклад результату дослідження одного з тестуємих ЦЗ). Даний результат може бути використаний у процесі СА: якщо в досліджуваного ЦЗ матриця містить блоки з 7 або 8 нульовими СНЧ, то зображення не зазнало СПР, яке збурювало б не менш 10% загального числа пікселів.

2) Для матриць СП при будь-якому ОВІ число блоків з максимально можливою кількістю нульових СНЧ завжди менше числа блоків, у яких нульових СНЧ на одиницю менше максимально можливої кількості. Ця властивість часто не виконується для блоків матриць ЦЗ-контейнерів, що сигналізує про відсутність вбудованої ДІ й може бути використана при СА.

Таблиця 3.

Залежність кількості блоків різного рангу матриці зображення від ОВІ

|                                |          | Кількість блоків матриці, що містять $m$ нульових СНЧ, стосовно загального числа блоків (%) |         |         |         |         |         |         |         |         |
|--------------------------------|----------|---------------------------------------------------------------------------------------------|---------|---------|---------|---------|---------|---------|---------|---------|
|                                |          | $m = 0$                                                                                     | $m = 1$ | $m = 2$ | $m = 3$ | $m = 4$ | $m = 5$ | $m = 6$ | $m = 7$ | $m = 8$ |
| Подане ЦЗ                      |          | 89.36                                                                                       | 4.21    | 1.71    | 1.43    | 1.06    | 0.95    | 0.57    | 0.59    | 0.12    |
| СП з<br>ОВІ<br>рівним<br>$k$ % | $k = 10$ | 93.40                                                                                       | 3.55    | 1.88    | 0.82    | 0.30    | 0.05    | 0       | 0       | 0       |
|                                | $k = 20$ | 95.45                                                                                       | 3.42    | 0.91    | 0.21    | 0.01    | 0       | 0       | 0       | 0       |
|                                | $k = 35$ | 98.24                                                                                       | 1.63    | 0.13    | 0       | 0       | 0       | 0       | 0       | 0       |
|                                | $k = 65$ | 99.78                                                                                       | 0.22    | 0       | 0       | 0       | 0       | 0       | 0       | 0       |

## Висновки

В роботі шляхом адаптації ЗПАІС в галузь стеганографії

- розроблені теоретичні основи загального стеганоаналітичного підходу, заснованого на зведенні процесу СА до аналізу СНЧ матриць блоків ЦЗ;
- отримані якісні відмінності сингулярних спектрів матриць блоків зображень, збережених у різних форматах;
- отримані основні якісні відмінності сингулярних спектрів блоків СП, сформованих на основі JPEG-контейнерів, з різними ОВІ від блоків ОП.

Отримані результати говорять про перспективність запропонованого нового стеганоаналітичного підходу. Визначення кількісних порогових значень для знайдених якісних відмінностей дозволять розробити універсальний метод СА, що є метою подальшої роботи автора.

## Список літератури

1. Gul G. SVD-Based Universal Spatial Domain Image Steganalysis / G. Gul, F. Kurugollu // IEEE Transactions on Information Forensics and Security. – 2010. – Vol.5, No.2. – PP. 349-353.
2. Грибунин В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: Солон-Пресс, 2002. – 272 с.
3. Gul G. Steganalytic features for JPEG compression based perturbed quantization / G. Gul, A.E. Dirik, and I. Avcibas // IEEE Signal Processing Letters. – 2007. – Vol.14, No.3. – PP. 205-208.
4. Lyu S. Detecting hidden messages using higher-order statistics and support vector machines / S. Lyu, H. Farid // Lecture Notes in Computer Science. – New York: Springer-Verlag, 2002. – Vol.2578. – PP. 340-354.
5. Avcibas I. Image steganalysis with binary similarity measures / I. Avcibas, M. Kharrazi, N. Memon, and B. Sankur // EURASIP Journal on Applied Signal Processing. – 2005. – Vol.2005, No.17. – PP. 2749-2757.
6. Кобозева А.А. Анализ информационной безопасности / А.А. Кобозева, В.А. Хорошко. – К.: Изд. ГУИКТ, 2009. – 251 с.
7. Кобозева А.А. Аналіз захищеності інформаційних систем / А.А. Кобозева, І.О. Мачалін, В.О. Хорошко. – К.: Вид. ДУІКТ, 2010. – 316 с.
8. Кобозева А.А. Общий подход к анализу состояния информационных объектов, основанный на теории возмущений / Вісник Східноукраїнського національного університету ім. В. Даля. – 2008. – №8(126), ч.1. – С. 72-81.
9. Кобозева А.А. Повышение эффективности метода обнаружения фальсификации цифрового изображения, основанного на анализе сингулярных чисел матрицы / А.А. Кобозева, Е.А. Трифонова // Труды Одесского политехнического университета. – 2008. – №1(29). – С. 183-190.
10. Кобозева А.А. Спектральна матрична норма як основа різницевого показника візуального викривлення цифрового зображення / Інформатика та математичні методи в моделюванні. – 2011. – Т.1, №1. – С. 5-11.

А.А. Кобозева

## НОВЫЙ ПОДХОД К ПРОБЛЕМЕ СТЕГАНОАНАЛИЗА

Работа посвящена созданию принципиально нового подхода к проблеме решения задач стеганоанализа на основе адаптации разработанного автором ранее общего подхода к анализу состояния и технологии функционирования информационных систем. Основным результатом является получение качественных характерных особенностей сингулярных спектров матриц изображений, позволяющих отделить контейнер от стеганосообщения, сформированного на основе цифрового изображения, хранимого в формате с потерями.

**Ключевые слова:** стеганоанализ, контейнер, стеганосообщение, возмущение, сингулярные числа

A. Kobozeva

## NEW APPROACH TO STEGANALYSIS

The article is devoted to creation of a fundamentally new approach to solving problems of steganalysis based on the adaptation of a common approach to the analysis of the state and functioning of information systems developed by the author. The main result is getting qualitative characteristics of singular matrix spectra of images that allow to distinguish the cover from stego-message formed on the basis of digital image stored in a lossy format.

**Keywords:** steganalysis, cover, stego message, disturbance, singular values

**ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ**

Том 1, номер 2, 2011. Одеса – 96 с., іл.

**ИНФОРМАТИКА И МАТЕМАТИЧЕСКИЕ МЕТОДЫ В МОДЕЛИРОВАНИИ**

Том 1, номер 2, 2011. Одесса – 96 с., ил.

**INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION**

Volume 1, No. 2, 2011. Odesa – 96 p.

---

**Засновник:** Одеський національний політехнічний університет

Зареєстровано Міністерством юстиції України 04.04.2011р.

Свідоцтво: серія КВ № 17610 - 6460Р

Друкується за рішенням Вченої ради Одеського національного політехнічного університету (протокол №8 від 26.04.2011)

**Адреса редакції:** Одеський національний політехнічний університет,  
проспект Шевченка, 1, Одеса, 65044 Україна

Web: <http://www.immm.opu.ua>

E-mail: [immm.ukraine@gmail.com](mailto:immm.ukraine@gmail.com)

© Одеський національний політехнічний університет, 2011