

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеський національний політехнічний університет

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ
МЕТОДИ В МОДЕЛЮВАННІ

INFORMATICS AND MATHEMATICAL
METHODS IN SIMULATION

Том 4, № 4

Volume 4, No. 4

Одеса – 2014
Odesa – 2014

Журнал внесений до переліку наукових фахових видань України
(технічні науки)
згідно наказу Міністерства освіти і науки України № 463 від 25.04.2013 р.

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:

Г.В. Ахмамет'єва

Редакційна колегія:

*Т.О. Банах, П.І. Бідюк, Н.Д. Вайсфельд,
А.Ф. Верлань, Г.М. Востров, В.Б. Дудикевич,
Л.Є. Євтушик, М.Б. Копитчук, С.В. Ленков,
І.І. Маракова, А.Д. Мілка, С.А. Нестеренко,
М.С. Никитченко, С.А. Положаєнко,
О.В. Рибальський, Х.М.М. Рубіо, В.Д. Русов,
І.М. Ткаченко-Горський, А.В. Усов,
В.О. Хорошко, М.Є. Шелест, М.С. Яджак*

Published 4 times a year

Founded by Odessa National Polytechnic
University in 2011

Certificate of State Registration

КВ № 17610 - 6460P of 04.04.2011

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

Associate editor:

A.A. Kobozeva

Executive editor:

A.V. Akhmamet'ieva

Editorial Board:

*T. Banakh, P. Bidyuk, V. Dudykevich,
L. Evtushik, V. Khoroshko, N. Kopytchuk,
S. Lenkov, I. Marakova, A. Milka, S. Nesterenko,
N. Nikitchenko, S. Polozhaenko, J. Rubio,
V. Rusov, O. Rybalsky, M. Shelest,
I. Tkachenko Gorski, 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: просп. Шевченка, 1, Одеса, 65044, Україна

Телефон: +38 048 705 8506

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

E-mail: immm.ukraine@gmail.com

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

Tel.: +38 048 705 8506

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

E-mail: immm.ukraine@gmail.com

© Одеський національний політехнічний університет, 2014

ЗМІСТ / CONTENTS

ІНТЕГРАЛЬНА ДИНАМІЧНА
МОДЕЛЬ РОЗПОВСЮДЖЕННЯ
ТЕПЛА У ШМАТКОВО-ОДНОРІДНИХ
СЕРЕДОВИЩАХ ДЛЯ ВИПАДКУ
БАГАТОВИМІРНОГО ПРОСТОРУ
С.А. Положаєнко

291

INTEGRAL DYNAMIC MODEL FOR
HEAT CONDUCTION IN PIECEWISE
HOMOGENEOUS MEDEUM FOR CASE
OF MULTIDIMENSIONAL SPACE
Polozhaenko S.

МОДЕЛІ КЕРУВАННЯ В СИСТЕМАХ
ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ
БЕЗПЕКИ ДЕРЖАВИ
М.М. Браїловський, С.В. Зибін,
В.О. Хорошко

304

CONTROL MODELS IN STATE
INFORMATION SECURITY SYSTEMS
Brailovsky N., Zybin S., Khoroshko V.

ДВОВИМІРНА ПРОЕКТИВНА
МОДЕЛЬ РУХУ ТІЛА ЛЮДИНИ ТА ЇЇ
ЗАСТОСУВАННЯ В ЗАДАЧАХ
ТЕЛЕМЕДИЦИНИ
В.О. Болтъонков, Нгуєн Гуй Кіонг

312

TWO-DIMENSIONAL PROJECTIVE
MODEL OF HUMAN BODY MOTIONS
AND ITS APPLICATION IN
TELEMEDICINE
Boltenkov V., Nhuen Hui Kionh

АНАЛІЗ ЗАХИСНИХ
ХАРАКТЕРИСТИК СУЧАСНИХ
ВИДІВ СКЛА В ШИРОКОМУ
ДІАПАЗОНІ ЧАСТОТ ПО
АКУСТИЧНОМУ КАНАЛУ ВИТОКУ
В.Б. Дудікевич, І.С. Собчук,
П.І. Гаранюк, В.О. Ракобовчук, В.А. Дей

324

WIDE-BAND ANALYSIS OF
PROTECTIVE PERFORMANCE OF
MODERN GLASS TYPES WITH
REGARD TO ACOUSTIC LEAKAGE
PATHS
Dudykevich V., Sobchuk I., Haranyuk P.,
Rakobovchuk V., Dej V.

МЕТОДИКА КІЛЬКІСНОЇ ОЦІНКИ
НАДІЙНОСТІ СПРИЙНЯТТЯ
ЦИФРОВОГО ЗОБРАЖЕННЯ
О.В. Наріманова, К.О. Трифонова,
А.Є. Кілін, М.С. Кучма

332

TECHNIQUE OF QUANTITATIVE
ASSESSMENT OF DIGITAL IMAGE
PERCEPTION RELIABILITY
Narimanova O., Trifonova K., Kilin A.,
Kuchma M.

МОДЕЛЬ ПРОЯВУ ТА ВИЯВЛЕННЯ
ВПЛИВУ НЕМОНОТОННОСТІ
СТАТИСТИЧНОЇ ХАРАКТЕРИСТИКИ
КВАНТУВАЧА РІВНЯ У ВИХІДНОМУ
СИГНАЛІ СИСТЕМИ АНАЛОГО-
ЦИФРО-АНАЛОГОВОГО
ПЕРЕТВОРЕННЯ
О.В. Рибальський, В.І. Соловійов

337

MODEL TO MANIFEST AND DETECT
THE INFLUENCE OF MONOTONICITY
OF STATIC CHARACTERISTIC OF
AMPLITUDE QUANTIZER IN OUTPUT
SIGNAL OF ALALOG TO DIGITAL TO
ANALOG CONVERSION SYSTEM
Rybalsky O., Solovyev V.

АЛГОРИТМИ ФАКТОРИЗАЦІЇ ДЛЯ
КРИПТОАНАЛІЗУ АСИМЕТРИЧНИХ
КРИПТОСИСТЕМ

Л.М. Тимошенко, К.В. Вербик,
Я.М. Николайчук, С.В. Івасєв

342

FACTORIZATION ALGORITHMS FOR
CRYPTOGRAPHIC ANALYSIS OF
ASYMMETRIC CRYPTO SYSTEMS

Timoshenko L., Verbik K.,
Nikolaichuk Ya., Ivasiev S.

КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ
КРИТИЧНИХ ПРОСТОРІВ
СПІВІСНУВАННЯ НА ФАЗОВИХ
ДІАГРАМАХ
БАГАТОКОМПОНЕНТНИХ ТВЕРДИХ
РОЗЧИНІВ

А.І. Казаков, Л.Т. Кваташидзе,
Г.В. Шаповалов

349

COMPUTER MODELING OF CRITICAL
COEXISTENCE SPACES AT PHASE
DIAGRAMS OF MULTICOMPONENT
SOLID SOLUTIONS

Kazakov A., Kvatashidze L.,
Shapovalov G.

АНАЛІЗ СТАТИСТИЧНОЇ БЕЗПЕКИ
КРИПТОАЛГОРИТМІВ
АСИМЕТРИЧНОГО ШИФРУВАННЯ
НА ОСНОВІ РЕКУРЕНТНИХ
ПОСЛІДОВНОСТЕЙ

Ю.Є. Яремчук

357

STATISTICAL SECURITY ANALYSIS
OF ASYMMETRIC CRYPTO
ALGORITHMS BASED ON
RECURRENT SEQUENCES

Yaremchuk Yu.

ХАРАКТЕРИСТИКА ТА ЗНАЧЕННЯ
МІЖНАРОДНОЇ СТАТИСТИКИ
КІБЕРЗЛОЧИННОСТІ

В.І. Трапезніков

363

CHARACTERISTIC AND
IMPORTANCE OF INTERNATIONAL
CYBER CRIME STATISTICS

Trapeznikov V.

ОРГАНІЗАЦІЯ МОЖЛИВОСТІ
САМОВИРАЖЕННЯ СТУДЕНТІВ
УНІВЕРСИТЕТУ ПРИ ВИВЧЕННІ
ДИСЦИПЛІНИ «ПРОГРАМУВАННЯ
ТА ПІДТРИМКА ВЕБ-
ЗАСТОСУВАНЬ»

Л.В. Скакун

370

ORGANIZATION OF OPPORTUNITY
FOR STUDENT SELF-EXPRESSION
WHEN STUDYING «WEB
APPLICATION PROGRAMMING AND
SUPPORT» DISCIPLINE

Skakun L.

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ
ФІЛЬТРАЦІЙНИХ ПРОЦЕСІВ
ГАЗОНАСИЧЕНИХ НЬЮТОНІВСЬКОЇ
ТА НЕНЬЮТОНІВСЬКОЇ РІДИН В
ЗОНІ ТИСКУ НАСИЧЕННЯ

В.С. Савіч, О.О. Ошовська

375

MATHEMATICAL MODELING OF
FILTRATION PROCESSES OF GAS-
SATURATED NEWTONIAN AND NON-
NEWTONIAN LIQUIDS IN
SATURATION PRESSURE REGION

Savich V., Oshovska O.

INTEGRAL DYNAMIC MODEL FOR HEAT CONDUCTION IN PIECEWISE HOMOGENEOUS MEDEUM FOR CASE OF MULTIDIMENSIONAL SPACE

S.A. Polozhaenko

Odesa National Polytechnic University,
1 Shevchenko Str., Odesa, 65044, Ukraine; e-mail: polozhaenko@mail.ru

Solving a thermal conductivity equation for piecewise homogeneous medium for the case of multidimensional space were considered. An initial problem was reduced to an integral equation (the essence of dynamic model) which was solved in the class of increasing functions. Solvability conditions for the problem were determined.

Keywords: thermal conductivity equation, piecewise homogeneous medium, integral dynamic model, resolvent, functional space.

Introduction

A considerable number of field theory problems are reduced to solving a thermal conductivity equation [1-3]. These problems involve those related to the computation of thermal fields of motors and components of electronic equipment [4, 5]; optimization of thermal conditions in rolling mills [6-8]; and determination of thermal flows in heat-and-power equipment in gas (oil, etc.) network systems [9].

In practical applications, it is sometimes required to solve a thermal conductivity equation for piecewise homogeneous media (ie, a set of homogeneous material layers). Computation of thermal fields in composites or analyses of soil thermal conductivity are the examples of such problems. An analytical solution for the problem mentioned (for the case of one-dimensional space) was described previously [10]. This paper expands and generalizes the result of that work for the case of n -dimensional space.

Statement of Problem

It is required to find the solution of a thermal conductivity equation

$$\frac{\partial u}{\partial t} = a^2(x_i) \sum_{i=1}^n \frac{\partial^2 u}{\partial x_i^2}, \quad (1)$$

which meets the initial condition

$$u(x_1, x_2, \dots, x_n, t)|_{t=0} = F(x_1, x_2, \dots, x_n) \quad (2)$$

and boundary conditions (in the form of reduction conditions)

$$u(x_1, x_2, \dots, x_n, t)|_{x_i=0} = u(0, x_2, \dots, x_n, t), \quad (3)$$

$$\begin{aligned} u(x_1, x_2, \dots, x_n, t) \Big|_{x_2=0} &= u(x_1, 0, \dots, x_n, t), \\ &\dots, \end{aligned} \quad (3)$$

$$\begin{aligned} u(x_1, x_2, \dots, x_n, t) \Big|_{x_n=0} &= u(x_1, x_2, \dots, 0, t), \\ k_1 u'_{x_1}(x_1, x_2, \dots, x_n, t) \Big|_{x_1=0} &= k_1 u'_{x_1}(0, x_2, \dots, x_n, t), \\ k_2 u'_{x_2}(x_1, x_2, \dots, x_n, t) \Big|_{x_2=0} &= k_2 u'_{x_2}(x_1, 0, \dots, x_n, t), \\ &\dots, \\ k_n u'_{x_n}(x_1, x_2, \dots, x_n, t) \Big|_{x_n=0} &= k_n u'_{x_n}(x_1, x_2, \dots, 0, t), \end{aligned} \quad (4)$$

where $k_i, i = \overline{1, n}$ are positive constants,

$$a^2(x_i) = \begin{cases} a_{i_1}^2 & \text{npu } x_i < 0, \\ a_{i_2}^2 & \text{npu } x_i > 0; \end{cases} \quad i = \overline{1, n}. \quad (5)$$

Function $F(x_1, x_2, \dots, x_n)$ is subjected to the following limitation:

$$|F(\cdot)|, |F'_{x_i}(\cdot)| < M \exp(\delta^2 r^2), \quad (6)$$

where $r^2 = \sum_{i=1}^n x_i^2$, M, δ are positive.

We shall seek for a solution in the class of functions satisfying the inequality

$$\max |u(x_1, x_2, \dots, x_n, t)| < M_0 \exp(\delta_0^2 r^2), \quad 0 \leq t \leq t_0, \quad (7)$$

where

$$\delta_0^2 = \frac{\delta^2}{1 - 4 a_0^2 \delta^2 t^2}, \quad (8)$$

$$a_0 = \max [a_{i_1}, a_{i_2}]. \quad (9)$$

Integral representation of the solution

We shall seek for a solution represented as follows (for $x_i < 0$):

$$\begin{aligned} u(x_1, x_2, \dots, x_n, t) &= \int_0^t \left\{ \int_{-\infty}^{+\infty} \dots \int_{-\infty}^{+\infty} G(x_1 - \xi_1, x_2 - \xi_2, \dots, x_n - \xi_n, t - \tau; a_0) \times \right. \\ &\quad \left. \times 2 a_0^2 \psi(\xi_1, \xi_2, \dots, \xi_n, \tau) d\xi_1 d\xi_2 \dots d\xi_n \right\} d\tau + \end{aligned} \quad (10)$$

$$+ \int_0^t \left\{ \int_{-\infty}^{+\infty} \cdots \int_{-\infty}^{+\infty} G(x_1 - \xi_1, x_2 - \xi_2, \dots, x_n - \xi_n, t; a_0) \times F(\xi_1, \xi_2, \dots, \xi_n) d\xi_1 d\xi_2 \dots d\xi_n \right. \quad (10)$$

and as follows (for $x_i > 0$)

$$\begin{aligned} u(x_1, x_2, \dots, x_n, t) = & - \int_0^t \left\{ \int_{-\infty}^{+\infty} \cdots \int_{-\infty}^{+\infty} G(x_1 - \xi_1, x_2 - \xi_2, \dots, x_n - \xi_n, t - \tau; a_0) \times \right. \\ & \times 2a_0^2 \varphi(\xi_1, \xi_2, \dots, \xi_n, \tau) d\xi_1 d\xi_2 \dots d\xi_n \Big\} d\tau + \\ & + \int_0^t \left\{ \int_{-\infty}^{+\infty} \cdots \int_{-\infty}^{+\infty} G(x_1 - \xi_1, x_2 - \xi_2, \dots, x_n - \xi_n, t; a_0) \times F(\xi_1, \xi_2, \dots, \xi_n) d\xi_1 d\xi_2 \dots d\xi_n, \right. \end{aligned} \quad (11)$$

where

$$G(x_1, x_2, \dots, x_n, t; a_0) = \frac{1}{\left(2\sqrt{\pi a_0^2 t}\right)^n} \exp\left[-\left(\sum_{i=1}^n x_i^2\right) / (4a_0^2 t)\right]. \quad (12)$$

One can use a direct check to establish that this function satisfies equation (1) and initial conditions (2).

It is necessary to select φ and ψ functions in such a way that $u(x_1, x_2, \dots, x_n, t)$ function satisfies the conditions for convergence of (3) and (4). In such a case, if φ and ψ satisfy the following conditions:

$$\begin{aligned} |\varphi(x_2, \dots, x_n, t)| & \leq M \exp[\delta^2 r^2(x_1)], \\ |\varphi(x_1, x_3, \dots, x_n, t)| & \leq M \exp[\delta^2 r^2(x_2)], \\ & \dots, \end{aligned} \quad (13)$$

$$\begin{aligned} |\varphi(x_2, \dots, x_{n-1}, t)| & \leq M \exp[\delta^2 r^2(x_n)], \\ |\varphi(x'_2, x'_3, \dots, x'_n, t) - \varphi(x''_2, x''_3, \dots, x''_n, t)| & \leq M \exp(\delta^2 n^2) \times r(|x'_1 - x''_1|), \\ |\varphi(x'_1, x'_3, \dots, x'_n, t) - \varphi(x''_1, x''_3, \dots, x''_n, t)| & \leq M \exp(\delta^2 n^2) \times r(|x'_2 - x''_2|), \\ & \dots, \end{aligned} \quad (14)$$

$$\begin{aligned} |\varphi(x'_2, x'_3, \dots, x'_{n-1}, t) - \varphi(x''_2, x''_3, \dots, x''_{n-1}, t)| & \leq M \exp(\delta^2 n^2) \times r(|x'_n - x''_n|), \\ |\psi(x_2, x_3, \dots, x_n, t)| & \leq \{(M) \exp[\delta^2 r^2(x_1)]\}, \\ |\psi(x_1, x_3, \dots, x_n, t)| & \leq \{(M) \exp[\delta^2 r^2(x_2)]\}, \\ & \dots, \end{aligned} \quad (15)$$

$$|\psi(x_1, x_2, \dots, x_{n-1}, t)| \leq \{(M/\sqrt{t}) \exp[\delta^2 r^2(x_n)]\},$$

$$\begin{aligned}
|\psi(x'_2, x'_3, \dots, x'_n, t) - \psi(x''_2, x''_3, \dots, x''_n, t)| &\leq M \exp(\delta^2 n^2) \times r(|x'_1 - x''_1|), \\
|\psi(x'_1, x'_3, \dots, x'_n, t) - \psi(x''_1, x''_3, \dots, x''_n, t)| &\leq M \exp(\delta^2 n^2) \times r(|x'_2 - x''_2|), \\
&\dots, \\
|\psi(x'_1, x'_3, \dots, x'_{n-1}, t) - \psi(x''_1, x''_3, \dots, x''_n, t)| &\leq M \exp(\delta^2 n^2) \times r(|x'_n - x''_n|),
\end{aligned} \tag{16}$$

and limitation (6) is met, then $u(x_1, x_2, \dots, x_n, t)$ function satisfies inequality (7).

It is easy to show that the integrals that dominate the integrals in (10) and (11) are not convergent for any t value. The following condition should be satisfied to make these integrals convergent:

$$0 \leq t \leq t_0 < \left[1/(4a_0^2 \delta^2)\right]. \tag{17}$$

In this case, δ_0 in expression (7) would be determined by expression (8). Therefore, further in this paper, we shall seek for φ and ψ functions in the class of functions satisfying inequalities (13) to (16).

Reduction of the problem to an integral equation

Now we proceed to determine φ and ψ functions in formulas (10), (11). Here it should be noted that the first term in formula (10) is a single-layer thermal potential, while the first term in formula (11) is a double-layer thermal potential.

Based on the conditions (3) and the properties of a double-layer thermal potential (i.e., component $x_1 = 0$), we may get the following:

$$\begin{aligned}
&\int_0^t \left\{ \int_{-\infty}^{+\infty} \dots \int_{-\infty}^{+\infty} G(0, x_2 - \xi_2, \dots, x_n - \xi_n, t - \tau; a_1) \times 2a_1^2 \varphi(\xi_1, \xi_2, \dots, \xi_n, \tau) d\xi_1 d\xi_2 \dots d\xi_n \right\} d\tau + \\
&+ \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} G(\xi_1, x_2 - \xi_2, \dots, x_n - \xi_n, t - \tau; a_1) \times F(\xi_1, \xi_2, \dots, \xi_n, \tau) d\xi_1 d\xi_2 \dots d\xi_n = \varphi(x_1, x_2, \dots, x_n, t) + \\
&+ \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} G(\xi_1, x_2 - \xi_2, \dots, x_n - \xi_n, t - \tau; a_2) \times F(\xi_1, \xi_2, \dots, \xi_n, \tau) d\xi_1 d\xi_2 \dots d\xi_n
\end{aligned}$$

or

$$\begin{aligned}
&\varphi(x_1, x_2, \dots, x_n, t) = \\
&= \int_0^t \left\{ \int_{-\infty}^{+\infty} \dots \int_{-\infty}^{+\infty} G(0, x_2 - \xi_2, \dots, x_n - \xi_n, t - \tau; a_1) \times 2a_1^2 \varphi(\xi_1, \xi_2, \dots, \xi_n, \tau) d\xi_1 d\xi_2 \dots d\xi_n \right\} d\tau + \\
&+ \sum_{j=1}^2 (-1)^{j-1} \times \int_{-\infty}^{+\infty} \dots \int_{-\infty}^{+\infty} G(\xi_1, x_2 - \xi_2, \dots, x_n - \xi_n, t - \tau; a_2) \times F(\xi_1, \xi_2, \dots, \xi_n, \tau) d\xi_1 d\xi_2 \dots d\xi_n,
\end{aligned} \tag{18}$$

where a_1 and a_2 are determined from (5) when $i = 1$.

Based on conditions (4) and the properties of the normal derivative of the single-layer thermal potential, it follows that:

$$\begin{aligned}
 & k_1 \left\{ \varphi(x_1, x_2, \dots, x_n, t) - \int_{-\infty}^{+\infty} \dots \int_{-\infty}^{+\infty} G'_{\xi_1}(\xi_1, x_2 - \xi_2, \dots, x_n - \xi_n, t - \tau; a_1) \times \right. \\
 & \times F(\xi_1, \xi_2, \dots, \xi_n, \tau) d\xi_1 d\xi_2 \dots d\xi_n \Big\} = k_2 \left\{ \lim_{x_1 \rightarrow +0} \frac{\partial}{\partial x_1} \int_{-\infty}^{+\infty} \dots \int_{-\infty}^{+\infty} G'_{x_1}(x_1, x_2 - \xi_2, \dots, x_n - \xi_n, t - \tau; a_2) \times \right. \\
 & \times 2 a_2^2 \varphi(\xi_1, \xi_2, \dots, \xi_n, \tau) d\xi_1 d\xi_2 \dots d\xi_n - \\
 & \left. - \int_{-\infty}^{+\infty} \dots \int_{-\infty}^{+\infty} G'_{\xi_1}(\xi_1, x_2 - \xi_2, \dots, x_n - \xi_n, t - \tau; a_2) \times F(\xi_1, \xi_2, \dots, \xi_n, \tau) d\xi_1 d\xi_2 \dots d\xi_n \right\}.
 \end{aligned} \quad (19)$$

After eliminating the function φ from the two last equations:

$$\begin{aligned}
 & k_1 \varphi(x_1, \dots, x_n, t) - k_1 \int_{-\infty}^{+\infty} \dots \int_{-\infty}^{+\infty} G'_{\xi_1}(\xi_1, x_2 - \xi_2, \dots, x_n - \xi_n, t - \tau; a_1) \times \\
 & \times F(\xi_1, \xi_2, \dots, \xi_n, \tau) d\xi_1 d\xi_2 \dots d\xi_n = \\
 & = -k_2 \lim_{x_1 \rightarrow +0} \frac{\partial}{\partial x_1} \int_0^t d\tau \int_{-\infty}^{+\infty} \dots \int_{-\infty}^{+\infty} \left[\int_{\tau}^t dt_1 \int_{-\infty}^{+\infty} \dots \int_{-\infty}^{+\infty} G'_{x_1}(x_1, x_2 - \xi'_2, \dots, x_n - \xi'_n, t - t_1; a_2) \times \right. \\
 & \times G(0, \xi'_2 - \xi_2, \dots, \xi'_n - \xi_n, t - \tau; a_1) d\xi'_2 \dots d\xi'_n \Big] 4 a_1^2 a_2^2 \psi(\xi_2, \xi_3, \dots, \xi_n, \tau) d\xi_2 d\xi_3, \dots, d\xi_n + I,
 \end{aligned} \quad (20)$$

where

$$\begin{aligned}
 I = & -k_2 \lim_{x_1 \rightarrow +0} \frac{\partial}{\partial x_1} \int_0^t d\tau \int_{-\infty}^{+\infty} \dots \int_{-\infty}^{+\infty} G'_{x_1}(x_1, x_2 - \xi_2, \dots, x_n - \xi_n, t - \tau; a_2) \times \\
 & \times 2 a_2^2 \left[\sum_{j=1}^2 (-1)^{j-1} \int_{-\infty}^{+\infty} \dots \int_{-\infty}^{+\infty} G'(\xi_1, \xi'_2 - \xi_2, \dots, \xi'_n - \xi_n, \tau; a_j) \times \right. \\
 & \times F(\xi_1, \xi_2, \dots, \xi_n) d\xi_1 d\xi_2 \dots d\xi_n \Big] d\xi'_2 \dots d\xi'_n - \\
 & - \int_{-\infty}^{+\infty} \dots \int_{-\infty}^{+\infty} G'_{\xi_1}(\xi_1, x_2 - \xi_2, \dots, x_n - \xi_n, t; a_2) \times F(\xi_1, \xi_2, \dots, \xi_n, \tau) d\xi_1 d\xi_2 \dots d\xi_n.
 \end{aligned} \quad (21)$$

By direct calculation we can show that:

$$\begin{aligned}
 & \pm 4 a_1^2 a_2^2 \int_{\tau}^t dt_1 \int_{-\infty}^{+\infty} \dots \int_{-\infty}^{+\infty} G'_{x_1}(x_1, x_2 - \xi'_2, \dots, x_n - \xi'_n, t - t_1; a_2) \times \\
 & \times G(0, \xi'_2 - \xi_2, \dots, \xi'_n - \xi_n, t - \tau; a_1) d\xi'_2 \dots d\xi'_n = \\
 & = \pm \frac{a_1}{a_2^{n-1} \pi^{3/2} (2\sqrt{\pi})^{n-2} (t - \tau)^{n/2}} \int_0^{\infty} \exp \left[-z^2 - \frac{x_1^2}{4 a_1^2 (t - \tau)} - \right. \\
 & \left. - \frac{\sum_{l=1}^n (x_l - \xi_l)^2}{4 a_2^2 (t - \tau)} \cdot \frac{x_1^2 + 4 a_2^2 (t - \tau) z^2}{x_1^2 + 4 a_1^2 (t - \tau) z^2} \right] \times \left[\frac{x_1^2 + 4 a_2^2 (t - \tau) z^2}{x_1^2 + 4 a_1^2 (t - \tau) z^2} \right]^{\frac{n-1}{2}} dz.
 \end{aligned} \quad (22)$$

In this formula, the sign of the right side matches the sign of x_1 in the left side.

We denote by I_1 the first term in formula (20). Then

$$I_1 = -\frac{a_1 k_2}{a_2} \psi(x_2, x_3, \dots, x_n, t) + \frac{a_1 k_2 (a_1^2 - a_2^2)}{2 \pi^{3/2} a_2} \times$$

$$\times \int_0^t d\tau \int_{-\infty}^{+\infty} K_0(x_2 - \xi_2, \dots, x_n - \xi_n, t - \tau) \psi(\xi_2, \xi_3, \dots, \xi_n, \tau) d\xi_2 \dots d\xi_n, \quad (23)$$

where

$$K_0(x_2 - \xi_2, \dots, x_n - \xi_n, t - \tau) = \frac{1}{(2\sqrt{\pi})^{n-2} (t - \tau)^{\frac{n+1}{2}}} \times$$

$$\times \int_0^\infty \exp \left[\frac{\sum_{l=1}^n (x_l - \xi_l)^2}{4 a^2(z) (t - \tau)} \right] \times \frac{\rho(z)}{a^{n-2}(z)} \left\{ (n-1) - \frac{\sum_{l=1}^n (x_l - \xi_l)^2}{2 a^2(z) (t - \tau)} \right\} dz, \quad (24)$$

$$a^2(z) = a_2^2 \frac{z^2 + a_1^2}{z^2 + a_2^2}, \quad \rho(z) = \frac{1}{(z^2 + a_1^2)^{3/2} (z^2 + a_2^2)^{3/2}}. \quad (25)$$

After substitution of I_1 into (20), we obtain the following integral equation:

$$\psi(x_2, x_3, \dots, x_n, t) = \frac{a_1 k_2 (a_1^2 - a_2^2)}{2 \pi^{3/2} (a_1 k_2 + a_2 k_1)} \int_0^t d\tau \int_{-\infty}^{+\infty} K_0(x_2 - \xi_2, \dots, x_n - \xi_n, t - \tau) \times$$

$$\times \psi(\xi_2, \xi_3, \dots, \xi_n, \tau) d\xi_2 \dots d\xi_n + f(x_2, x_3, \dots, x_n, t). \quad (26)$$

After the limit of the derivative of I_1 is computed, we determine f function finally using the following formula:

$$f(x_2, x_3, \dots, x_n, t) = -\frac{a_2}{a_1 k_2 + a_2 k_1} \left\{ \sum_{j=1}^2 (-1)^{j-1} \int_{-\infty}^{+\infty} G'(\xi_1, \xi_2' - \xi_2, \dots, \xi_n' - \xi_n, \tau; a_j) \times \right.$$

$$\times F(\xi_1, \xi_2, \dots, \xi_n) d\xi_1 d\xi_2 \dots d\xi_n + \frac{2 k_2}{(2\sqrt{\pi})^{n+1} a_2 t^{\frac{n+2}{2}}} \sum_{j=1}^2 \int_{-\infty}^{+\infty} \frac{|\xi_1| F(\xi_1, \xi_2, \dots, \xi_n)}{a_j^{n+1}} \times$$

$$\times \left[\int_0^\infty \exp \left(-z^2 - \frac{\xi_1^2}{4 a j^2 t} - \frac{\sum_{l=2}^n (x_l - \xi_l)^2}{4 a j^2 t} \cdot \frac{\xi_1^2 + 4 a_1^2 t z^2}{\xi_1^2 + 4 a_2^2 t z^2} \right) \times \right.$$

$$\times \left. \left(\frac{\xi_1^2 + 4 a_1^2 t z^2}{\xi_1^2 + 4 a_2^2 t z^2} \right)^{\frac{n-1}{2}} dz \right] d\xi_1 d\xi_2 \dots d\xi_n + \frac{2 k_2 (a_1^2 - a_2^2)}{(2\sqrt{\pi})^{n+1} a_1 a_2 t^{\frac{n+2}{2}}} \int_{-\infty}^{+\infty} F(\xi_1, \xi_2, \dots, \xi_n) \times$$

$$\times \left[\int_0^\infty \exp \left(-\frac{\xi_1^2}{4 a_1^2 t} - \frac{\xi_1^2}{4 a_1^2 a_2^2 t z^2} - \frac{\sum_{l=2}^n (x_l - \xi_l)^2}{4 a j^2 t} \right) \times \right.$$

$$\left. \right\} \quad (27)$$

$$\times \left[(n-1) - \frac{\sum_{l=2}^n (x_l - \xi_l)^2}{4a^2(z)t} \right] dz \left\{ d\xi_1 d\xi_2 \dots d\xi_n \right\}. \quad (27)$$

Solving an integral equation

Let us consider the following integral equation:

$$\begin{aligned} \psi(x_2, x_3, \dots, x_n, t) = & f(x_2, x_3, \dots, x_n, t) + \lambda \int_0^t \left\{ \int_{-\infty}^{+\infty} K_0(x_2 - \xi_2, \dots, x_n - \xi_n, t - \tau) \times \right. \\ & \left. \times \psi(\xi_2, \xi_3, \dots, \xi_n, \tau) d\xi_2 \dots d\xi_n \right\} d\tau. \end{aligned} \quad (28)$$

We denote by H_0 the class of functions $\varphi(x_1, x_2, \dots, x_n, t)$ that can be subjected to Fourier and Laplace transformations. Denote

$$\int_{-\infty}^{+\infty} \dots \int_{-\infty}^{+\infty} e^{-2\pi i \sum_{j=1}^n u_j x_j} \varphi(x_2, x_3, \dots, x_n, t) dx_2 \dots dx_n = \tilde{\varphi}(u_2, u_3, \dots, u_n, t), \quad (29)$$

$$p \int_0^{\infty} e^{-pt} \tilde{\varphi}(u_2, u_3, \dots, u_n, t) dt = \tilde{\varphi}(u_2, u_3, \dots, u_n, p). \quad (30)$$

Initially, we assume that $f \in H_0$, and shall seek for the solution of equation (28) in H_0 . We shall subject both sides of equation (28) to Fourier transformation. Then

$$\tilde{\psi}(u_2, u_3, \dots, u_n, t) = \tilde{f}(u_2, u_3, \dots, u_n, t) + \lambda \int_0^t \tilde{K}_0(u_2, u_3, \dots, u_n, t - \tau) \tilde{\psi}(u_2, u_3, \dots, u_n, \tau) d\tau. \quad (31)$$

By direct calculation it is easy to show that:

$$\begin{aligned} \int_0^t \tilde{K}_0(u_2, u_3, \dots, u_n, t - \tau) d\tau &= \int_{-\infty}^{+\infty} K_0(x_2, x_3, \dots, x_n, t - \tau) \exp \left[-2\pi i \sum_{j=2}^n u_j x_j \right] dx_2 \dots dx_n = \\ &= 16\pi^{3/2} \sum_{j=2}^n u_j^2 \int_0^{\infty} \rho(z) a^3(z) \exp \left[-4\pi^2 a^2(z)(t - \tau) \sum_{j=2}^n u_j^2 \right] dz. \end{aligned} \quad (32)$$

Now we shall subject both sides of equation (31) to a Laplace transformation. Then:

$$\tilde{\psi}_1(u_2, u_3, \dots, u_n, p) = \tilde{f}_1(u_2, u_3, \dots, u_n, p) + \lambda \tilde{K}_{01}(u_2, u_3, \dots, u_n, p) \tilde{\psi}_2(u_2, u_3, \dots, u_n, p), \quad (33)$$

where

$$\tilde{K}_{01}(u_2, u_3, \dots, u_n, p) = \int_0^\infty e^{-pt} K_0(u_2, u_3, \dots, u_n, t) dt = \frac{2\pi^{3/2}}{(a_2^2 - a_1^2)} \left[\sqrt{\frac{p + 4a_2^2\pi^2 \sum_{j=2}^n u_j^2}{p + 4a_1^2\pi^2 \sum_{j=2}^n u_j^2}} - 1 \right]. \quad (34)$$

Therefore, from expression (31), we get:

$$\tilde{\psi}_1(u_2, u_3, \dots, u_n, p) = \mu \tilde{f}_1(u_2, u_3, \dots, u_n, p) : \left(v + \sqrt{\frac{p + 4a_2^2\pi^2 \sum_{j=2}^n u_j^2}{p + 4a_1^2\pi^2 \sum_{j=2}^n u_j^2}} \right), \quad (35)$$

where $\mu = \frac{a_1^2 - a_2^2}{2\pi^{3/2}\lambda}$, $v = \frac{a_1^2 - a_2^2}{2\pi^{1/2}\lambda}$.

Applying the convolution formula to (35) gives the original function:

$$\begin{aligned} \tilde{\psi}(u_2, u_3, \dots, u_n, t) = & \tilde{f}(u_2, u_3, \dots, u_n, t) + \frac{4\pi^2\mu(|v| - v)(a_1^2 - a_2^2)}{(v^2 - 1)^2} \times \\ & \times \int_0^t \sum_{j=2}^n u_j^2 \tilde{f} \exp \left[-4\pi^2 d_0 (t - \tau) \sum_{j=2}^n u_j^2 \right] d\tau + 8\pi a_1 \mu (a_1^2 - a_2^2) \times \\ & \times \int_0^t \int_0^\infty \frac{z^2 a^2(z) \sum_{j=2}^n u_j^2 \exp \left[-4\pi^2 a^2(z) (t - \tau) \sum_{j=2}^n u_j^2 \right]}{(z^2 - a_1^2)(z^2 - a_2^2)(v^2 z^2 - a_1^2)} dz \times \tilde{f}(u_2, u_3, \dots, u_n, \tau) d\tau, \end{aligned} \quad (36)$$

where

$$d_0 = \frac{a_1^2 v^2 - a_2^2}{v^2 - 1}. \quad (37)$$

It is apparent that the right side of the last equality increases with the increase in u , if $d_0 \leq 0$ and $v < 0$. Therefore, in this case we cannot apply the formula of Fourier transformation. Assuming that $d_0 = b^2 > 0$ or $v = -v \geq 0$, we shall apply the formula of Fourier transformation to (36). Then

$$\begin{aligned} \psi(x_2, x_3, \dots, x_n, t) = & f(x_2, x_3, \dots, x_n, t) + \frac{4\pi^2\mu(|v| - v)(a_1^2 - a_2^2)}{(v^2 - 1)^2} \times \\ & \times \int_0^t d\tau \int_{-\infty}^{+\infty} \sum_{j=2}^n u_j^2 f(u_2, u_3, \dots, u_n, \tau) \exp \left[-2\pi \sum_{j=2}^n u_j x_j - 4\pi^2 b^2 (t - \tau) - \right. \\ & \left. - 2\pi \sum_{j=2}^n u_j \right] du_2 \dots du_n + 8\pi a_1 \mu (a_1^2 - a_2^2) \int_0^t d\tau \int_{-\infty}^{+\infty} \tilde{f}(u_2, u_3, \dots, u_n, \tau) \exp \left[2\pi \sum_{j=2}^n u_j x_j \right] \times \end{aligned} \quad (38)$$

$$\times \left\{ \int_0^{\infty} \frac{z^2 a^2(z) \sum_{j=2}^n u_j^2 \exp \left[-4\pi^2 a^2(z) (t-\tau) \sum_{j=2}^n u_j^2 \right]}{(z^2 - a_1^2) (z^2 - a_2^2) (v^2 z^2 - a_1^2)} dz \right\} du_2 \dots du_n, \quad (38)$$

but

$$\tilde{f}_1(u_2, u_3, \dots, u_n, p) = \int_{-\infty}^{+\infty} \dots \int_{-\infty}^{+\infty} f(\xi_2, \xi_3, \dots, \xi_n, \tau) \exp \left[-2\pi \sum_{j=2}^n \xi_j x_j \right] d\xi_2 \dots d\xi_n. \quad (39)$$

We shall substitute (39) in equation (38). Because $f \in H_0$, we can interchange the integrals (i.e., interchange the order of integration) to get:

$$\begin{aligned} \psi(x_2, x_3, \dots, x_n, t) &= f(x_2, x_3, \dots, x_n, t) + \frac{4\pi^2 b^2 \mu (|v| - v) (a_1^2 - a_2^2)}{(v^2 - 1)^2} \times \\ &\times \int_0^{\infty} \left\{ \int_{-\infty}^{+\infty} \dots \int_{-\infty}^{+\infty} f(u_2, u_3, \dots, u_n, \tau) \times \int_{-\infty}^{+\infty} \sum_{j=2}^n u_j^2 \exp \left[-4\pi^2 b^2 (t-\tau) \sum_{j=2}^n u_j^2 + 2\pi \sum_{j=2}^n (x_j - \right. \right. \\ &\left. \left. - \xi_j) u_j \right] d\xi_2 \dots d\xi_n \right\} d\tau + 8\pi a_1 \mu (a_1^2 - a_2^2) \int_0^t \left\{ \int_{-\infty}^{+\infty} \dots \int_{-\infty}^{+\infty} f(\xi_2, \xi_3, \dots, \xi_n, \tau) \times \right. \\ &\times \left\{ \int_0^{\infty} \frac{z^2 a^2(z)}{(z^2 - a_1^2) (z^2 - a_2^2) (v^2 z^2 - a_1^2)} \times \int_{-\infty}^{+\infty} \sum_{j=2}^n u_j^2 \exp \left[-4\pi^2 a^2 (t-\tau) \sum_{j=2}^n u_j^2 + 2\pi \sum_{j=2}^n (x_j - \right. \right. \\ &\left. \left. - \xi_j) u_j \right] du_2 \dots du_n dz \right\} d\xi_2 \dots d\xi_n \bigg\} d\tau. \end{aligned} \quad (40)$$

Inner integrals in (40) can be computed exactly. Sequentially computing these integrals gives:

$$\begin{aligned} \psi(x_2, x_3, \dots, x_n, t) &= f(x_2, x_3, \dots, x_n, t) + \\ &+ \lambda \int_0^t \left\{ \int_{-\infty}^{+\infty} \dots \int_{-\infty}^{+\infty} R(x_2 - \xi_2, x_3 - \xi_3, \dots, x_n - \xi_n, t - \tau) f(\xi_2, \xi_3, \dots, \xi_n, \tau) d\xi_2 \dots d\xi_n \right\} d\tau, \end{aligned} \quad (41)$$

where

$$\begin{aligned} R(x_2 - \xi_2, x_3 - \xi_3, \dots, x_n - \xi_n, t) &= \\ &= \frac{4\pi^{3/2} (|v| - v)}{(v^2 - 1)^2} \left(\frac{1}{2b\sqrt{\pi t}} \right)^{n-1} \left[(n-1) - \frac{\sum_{j=2}^n x_j^2}{2b^2 t} \right] \exp \left[-\frac{\sum_{j=2}^n u_j^2}{4b^2 t} \right] + \\ &+ \frac{8\pi a_2^2 \mu \pi^{3/2}}{(2b\sqrt{\pi t})^{n+1}} \int_0^{\infty} \frac{z^2}{(z^2 - a_2^2) (v^2 z^2 - a_2^2) a^{n+1}(z)} \left[(n-1) - \frac{\sum_{j=2}^n x_j^2}{2b^2 t} \right] \exp \left[-\frac{\sum_{j=2}^n x_j^2}{4a^2(z)t} \right] dz. \end{aligned} \quad (42)$$

When solving integral equation (28), we have assumed that $d_0 > 0$ or $v \geq 0$. Solving these conditions with respect to λ gives the following solvability conditions:

$$\lambda < \frac{a_1(a_1 + a_2)}{2\pi^{3/2}} = \lambda_0. \quad (43)$$

One can show that integral equation (28) cannot be solved for any f function, if $\lambda \geq \lambda_0$. Moreover, this equation always has a solution in the class of generalized functions, for arbitrary λ . It is a necessary and sufficient condition for the generalized function which is the solution of equation (28) to be an ordinary function, that λ satisfies (43).

Resolvent integral equation

We shall apply the name resolvent to the function defined by (42). Resolvent satisfies the following integral equations:

$$R(x_2, x_3, \dots, x_n, t) = K_0(x_2, x_3, \dots, x_n, t) + \lambda \int_0^t d\tau \int_{-\infty}^{+\infty} \dots \int_{-\infty}^{+\infty} K_0(x_2 - \xi_2, \dots, x_n - \xi_n, t - \tau) \times \\ \times R(\xi_2, \xi_3, \dots, \xi_n, \tau) d\xi_2 \dots d\xi_n, \quad (44)$$

$$R(x_2, x_3, \dots, x_n, t) = K_0(x_2, x_3, \dots, x_n, t) + \lambda \int_0^t d\tau \int_{-\infty}^{+\infty} \dots \int_{-\infty}^{+\infty} R(x_2 - \xi_2, \dots, x_n - \xi_n, t - \tau) \times \\ \times K_0(\xi_2, \xi_3, \dots, \xi_n, \tau) d\xi_2 \dots d\xi_n. \quad (45)$$

Since a resolvent is defined if and only if $d_0 > 0$ or $v \geq 0$, equations (44), (45) are true if and only if $\lambda \geq \lambda_0$. To prove equation (44), we begin with substituting expression (41) into equation (28). After interchanging the integrals and using the arbitrariness of function $f \in H$, one can arrive at equation (44). Equation (45) can be arrived at in a similar way.

Solving the integral equation in the class of increasing functions

We denote by H_2 the function space with functions $\varphi(x_2, x_3, \dots, x_n, t)$ that satisfy the following inequalities within $-\infty < x_1 < +\infty$, $0 < t \leq T_0$:

$$|\varphi(x_2, x_3, \dots, x_n, t)| \leq M \exp[\delta^2 r_1^2(x)], \quad (46)$$

$$|\varphi(x'_2, x'_3, \dots, x'_n, t) - \varphi(x''_2, x''_3, \dots, x''_n, t)| \leq M \exp[\delta^2 m^2] r_1^2(|x' - x''|), \quad (47)$$

where we denote by H_2 , $r_1(x) = \sqrt{\sum_{i=1}^n x_i^2}$, $m = \max[|x'_2|, |x'_3|, \dots, |x'_n|, |x''_2|, |x''_3|, \dots, |x''_n|]$.

It is apparent that $H_0 \in H_2$ and that the functions that satisfy inequalities (15), (16) belong to H_2 . It is easy to show that if $F(x_2, x_3, \dots, x_n)$ is a function which satisfies condition (6), then $f(x_2, x_3, \dots, x_n, t)$ defined by (27) belongs to function space H_2 . Now let us consider integral equation (28), when $f(x_2, x_3, \dots, x_n, t) \in H_2$. We shall seek for a solution of equation (28) in class H_2 . Let $\gamma(x_2, x_3, \dots, x_n, t) \in H_2$. We shall introduce the following notation:

$$K^0 \gamma = \gamma - \lambda \int_0^t d\tau \int_{-\infty}^{+\infty} \cdots \int_{-\infty}^{+\infty} K_0(x_2 - \xi_2, \dots, x_n - \xi_n, t - \tau) \gamma(\xi_2, \dots, \xi_n, t - \tau) d\xi_2 \dots d\xi_n, \quad (48)$$

$$K^{0^{-1}} \gamma = \gamma + \lambda \int_0^t d\tau \int_{-\infty}^{+\infty} \cdots \int_{-\infty}^{+\infty} R(x_2 - \xi_2, \dots, x_n - \xi_n, t - \tau) \gamma(\xi_2, \dots, \xi_n, t - \tau) d\xi_2 \dots d\xi_n. \quad (49)$$

One can state that the following expressions are true:

$$\begin{aligned} K^0 K^{0^{-1}} \gamma &= \gamma + \lambda \int_0^t d\tau \int_{-\infty}^{+\infty} \cdots \int_{-\infty}^{+\infty} R(x_2 - \xi_2, \dots, x_n - \xi_n, t - \tau) \gamma(\xi_2, \dots, \xi_n, t - \tau) d\xi_2 \dots d\xi_n - \\ &\quad - \lambda \int_0^t dt_1 \int_{-\infty}^{+\infty} \cdots \int_{-\infty}^{+\infty} K_0(x_2 - \xi'_2, \dots, x_n - \xi'_n, t - t_1) \gamma(\xi_2, \dots, \xi_n, t - t_1) [\gamma(\xi'_2, \dots, \xi'_n, t_1) + \\ &\quad + \int_0^{t_1} d\tau \int_{-\infty}^{+\infty} \cdots \int_{-\infty}^{+\infty} R(x_2 - \xi_2, \dots, x_n - \xi_n, t_1 - \tau) \gamma(\xi_2, \dots, \xi_n, t_1 - \tau) d\xi_2 \dots d\xi_n] d\xi'_2 \dots d\xi'_n = \\ &= \gamma + \lambda \int_0^t d\tau \int_{-\infty}^{+\infty} \cdots \int_{-\infty}^{+\infty} R(x_2 - \xi_2, \dots, x_n - \xi_n, t - \tau) \gamma(\xi_2, \dots, \xi_n, t - \tau) d\xi_2 \dots d\xi_n - \\ &\quad - \lambda \int_0^t dt_1 \int_{-\infty}^{+\infty} \cdots \int_{-\infty}^{+\infty} K_0(x_2 - \xi'_2, \dots, x_n - \xi'_n, t - t_1) \gamma(\xi'_2, \dots, \xi'_n, t - t_1) d\xi'_2, \dots, d\xi'_n - \\ &\quad - \lambda^2 \int_0^t dt_1 \int_{-\infty}^{+\infty} \cdots \int_{-\infty}^{+\infty} K_0(x_2 - \xi'_2, \dots, x_n - \xi'_n, t - t_1) \times \left[\int_0^{t_1} d\tau \int_{-\infty}^{+\infty} \cdots \int_{-\infty}^{+\infty} R(x_2 - \xi_2, \dots, x_n - \xi_n, t_1 - \tau) \times \right. \\ &\quad \left. \times \gamma(\xi_2, \dots, \xi_n, \tau) d\xi_2 \dots d\xi_n \right] d\xi'_2 \dots d\xi'_n. \end{aligned} \quad (50)$$

Taking into account that

$$\int_{-\infty}^{+\infty} \cdots \int_{-\infty}^{+\infty} K_0(x_2 - \xi_2, \dots, x_n - \xi_n, t - \tau) d\xi_2 \dots d\xi_n = 0, \quad (51)$$

$$\int_{-\infty}^{+\infty} \cdots \int_{-\infty}^{+\infty} R(x_2 - \xi_2, \dots, x_n - \xi_n, t - \tau) d\xi_2 \dots d\xi_n = 0, \quad (52)$$

one may prove that:

$$\begin{aligned} &\int_0^t dt_1 \int_{-\infty}^{+\infty} \cdots \int_{-\infty}^{+\infty} K_0(x_2 - \xi'_2, \dots, x_n - \xi'_n, t - t_1) \left[\int_0^{t_1} d\tau \int_{-\infty}^{+\infty} \cdots \int_{-\infty}^{+\infty} R_0(\xi'_2 - \xi_2, \dots, \xi'_n - \xi_n, t_1 - \tau) \times \right. \\ &\quad \times \gamma(\xi_2, \dots, \xi_n, \tau) d\xi_2 \dots d\xi_n \left. \right] d\xi'_2 \dots d\xi'_n = \int_0^t dt_1 \int_{-\infty}^{+\infty} \cdots \int_{-\infty}^{+\infty} \gamma(\xi_2, \dots, \xi_n, \tau) \times \\ &\quad \times \left[\int_0^t dt_1 \int_{-\infty}^{+\infty} \cdots \int_{-\infty}^{+\infty} K_0(x_2 - \xi'_2, \dots, x_n - \xi'_n, t - t_1) R(\xi'_2 - \xi_2, \dots, \xi'_n - \xi_n, t_1 - \tau) \right] d\xi_2 \dots d\xi_n. \end{aligned} \quad (53)$$

The last expression, actually, represents the interchange formula for two singular integrals. Interchanging the order of integration for two singular integrals usually results in a separation of an additional term. However, this is not true for the case considered here due to the presence of two equalities, (51) and (52).

After substituting expression (53) into formula (50) we get the following:

$$\begin{aligned} K^0 K^{0-1} \gamma = & \gamma + \lambda \int_0^t d\tau \int_{-\infty}^{+\infty} \gamma(\xi_2, \dots, \xi_n, \tau) [R(x_2 - \xi_2, \dots, x_n - \xi_n, t - \tau) - \\ & - K_0(x_2 - \xi_2, \dots, x_n - \xi_n, t - \tau) - \lambda \int_0^t dt_1 \int_{-\infty}^{+\infty} K_0(x_2 - \xi'_2, \dots, x_n - \xi'_n, t - t_1) \times \\ & \times R(\xi'_2 - \xi_2, \dots, \xi'_n - \xi_n, t_1 - \tau) d\xi'_2 \dots d\xi'_n] d\xi_2 \dots d\xi_n \end{aligned}$$

However, on the basis of resolvent equation (44), the integrand is identically equal to zero. Therefore,

$$K^0 K^{0-1} \gamma = \gamma. \quad (54)$$

Similarly,

$$K^{0-1} K^0 \gamma = \gamma. \quad (55)$$

After establishing the last two equalities, it is easy to solve equation (28), if $f(x_2, x_3, \dots, x_n, t)$ is an increasing function. Let us rewrite equation (28) using introduced notation (48):

$$K^0 \psi = f(x_2, x_3, \dots, x_n, t). \quad (56)$$

We shall apply operator K^{0-1} to both sides of the equation. Then, taking into account (54):

$$\psi = K^{0-1} f. \quad (57)$$

Note that (57) represents formula (41) in symbolic notation. Therefore, a solution of equation (28) is determined by formula (41) also when $f \in H_2$, if $\lambda < \lambda_0$.

Conclusion

The basic problem was reduced to determining functions φ and ψ in expressions (10) to (12). As we have already noted, if $f(x_1, x_2, \dots, x_n)$ satisfies condition (6), then function $F(x_2, x_3, \dots, x_n, t)$, which is determined by expression (27), belongs to H_2 . Therefore, the investigation of the solvability conditions for the problem is reduced to the analysis of the coefficient of equation (25). However, it is easy to see that:

$$(a_1 k_2 (a_1^2 - a_2^2)) / (2\pi^{3/2} (a_1 k_2 - a_2 k_1)) < (a_1 (a_1 + a_2)) / (2\pi^{3/2}). \quad (58)$$

Therefore, function $\psi(x_2, x_3, \dots, x_n, t)$ is determined by formula (41), and function $\varphi(x_2, x_3, \dots, x_n, t)$ is determined by formula (18). On this basis, a solution of the initial problem is completely determined.

It should be noted that in the case considered:

$$v = ((a_1^2 - a_2^2) - 2\pi^{3/2} \lambda) / (2\pi^{3/2} \lambda) = (a_2 k_1) / (a_1 k_2) > 0. \quad (59)$$

Then the resolvent can be represented with formula (42), and the first term in this expression becomes equal to zero. Correspondingly, seeking the function $\psi(x_2, x_3, \dots, x_n, t)$ is simplified.

References

1. Тихонов, А.Н. Уравнения математической физики / А.Н. Тихонов, А.А. Самарский. – М.: Наука, 1980. – 724 с.
2. Мацевитый, Ю.М. Моделирование теплового состояния элементов турбомашин / Ю.М. Мацевитый, В.А. Маляренко. — К.: Наукова думка, 1979. – 253 с.
3. Коздоба, Л.А. Решения нелинейных задач теплопроводности / Л.А. Коздоба. – К.: Наукова думка, 1976. – 136 с.
4. Дульнев, Г.Н. Тепловые режимы электронной аппаратуры / Г.Н. Дульнев, Н.И. Тарановский. –Л.: Энергия, 1991. – 248 с.
5. Шеховцов, А.Ф. Математическое моделирование теплопередачи в быстроходных двигателях / А.Ф. Шеховцов. – Харьков: Высшая школа, 1978. – 153 с.
6. Бровман, М.Я. Расчет температурного поля в прокатных валках / М.Я. Бровман, Ю.С. Додин // Инж.-физ. журн. – 1964. – Т.7, № 11. – С. 77-81.
7. Маковский, В.А. Динамика металлургических объектов с распределенными параметрами / В.А. Маковский. – М.: Металлургия, 1991. – 384 с.
8. Бутковский, А.Г. Теория подвижного управления системами с распределенными параметрами / А.Г. Бутковский, Л.Ш. Пустыльников. – М.: Наука, 1980. – 383 с.
9. Максимов, М.М. Математическое моделирование процессов разработки нефтяных месторождений / М.М. Максимов, Л.П. Рыбickaя. – М.: Недра, 1986. – 264 с.
10. Подстригач, Я.С. Термоупругость тел неоднородной структуры / Я.С. Подстригач, В.А. Ломакин, Ю.М. Коляно. – М.: Наука, 1984. – 368 с.

ІНТЕГРАЛЬНА ДИНАМІЧНА МОДЕЛЬ РОЗПОВСЮДЖЕННЯ ТЕПЛА У ШМАТКОВО-ОДНОРІДНИХ СЕРЕДОВИЩАХ ДЛЯ ВИПАДКУ БАГАТОВИМІРНОГО ПРОСТОРУ

С. А. Положаєнко

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: polozhaenko@mail.ru

Розглянуто розв'язання рівняння теплопровідності для шматково-однорідних середовищ у випадку багатовимірного простору. Вихідну задачу було зведено до інтегрального рівняння (суть динамічної моделі), розв'язок якого отримано в класі зростаючих функцій. Визначено умови, за яких задача має розв'язок.

Ключові слова: рівняння теплопровідності, шматково-однорідні середовища, інтегральна динамічна модель, резольвента, функціональний простір.

ИНТЕГРАЛЬНАЯ ДИНАМИЧЕСКАЯ МОДЕЛЬ РАСПРОСТРАНЕНИЯ ТЕПЛА В КУСОЧНО-ОДНОРОДНЫХ СРЕДАХ ДЛЯ СЛУЧАЯ МНОГОМЕРНОГО ПРОСТРАНСТВА

С.А. Положаєнко

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

Рассмотрено решение уравнения теплопроводности для кусочно-однородных сред в случае многомерного пространства. Исходная задача сведена к интегральному уравнению (суть динамической модели), решение которого получено в классе возрастающих функций. Определены условия разрешимости задачи.

Ключевые слова: уравнение теплопроводности, кусочно-однородная среда, интегральная динамическая модель, резольвента, функциональное пространство.

МОДЕЛИ УПРАВЛЕНИЯ В СИСТЕМАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА

Н.Н. Браиловский¹, С.В. Зыбин¹, В.А. Хорошко²

¹ Государственный университет телекоммуникаций,
ул. Соломенская, 7, Киев, 03680, Украина; e-mail: duikt@ua.fm

² Национальный авиационный университет,
просп. Космонавта Комарова, 1, Киев, 03058, Украина; e-mail: professor_va@ukr.net

Рассматривается обобщённый подход к идентификации аппроксимируемой модели, которая может использоваться для описания эволюции системы с распределёнными параметрами. Приближенные уравнения, которые исходят из метода Галёркина, предложены для создания модели. На основе этих уравнений можно провести взаимосвязанную процедуру идентификации и изменения динамических характеристик системы.

Ключевые слова: прогнозирование, системы управления, моделирование процессов, операторы Вольтерры, аппроксимирующая модель.

Введение

Всякая математическая модель, которая используется для описания процессов, протекающих в системах обеспечения информационной безопасности (СОИБ) государства, является только его аппроксимацией. Поэтому выбор типа и структуры модели СОИБ может быть необозначенным и диктуется, в основном, стремлением к наиболее адекватному описанию процессов, протекающих в ней. Возможны различные формы описания одних и тех же процессов. При этом сохраняется полная эквивалентность результатов моделирования по входным и выходным переменным.

В управлении СОИБ часто применяется преобразованное описание, когда не только меняется структура модели, но и формы представления входных и выходных переменных. Так, для линейных динамических систем возможно как временное описание поведения изображающей точки в пространстве состояний, так и преобразованное в частотную область описание на основе передаточных функций. Когда структура модели системы выбрана и по результатам идентификационного эксперимента сделана оценка его параметров или характеристик, возникает проблема дальнейшего использования полученной модели. Обычно вначале исследуются динамические свойства системы аналитическими методами или моделированием отклика системы на различные входные воздействия. При этом в сложных случаях используют преобразования уравнений, которые описывают систему, к виду, удобному для проведения исследований и дальнейшего использования. Для этого применяются канонические представления или аппроксимирующие разложения. Обычно, для выбора обратной связи по заданному спектру в линейных стационарных СОИБ с описанием в пространстве состояний вместо матриц и векторов общего вида, определяющих динамическую модель системы, применяют нормальную или каноническую формы, их представления. Особое значение аппроксимация имеет для распределённых систем, которыми и являются СОИБ государства, описываемые уравнениями в частных производных и соответствующими краевыми и начальными условиями. Без аппроксимации практически невозможно моделировать происходящие процессы в

системах. Поэтому представляется естественным идентифицировать СОИБ в классе аппроксимирующих моделей.

Цель работы

Исследование общего подхода к идентификации аппроксимирующей модели СОИБ, которая может использоваться для описания эволюции системы с распределёнными параметрами, что характерно для систем этого типа.

Основная часть

Чтобы избавиться от неоднозначности при выборе структуры модели и её возможных аппроксимаций, необходимо учитывать, прежде всего, для каких целей идентифицируется модель СОИБ. Модель, используемая для прогнозирования, может существенно отличаться от модели, предназначенной для синтеза управления системы с обратной связью. Это можно увидеть на примерах систем с распределёнными параметрами. Пусть интересующие процессы протекают на интервале времени T (конечном или бесконечном) в системе с параметрами, распределёнными в некоторой пространственной области G . И пусть эти процессы носят эволюционный характер и в классической формулировке описываются уравнениями в частных производных и некоторыми краевыми и начальными условиями. Для идентификации модели таких систем более общей является функционально-аналитическая запись структуры эволюционных уравнений. Под функционально-аналитическим описанием будем понимать задачу Коши:

$$q'(t) + \theta q(t) = f(t), t \in T, q(0) = q_0, q' \in (X \rightarrow X^*), \theta \in (X \rightarrow X^*), f \in X^*, \quad (1)$$

где с помощью функции времени $q(t)$ каждому моменту времени из T ставится в соответствие функция распределения в области G [3]. Под X понимается функциональное пространство со специальной нормой, которое оператором θ отображается в сопряжённое к X пространство X^* . В общем случае θ может быть радиально непрерывным монотонным коэрцитивным оператором Вольтерры. При этом гарантируется существование и единственность решения прямой задачи (1). Функционально-аналитическая задача детально описана в [1,2]. В структуре (1) предполагается также, что граничные условия однородны. Это допустимо, ибо всегда можно указать преобразование, с помощью которого краевую задачу с неоднородными условиями можно свести к однородной. В результате $f(t)$ определяет как объёмное, так и поверхностное входное воздействие на систему. Во многих случаях оператор θ имеет вид $\theta = L^* \theta_0 L$, где L – непрерывный линейный оператор со структурой, известной из простых физических соображений, а L^* – ему сопряжённый. Кроме этих параметров, идентификации могут подлежать начальное распределение q_0 , множество D , допустимыми краевыми условиями и особенностями оператора θ функций из пространства X , а также в некоторых случаях неопределённой может быть область G , на которой определяется функция q . Последнее имеет место, когда отсутствует естественная жёсткая граница области, т.е. когда она имеет размытый характер. При идентификации модели со структурой (1) достаточно предполагать, что измеряемый отклик системы на любое допустимое входное воздействие взаимно однозначный. Тогда класс включаемых в рассмотрение операторов может быть шире указанного раньше. В задачах моделирования процессов, описываемых (1), и других применениях

этой модели широко используется переход к аппроксимирующим (1) приближенным уравнениям с использованием метода Галёркина [2]. В результате модель (1) является как бы промежуточной, имеющей чисто теоретическое значение. Поэтому естественным представляется подход к идентификации модели процессов, которые по своей физической природе соответствуют (1), с использованием связи аппроксимирующих моделей и, в частности, её структуры, вытекающей из метода Галёркина. Пусть $\{h_1, h_2, \dots\}$ – какая-либо полная система линейно независимых элементов, взятых из множества функций области определения оператора (определяемой, главным образом, краевыми условиями). Это множество, в свою очередь, принадлежит некоторому пространству функций положения H , являющимся, гильбертовым пространством. Этому же пространству H принадлежит и функция q_0 , определяющая начальное состояние системы. Пусть H_n – линейная оболочка множества $\{h_1, h_2, \dots\}$, наделённая скалярным произведением, индуцированным из H . Будем считать H_n и ему сопряжённое H_n^* отождествлёнными. Соответственно определяются X_n и X_n^* , а скалярное произведение элементов $f \in X_n^*$ и $q \in X_n$ задаётся выражением $\int_T [f(t), q(t)] dt = \langle f, q \rangle$, где интегрирование понимается по Бохнеру [3].

Каждому оператору θ устанавливается соответствие с оператором $\theta_n \in (X_n \rightarrow X_n^*)$ по правилу $\langle \theta_n q, v \rangle = \langle \theta q, v \rangle, \forall v \in X_n$, и аналогичное соотношение для $f_n \in X_n^*$ примет вид: $\langle f_n, v \rangle = \langle f, v \rangle, \forall v \in X_n$. Тогда для любой последовательности $\{q_{0n}\} \in H_n$, сходящейся в H к q_0 , решение уравнения Галёркина

$$q'_n + \theta_n q_n = f_n q_n(0) = q_{0n}, q_n \in X_n \quad (2)$$

обладает следующими свойствами. На множестве всех непрерывных функций $C(T, H)$ решение q_n при $n \rightarrow \infty$ сходится к решению задачи (1), а на X гарантируется слабая сходимости q_n к q . Таким образом, когда задача (1) разрешима, уравнения Галёркина при достаточно больших n хорошо аппроксимируют процессы, протекающие в рассматриваемом классе систем [4]. Если оператор θ задан с помощью семейства операторов $\{\theta(t)\}$, т.е. $(\theta_q)(t) = \theta(t)q(t)$, то задача (2) представляет собой задачу Коши для системы обыкновенных дифференциальных уравнений. Здесь (θ_q) обозначает функцию с обычным применением оператора θ для фиксированного времени. Операторы Вольтерры, характеризующиеся предысторией, не допускают такого локального представления. Уравнение Галёркина в случае семейства операторов можно записать в виде

$$\langle q'_n(t) + \theta(t) \cdot q_n(t), h_i \rangle = \langle f, h_i \rangle, i = \overline{1, n}. \quad (3)$$

Кроме функционально-аналитической формулировки задачи Коши в виде (1), существуют и другие типы задач, характерные для систем с распределёнными параметрами. Рассмотрим некоторые из них. Пусть имеется гильбертово пространство H для семейства: $M = \{M(t)\}, t \in T$ и $\theta = \{\theta(t)\}, t \in T$, операторов из $H \rightarrow H^*$ и функция $f \in T \rightarrow H^*$. Тогда можно сформулировать два типа задач, известных как псевдопараболические дифференциальные уравнение, называемые также уравнениями Соболева – Гальперна [2]. Первый тип имеет вид

$$M(t)q'(t) + \theta(t)q(t) = f(t), \forall t \in T \quad (4)$$

с начальным условием $q(0) = q_0$, а второй тип уравнений –

$$[M(t)q(t)]' + \theta(t)q(t) = f(t), \forall t \in T \quad (5)$$

с начальным условием $M(0)q(0) = m_0, m_0 \in H^*$.

Структуры уравнений (4) и (5) характерны для различных задач механики сплошной среды. При рассмотрении волновых процессов (электрические и электромагнитные волны) в нелинейных средах может использоваться функционально-аналитическая формулировка модели:

$$q''(t) + M(t)q'(t) + \theta(t)q(t) = f(t), \forall t \in T \quad (6)$$

с начальными условиями $q(0) = q_0, q'(0) = q_1$. Обычно при этом рассматривают гильбертово пространство H и непрерывное плотно вложенное в H рефлексивное банахово пространство V [4]. Под M и θ понимается семейство операторов $M = \{M(t)\}, t \in T$ и $\theta = \{\theta(t)\}, t \in T$, действующих из V в V' . Для остальных функций в выражении (6) имеем: $f \in (T \rightarrow V^*), q \in (T \rightarrow V), q' \in (T \rightarrow V)$ и $q'' \in (T \rightarrow V^*)$.

Вместо семейств операторов $\{M(t)\}$ и $\{\theta(t)\}$, которые записаны в (4) – (6), могут рассматриваться более общие операторы – M и θ , в том числе операторы Вольтерры. При этом все указанные выше формулировки задач удовлетворяют условиям разрешимости при достаточно общих предположениях о свойствах операторов и множеств, на которых они действуют. Кроме того, сходимость галёркинских приближений к решениям соответствующих приведённых уравнений. Если, используя базис $\{h_1, h_2, \dots, h_n\}$ конечномерного подпространства $H_n \subset H$, представить галёркинские приближения в виде

$$q_n(t) = \sum_{k=1}^n x_k(t)h_k, t \in T, \quad (7)$$

то уравнения Галёркина оказываются системой, вообще говоря, нелинейных обыкновенных дифференциальных уравнений относительно временных функций $\{x_k(t)\}, k = \overline{1, n}$. Далее рассмотрим вопрос использования для целевой идентификации структуры модели рассматриваемых процессов в форме приближенных уравнений Галёркина[3].

Рассмотрим подробнее вопрос, в каких случаях модели, основанные на приближенных уравнениях Галёркина, могут использоваться при идентификации систем с распределёнными параметрами. Для этого необходимо определиться с входным воздействием на систему и определяется выходом, с помощью которого осуществляется наблюдение за процессами, протекающими в системе. При выборе структуры уравнений (1) и (4) – (6) отмечалось, что краевые условия, определяющие множество допустимых функций положения, предполагались однородными, что вполне допустимо и не ограничивает общности, поскольку, как указывалось, всякое граничное воздействие можно привести к воздействию $f(t)$, стоящему в правой части операторных уравнений. Число внешних управляемых воздействий на систему, как правило, конечно и в большинстве случаев может быть представлено в виде

$f(t) = \sum_{j=1}^r U_j(t) f_j$, где $U_j(t)$ – функция времени; f_j – функция положения из соответствующего пространства. Тогда имеем

$$\langle f, h_i \rangle = \sum_{j=1}^r b_{ij} u_j(t) = b_i^T u(t), i = \overline{1, n}, \quad (8)$$

где b_i и $u(t)$ – векторы размерности r , причём вектор b_i – с постоянными коэффициентами. Таким образом, в уравнениях Галёркина входное воздействие на систему принимает стандартное представление как произведение матрицы с постоянными коэффициентами на вектор входных переменных u . Наблюдаемый выход системы определяется определениями, осуществляемыми в процессе функционирования системы. Из практических соображений ясно, что каналов контроля всегда конечное число, которое может быть и достаточно большим. Контроль или определения могут быть локальными, когда элементы системы контроля расположены в точках области G , занимаемой системой, или интегральными, когда определяются интегрированные по линиям, поверхностям или участкам области G значения наблюдаемых параметров системы. В любом из этих указанных случаев веток контроля y в галёркинском приближении будет иметь структуру

$$y = g(x, t) + \xi, \quad (9)$$

которая в линейном случае также принимает стандартный вид

$$y = Cx + \xi, \quad (10)$$

где x – вектор, составленный из амплитуд x_k , разложенный (7), ξ – вектор аддитивных помех в каналах контроля. Матрица C в реальных ситуациях, в основном, постоянная. Уравнения Галёркина (2) и (3) или аналогичные им, записанные для операторных уравнений (4) – (6), совместно с (7) и (8) – (10) образуют аппроксимирующую модель рассматриваемых процессов в системах с распределёнными параметрами. Данная модель обладает тем свойством, что её решения при $n \rightarrow \infty$ сходятся к решениям точных уравнений. Кроме того, при решении задачи идентификации в такой постановке могут использоваться существующие методы и алгоритмы. Идентификационный эксперимент должен быть спланирован и поставлен таким образом, чтобы установить структуру оператора θ_n (2), оценить его параметры, идентифицировать матрицу $B = [b_1, b_2, \dots, b_n]$ и вектор – функцию $g(x, t)$ в (9) или матрицу C в (10). Этим полностью определяются динамические свойства и параметры системы. Для нахождения характеристики, определяющих пространственную структуру СОИБ в рамках галёркинских приближений, необходимо по местоположению контролирующих приборов и особенностям интегрального контроля записать соотношения между функциями $g(x, t)$ в (9) или элементами матрицы C в (10) со значениями $\{h_1, h_2, \dots, h_n\}$ в точках области или их интегралами. Полученные в результате выражения служат для восстановления функции h_i . Эта задача, по сути, близка к задаче аппроксимации функций, заданных дискретно. Поскольку она относится к некорректно поставленной задаче и для её решения следует применять регуляризирующие алгоритмы. Пространственная структура и число независимых изменений должны удовлетворять информационной достаточности для идентификации функций h_i . После решения задачи восстановления базисных функций

$h_i, i = \overline{1, n}$, появляется возможность восстановить границу области, где протекают процессы, и краевые условия, которым удовлетворяет всякое решение и, соответственно, все элементы h_i . Для этого необходимо построить изоповерхности, на которых $h_i = \text{const}$ и $\frac{\partial h_i}{\partial v_j} = \text{const}, h_i = \overline{1, n}, v_j$ – нормаль к j -й поверхности. Та

поверхность, на которой удаётся получить однородные краевые условия, удовлетворяемые всеми базисными функциями, и будет границей Γ области G . Математически задачу о нахождении границы Γ и краевых условий на ней можно поставить строго и разработать соответствующий алгоритм её решения. Однако, как указывалось в [3], её дальнейшее практическое использование возможно только через аппроксимирующие модели. Остановимся теперь на некоторых особенностях такого подхода к идентификации систем с распределёнными параметрами, прежде всего на вопросе информационной достаточности. Для восстановления базисных функций, которые определяют пространственную структуру СОИБ, необходимо, чтобы, во-первых, размерность вектора y была достаточно большой, а, во-вторых, контроль должен распределяться по всей области и, по возможности, с учётом неоднородности. Элементы контроля должны размещаться в гуще, где предполагается неоднородность больше [5]. В результате размерность вектора y оказывается больше n , т.е. числа базисных элементов галёркинского разложения. При уравнивании их размерностей задача восстановления h_i для больших номеров становится некорректно поставленной. Действительно, для восстановления таких элементов необходимо высокое пространственное разрешение. Информативность входного воздействия для идентификации обыкновенных дифференциальных уравнений динамики определяется известными результатами теории идентификации динамических систем [1,3]. Самостоятельный интерес представляют случаи, когда в силу разных обстоятельств ограничиваются идентификацией только динамической части модели, т.е. базисные элементы h_i не восстанавливаются и соответственно не могут быть определены другие пространственные характеристики системы.

Пусть оператор θ в (1) и операторы M, θ в (4) – (6) – линейны и их параметры стационарны, контролируемые параметры также линейны и представлены выражением (10) для галёркинского разложения. Рассмотрим для простоты случай с одним входом в (8) и одним выходом в (10). Тогда уравнения Галёркина примут вид:

$$\begin{aligned} \dot{x} &= Ax + bu, \\ y &= c^T x + \xi, \end{aligned} \quad (11)$$

где матрица A и векторы b, c имеют размерность $n \rightarrow \infty$. Поэтому для любого конечного n правые части обоих уравнений должны содержать дополнительные члены, соответствующие немоделируемой (11) динамике системы. При решении задач управления возникает естественный вопрос, каково должно быть соотношение между детерминированной частью системы, определяемой (11), и её неопределённой частью. Другими словами, каким следует выбирать порядок n аппроксимирующей модели. Очевидно, в конкретных задачах его значение может быть различным. Следовательно, при построении аппроксимирующей модели (11) процедура идентификации должна включать поиск подходящей структуры. В данной статье развивается методология, предусматривающая такую ориентированную на управление идентификацию. Её схема состоит из идентификации и синтеза управления, для последовательности субмоделей. Начнём с того, что с помощью неособого преобразования приведём систему (11) к канонической форме Лурье с жордановой формой матрицы A . В результате получаем:

$$\dot{x}_1 = J_1 x_1 + b_1 u,$$

...

$$\dot{x}_p = J_p x_p + b_p u, \quad (12)$$

$$y = \sum_{j=1}^p y_j x_j^T = (x_{j1}, x_{j2}, \dots, x_{ji}, \dots, x_{jm_j})$$

$$y_j = C_j^T x_j, C_j^T = (C_{j1}, C_{j2}, \dots, C_{jm_j}), b_j^T = (0, 0, \dots, 1),$$

вектор-строка размерности

$$m_j, \sum_{j=1}^p m_j = n,$$

$$J_j = \begin{bmatrix} \lambda_j & 1 & \dots & 0 \\ 0 & \lambda_j & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \\ 0 & 0 & \dots & \lambda_j \end{bmatrix} - \text{жорданова клетка.}$$

Преобразование P , с помощью которого осуществляется переход от (11) к (12), означает не что иное, как замену базиса $h^T = \{h_1, h_2, \dots, h_n\}$ конечного пространства H_n на новый $h^{*T} = \{h_1^*, h_2^*, \dots, h_n^*\}$. Действительно, $q_n(t) = h^T x(t) = h^T P x^*(t)$, где $x^{*T}(t) = (x_1^T, x_2^T, \dots, x_p^T) h^* = P^T h$.

Новая система функций положения h^* галёркинское разложения, является нормированным по входу квазиортогональным базисом. Для простых собственных значений базис будет строго ортогональным. Вторая каноническая форма представления системы соответствует нормированному по выходу квазиортогональному базису. В дальнейшем предполагаем, что все собственные значения λ_j действительные, что оправдано для операторов θ параболического или квазипараболического типов. Применяемый подход легко обобщить и на случай с комплекснозначными λ_j . Группа уравнений, соответствующая каждой жордановой клетке, рассматривается как субмодель системы, которая играет ключевую роль в развиваемом подходе к совместной идентификации и синтезе управления. Предполагается осуществить итерационный синтез обратной связи по идентифицированной субмодели с наименьшим собственным значением. Не нарушая общности, можно считать, что это значение принадлежит первому блоку.

Выводы

Предлагаемый подход, в котором идентификация модели и синтез стабилизирующей обратной связи рассматривается взаимосвязано как унифицированный итерационный процесс, может служить основой для создания методик проектирования систем обеспечения информационной безопасности с

управлінням як любого об'єкта, так і государства. Его главное преимущество в том, что указана последовательность достаточно простых операций, приводящих от экспериментальных наблюдений за системой к приемлемым с практической точки зрения структуре и параметрам системы. Описанная методика удовлетворительно аппроксимируется линейными динамическими уравнениями высокого порядка. Основная трудность описанного подхода состоит в том, как правильно обосновать и определить порядок субмодели.

Список литературы

1. Баранов, В.Л. Відновлення та оптимізація інформації в системах прийняття рішень / В.Л. Баранов, М.М. Браїловський, А.А. Засядько, Н.Ф. Казакова, В.О. Хорошко. – К: Вид. ДУІКТ, 2009. – 134с.
2. Гаевский, Х. Нелинейные операторные уравнения и операторные дифференциальные уравнения / Х. Гаевский, К. Грегер, К. Захариас – М: Мир, 1978. – 336с.
3. Баранов, В.Л. Моделювання фізичних процесів в інформаційній безпеці / В.Л. Баранов, М.В. Капустян, Р.М. Костюченко, В.О. Хорошко. – К: Вид. ДУІКТ, 2009. – 175с.
4. Гиг Дж Ван. Прикладная общая теория систем: в 2-х томах / Гиг Дж Ван. – М: Мир, 1981. – 733 с.
5. Губарев, В.Ф. Оценивание векторов состояния динамических систем в условиях неопределённости / В.Ф. Губарев // Проблемы управления и информатики. – 1996. – № 1-2. – С. 91-100.

МОДЕЛІ КЕРУВАННЯ В СИСТЕМАХ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

М.М. Браїловський¹, С.В. Зибін¹, В.О. Хорошко²

¹ Державний університет телекомунікацій,
вул. Соломянська, 7, Київ, 03110, Україна; e-mail: duikt@ua.fm

² Національний авіаційний університет,
просп. Космонавта Комарова, 1, Київ, 03058, Україна; e-mail: professor_va@ukr.net

Розглядається загальний підхід до ідентифікації апроксимуючої моделі, що може використовуватись для опису еволюції системи з розподіленими параметрами. Наближені рівняння, що виходять з методу Гальоркіна, запропоновані для утворення моделі. На основі цих рівнянь можна провести взаємозв'язану процедуру ідентифікації і зміну динамічних характеристик системи.

Ключові слова: прогнозування, системи керування, моделювання процесів, оператори Вольтерри, апроксимуюча модель.

CONTROL MODELS IN STATE INFORMATION SECURITY SYSTEMS

N.N. Brailovsky¹, S.V. Zybin¹, V.A. Khoroshko²

¹State University of Telecommunications
7, Solomyanska Str., Kyiv, 03110, Ukraine; e-mail: duikt@ua.fm

²National Aviation University,
1, Kosmonavta Komarova ave., Kyiv, 03058, Ukraine; e-mail: professor_va@ukr.net

We discuss a generalized approach to the identification of approximation model that can be used to define the evolution of a distributed parameter system. The approximate equations generated by Galerkin's method are proposed to develop the model. Based on these equations, one may perform interrelated procedures to identify the model and to change the system dynamics.

Keywords: prediction, control systems, process modeling, Volterra operators, approximation model.

ДВУМЕРНАЯ ПРОЕКТИВНАЯ МОДЕЛЬ ДВИЖЕНИЯ ТЕЛА ЧЕЛОВЕКА И ЕЕ ПРИМЕНЕНИЕ В ЗАДАЧАХ ТЕЛЕМЕДИЦИНЫ

В.А. Болтенков, Нгуен Гуи Кионг

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

Предложена двумерная проективная точечная модель движения тела человека на основании анализа видеопотока. Модель предназначена для построения системы дистанционной двигательной реабилитации пациентов с заболеваниями опорно-двигательного аппарата. Проверка адекватности модели проведена на прототипе системы. Разработана методика выработки рекомендаций по корректировке движений пациента на основе мер близости векторов.

Ключевые слова: модель движения тела человека, анализ видеопотока, двигательная реабилитация, кинематические параметры, меры близости векторов

Введение, актуальность проблемы, постановка цели и задач исследования

Автоматизированный анализ движения тела человека сегодня является чрезвычайно востребованной темой исследований в области компьютерного зрения и интеллектуальной обработки изображений. В области телемедицины [1], спорта [2,3] и видеонаблюдения [4] анализ движений человека является эффективным исследовательским и диагностическим инструментом и средством мониторинга. Анализ опирается на исследование положения тела и его частей в последовательных кадрах видеопотока с целью трекинга местоположения, ориентации и динамики частей тела. В зависимости от цели анализа представление движений базируется на математических моделях различного уровня сложности.

Особый практический интерес в условиях стремительного развития телемедицины и недостаточного финансирования отрасли здравоохранения представляют дистанционные системы двигательной реабилитации. Действие подобных систем основано на многократном повторении пациентом движений, продемонстрированных удаленным врачом-инструктором и зарегистрированных в видеопотоке [5]. На основании анализа движений пациента автоматическая система должна выдать ему конкретные рекомендации по коррекции неправильно выполненных движений. Основным требованием к таким системам с точки зрения удобства пользователя является ее функционирование в реальном масштабе времени. С другой стороны, для того, чтобы система была общедоступной, она должна быть реализована на несложной аппаратной платформе (бытовая веб-камера, компьютер средней производительности) со свободным программным обеспечением.

Целью данного исследования является построение и предварительная верификация простой и адекватной модели движения тела человека для доступных широкому кругу пользователей систем двигательной реабилитации пациентов с болезнями опорно-двигательного аппарата. Для достижения цели решены следующие задачи:

- классификация и анализ существующих моделей движения тела человека в видеопотоке,
- построение двумерной кинематической проективной модели движения,
- исследование количественных мер отклонения движения пациента от обучающего движения инструктора.

Основная часть

Анализ и классификация существующих моделей движения тела человека. Все существующие модели движения тела человека при анализе видеопотока можно разделить по двум принципам: формирования модели внутри кадра видеопотока; моделирования движения при последовательном анализе кадров видеопотока (рис.1).

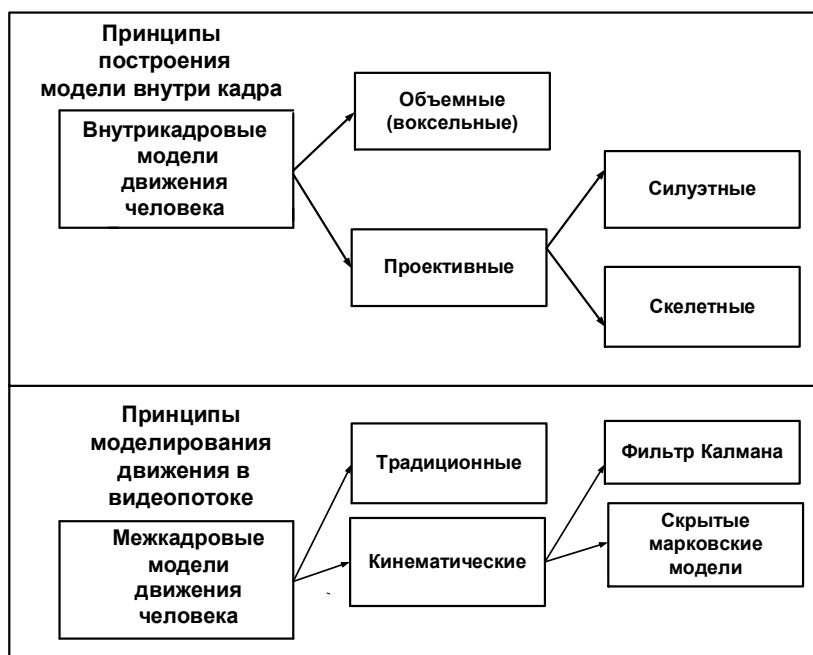


Рис.1. Классификация моделей движения тела человека в видеопотоке

По принципу формирования внутри кадра видеопотока модели делятся на объемные или воксельные (термин воксель, англ. voxel введен по аналогии с пикселем как объемный элемент – volume element) и проективные, т.е. двумерные.

Объемные модели [6,7] достаточно точны и наглядны, однако требуют для своего построения применения трехмерных приемников видеоизображения с датчиками дальности типа Kinect [8], а для обработки видеопотока в реальном масштабе времени – серьезных вычислительных мощностей или применения видеоускорителей на графических процессорах. Такие модели не могут быть рекомендованы для систем широкого применения ввиду высокой стоимости аппаратной части и специализированного программного обеспечения видеоприемников Kinect. Кроме того, построение объемных моделей требует от пользователя использования нателных маркеров или специальной разноцветной одежды, что создает определенные неудобства для пациентов.

Проективные или двумерные модели, в свою очередь, могут быть разделены на силуэтные [9] и скелетные [10]. Силуэтные модели формируются на основании множества точек выделенного на изображении силуэта человека. Получение

качественного силуэта требует применения видеокамер высокого разрешения и специального освещения. Кроме того, необходимость трекинга большого количества точек силуэта предъявляет высокие требования к производительности вычислительной системы. Скелетные модели, основанные на выделении скелета (т.е. однопиксельной центральной линии фигуры) изображения человека, известны достаточно давно [10]. Особенно популярна «звездная» модель (англ. star model) [11], согласно которой тело человека описывается конечными точками скелета (голова, конечности) и его центроидом, построенным по пяти точкам. Звездная модель экономна в вычислительном отношении, однако описание движения тела человека 6-ю точками не позволяет точно отследить детали движения частей тела. Такие модели пригодны только для систем охранного видеонаблюдения.

По принципу моделирования движения в моделях можно выделить наибольший класс «традиционных». Эти модели основаны на описании движения фильтром Калмана [12] или скрытой марковской цепью [13]. Как калмановские, так и марковские модели построены на состояниях, каждое состояние описывается координатами x, y набора характерных точек и их производными $dx/dt, dy/dt$, и при работе в реальном масштабе времени требовательны к вычислительным ресурсам. Кинематические модели [14], в том числе и предложенная ниже, основаны на содержательных физических моделях движения.

Проведенный анализ показывает, что существующие модели движения человека на основании анализа видеопотока требуют серьезных затрат на аппаратно-программную реализацию и не могут быть рекомендованы для построения доступных систем двигательной реабилитации пациентов. Поэтому далее предлагается модель, свободная от установленных недостатков.

В двумерной проекции, которой является кадр видеопотока, любое положение тела человека может быть полностью описано набором характерных точек (ХТ) (рис.2), перечень которых приведен в таблице 1 [15].

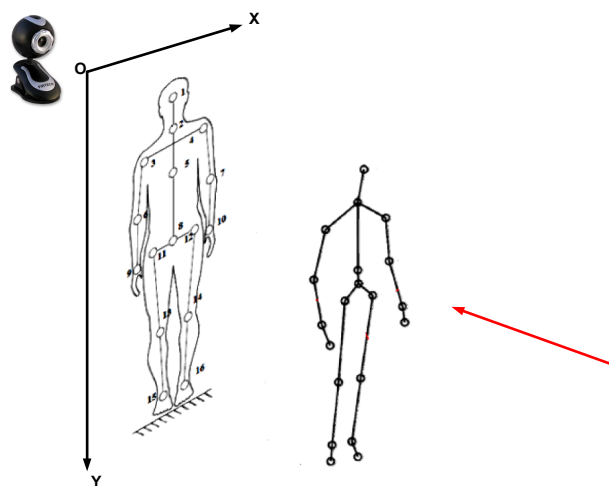


Рис.2. Схема формирования двумерной точечной проективной модели движения тела человека

Будем обозначать ХТ их номером $n (n=1,...,16)$. Для ракурсной проекции, отличной от нормальной (с углом зрения камеры, отличным от нуля) на изображении тела могут быть видны не все точки, но наблюдаемой совокупности практически всегда достаточно для решения задачи сравнения наблюдаемого движения с эталонным и оценки их отличия. С приемлемой для нашей задачи точностью можно совместить

точки 9 и 10 с центрами соответствующих ладоней, точки 1 – с головным окончанием скелета, а 15 и 16 – с окончаниями ног человека в процедуре скелетизации.

Таблица 1.

Перечень характерных точек тела человека

Номер ХТ	Описание ХТ	Номер ХТ	Описание ХТ
1	Проекция центра масс головы	9	Правый кистевой сустав
2	C7- проекция последнего шейного позвонка (центр вращения головы)	10	Левый кистевой сустав
3	Правый плечевой сустав	11	Правый бедренный сустав
4	Левый плечевой сустав	12	Левый бедренный сустав
5	5-ый грудной позвонок (примерная проекция центра масс человека)	13	Правый коленный сустав
6	Правый локтевой сустав	14	Левый коленный сустав
7	Левый локтевой сустав	15	Правый голеностопный сустав
8	L1 - проекция 1-го поясничного позвонка (центр вращения тела вокруг ножной опоры)	16	Левый голеностопный сустав

Любое движение тела с достаточной точностью может быть представлено последовательностью набора ХТ, зарегистрированных на последовательных кадрах видеопоследовательности. Для построения двигательной (кинематической) модели рассмотрим фрагмент из N последовательных кадров видеопотока с частотой повторения кадров f (межкадровый период $\tau = 1/f$). Предполагая, что частота кадров достаточно велика, будем считать, что каждая из ХТ, участвующая в сложном движении тела на протяжении трех последовательных кадров совершает вращательное движение. В этом случае траектория каждой ХТ в пределах трех кадров представляет собой дугу окружности. Для каждого фрагмента траектории может быть найден мгновенный центр вращения и радиус дуги (рис. 3). На рис.3 для ясности изложения показаны прореженные последовательные кадры движения тела, т.е. рисунок реально соответствует малой частоте повторения кадров.

Для данного трехкадрового фрагмента j ($j=1, \dots, N-2$) может быть рассчитано положение центра мгновенного вращения O_j по координатам трех последовательных положений ХТ n_i ($i=1,2,3$) в кадре - $(x_i, y_i), (x_{i+1}, y_{i+1}), (x_{i+2}, y_{i+2})$ и радиус вращения R_j (в частности, на рис.3 построения приведены для точки $n=9$ (правая кисть). Построение центра окружности по трем точкам – известная и вычислительно простая задача аналитической геометрии [16].

Для известного радиуса вращательного движения можно оценить тангенциальную скорость $v_{\tau j}$ и тангенциальное ускорение $a_{\tau j}$: $v_{\tau j} = \omega_j R_j$, $a_{\tau j} = \varepsilon_j R_j$, где ω_j и ε_j – угловая скорость и угловое ускорение точки n для кадрового фрагмента j .

Угловую скорость можно оценить на участке траектории AB как $\omega_{j1} = \Delta\phi_1/\tau$, на участке траектории BC как $\omega_{j2} = \Delta\phi_2/\tau$, где $\Delta\phi_1$ и $\Delta\phi_2$ – угловые приращения положения точки n от кадра к кадру, τ – период повторения кадров. $\Delta\phi_1$ и $\Delta\phi_2$ находятся как углы между векторами $O_j A$, $O_j B$ и $O_j B$, $O_j C$ с известными

координатами. Угловая скорость для фрагмента j ω_j оценивается как среднее арифметическое ω_{j1} и ω_{j2} . Угловое ускорение для фрагмента j ε_j рассчитывается как $\varepsilon_j = \Delta\varepsilon_j / \Delta t = (\omega_{j2} - \omega_{j1}) / \tau$, а линейное ускорение как $a_{\tau j} = \varepsilon_j R_j$.

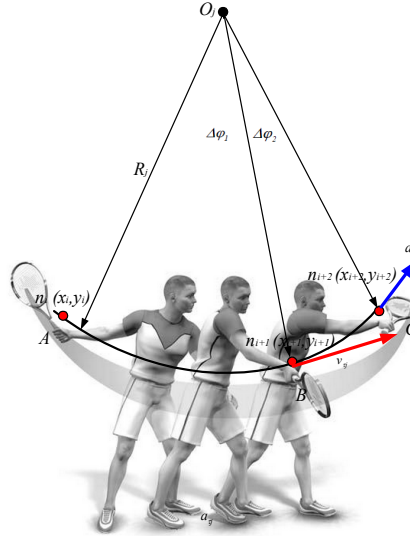


Рис.3. Построение фрагмента траектории и оценка кинематических параметров для характерной точки

Таким образом, для последовательности N кадров из видеопотока можно построить для каждой точки n , наблюдаемой в кадрах $(N - 2)$ столбца, описывающих движение тела в двумерной проекции, представляющих собой набор координат точки, ее тангенциальную скорость и тангенциальное ускорение.

Отметим, что при малой кривизне фрагмента траектории ХТ координаты мгновенного центра вращения $O_j(x_{oj}, y_{oj})$ и величина радиуса вращения R_j могут выходить за пределы кадра в кадровых пиксельных координатах в любой квадрант, смежный с кадром. Тем не менее, такое «расширение кадра» не влияет на результаты расчетов мгновенных кинематических параметров.

Таким образом, модель движения тела в рамках фрагмента видеопоследовательности из N кадров можно представить в виде следующей матрицы

$$\begin{pmatrix} 1 & 1,2,3 & x_1^1, y_1^1 & v_{\tau_1}^1 & a_{\tau_1}^1 & \dots & x_1^n, y_1^n & v_{\tau_1}^n & a_{\tau_1}^n & \dots & x_1^{16}, y_1^{16} & v_{\tau_1}^{16} & a_{\tau_1}^{16} \\ 2 & 2,3,4 & x_2^1, y_2^1 & v_{\tau_2}^1 & a_{\tau_2}^1 & \dots & x_2^n, y_2^n & v_{\tau_2}^n & a_{\tau_2}^n & \dots & x_2^{16}, y_2^{16} & v_{\tau_2}^{16} & a_{\tau_2}^{16} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ j & j, j+1, j+2 & x_j^1, y_j^1 & v_{\tau_j}^1 & a_{\tau_j}^1 & \dots & x_j^n, y_j^n & v_{\tau_j}^n & a_{\tau_j}^n & \dots & x_j^{16}, y_j^{16} & v_{\tau_j}^{16} & a_{\tau_j}^{16} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ K & N-2, N-1, N & x_K^1, y_K^1 & v_{\tau_K}^1 & a_{\tau_K}^1 & \dots & x_K^n, y_K^n & v_{\tau_K}^n & a_{\tau_K}^n & \dots & x_K^{16}, y_K^{16} & v_{\tau_K}^{16} & a_{\tau_K}^{16} \end{pmatrix}. \quad (1)$$

Опишем структуру построения матрицы. Первый элемент строки – номер трехкадрового фрагмента j ($j = 1, 2, \dots, K = N - 2$), поскольку для построения первого фрагмента используются три кадра). Второй элемент строки $i, i+1, i+2$ – номера кадров, обрабатываемых в j -м фрагменте ($i = 1, 2, \dots, N$). Последующие элементы строки связаны с координатами, скоростями и ускорениями ХТ, поэтому в качестве верхнего индекса они содержат номер n ХТ ($i = 1, \dots, 16$). В частности, x_j^n, y_j^n –

координаты точки n в середине фрагмента j , $v_{\tau_j}^n$, $a_{\tau_j}^n$ – касательные скорость и ускорение точки n соответственно, рассчитанные для фрагмента j видеопотока.

Матрица (7) не всегда будет полноразмерной по n , поскольку все ХТ могут наблюдаться только при движении всего тела в полном фронтальном ракурсе. При любых угловых ракурсах и объемных движениях наблюдается только часть ХТ, т.е. при таких ракурсах в матрице, начиная с третьего столбца, будут участвовать только элементы с верхними индексами, соответствующими реально обнаруженным в кадре точкам.

С целью проверки предложенных принципов построения дистанционной системы двигательной реабилитации был разработан прототип системы. Для реализации прототипа была использована следующая аппаратная платформа: бытовая видеокамера Logitech HD Webcam C310, кадр 640*480 пс, компьютер CPU: Intel 2 Duo Chipset, RAM 4GB DDR3 1,6 ГГц, Win 7. Программная часть системы реализована на языке C⁺⁺. Основные алгоритмы реализованы с использованием популярной библиотеки с открытым кодом для обработки видео OpenCV [17]. Кратко изложим этапы предварительной внутрикадровой обработки видеопотока для реализации системы. В каждом кадре видеопотока, следующего с веб-камеры с частотой кадров 25 1/с производятся следующие операции.

1. Выделение фона изображения.
2. Вычитание фона из исходного изображения с одновременной бинаризацией.

Результатом операции является бинаризованное изображение тела.

3. Операция построения скелета. Результатом операции является однопиксельная центральная линия тела, называемая скелетом.

Пример осуществления трех перечисленных операций внутрикадровой обработки приведен на рис. 4.

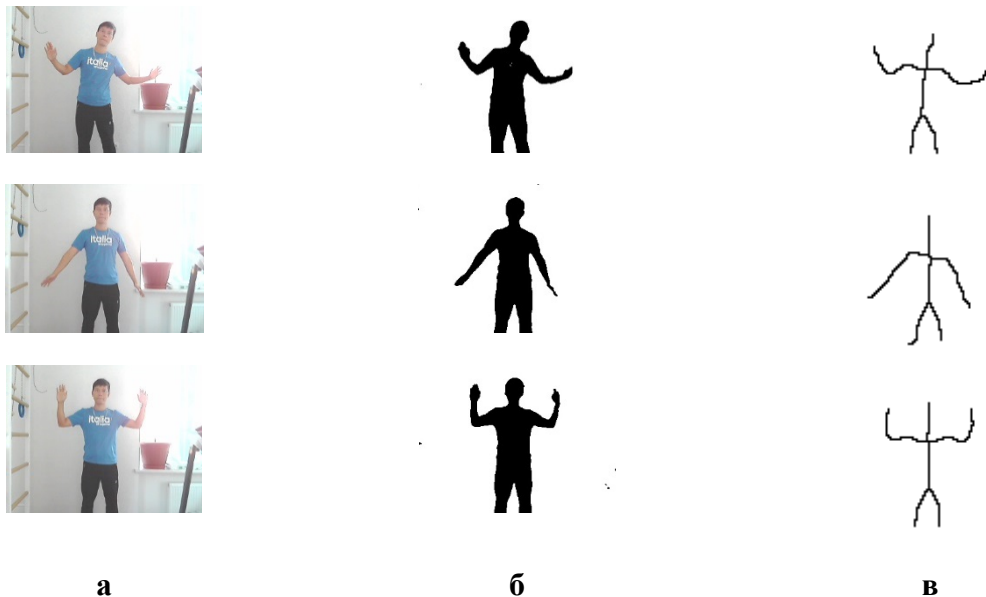


Рис.4. Пример предварительной внутрикадровой обработки изображения движений: а – исходное изображение; б – выделение бинаризованного изображения тела; в – результат скелетизации

Следующим этапом внутрикадровой обработки является выделение наблюдаемых в кадре ХТ тела. Конечные (тупиковые или вершинные) точки скелета определяются простым обходом всех ХТ. Алгоритмы скелетизации и выделения ХТ в реальном

масштабе времени достаточно подробно изложены в работах [5, 18]. В результате перечисленных операций получаются множества координат наблюдаемых ХТ модели.

Рассмотрим принцип построения системы двигательной реабилитации на основании предложенной модели. Инструктор выполняет правильные движения, регистрируемые видеокамерой в виде обучающего видеопотока. На основании пофрагментного анализа для каждого обязательного движения инструктора строится описанная выше матрица кинематических параметров движения, которую будем называть эталонной $M_{эт}$. Далее при том же ракурсе и на том же расстоянии от камеры на основании обучающей видеозаписи требуемые движения предлагается выполнить пользователю системы дистанционной тренировки. Постоянство ракурса и координат «камера-пользователь» легко достигаются путем разметки помещения. Синхронизация движения достигается подачей звукового стартового сигнала. Задача пользователя системы – повторить движения инструктора максимально точно – по амплитуде (координатам ХТ), темпу (их скорости) и резкости движений (ускорению ХТ). В процессе видеозаписи движений, повторяемых пользователем, по описанной модели строится матрица кинематических параметров движения пользователя $M_{польз}$. Матрицы $M_{эт}$ и $M_{польз}$ являются равноразмерными.

Основная цель системы – выдача конкретных рекомендаций пользователю по коррекции его неправильно выполняемых движений. Для этого необходимо количественно сравнить матрицы $M_{эт}$ и $M_{польз}$.

На этапе верификации и тестирования системы в качестве инструктора и пользователя выступало одно и то же лицо, заведомо выполнявшее неверные движения в роли пользователя. На рис.5 представлены на кадровые (прореженные для удобства восприятия наложенные кадры с изображением исходного положения тела, последовательных положений наблюдаемых ХТ, обозначенных белыми квадратами и сглаженных траекторий ХТ).



Рис.5. Кадровые кадры движений: а – правильного; б – неправильного

Результаты обработки видефрагмента, показанного на рис.5, представлены в таблице 2. Кинематические характеристики рассчитаны непосредственно в пиксельных координатных единицах.

Достаточно сложной задачей количественного сравнения двух движений является выбор метрики различия векторов модельной матрицы (1). Хотя задачи выбора метрик достаточно детально исследованы в задачах распознавания образов, в частности в кластерном анализе [19], в задаче коррекции движений к метрике предъявляются

особые требования: метрика должна быть достаточно чувствительной к различию векторов; с точки зрения задачи реального времени метрика должна обладать минимальной вычислительной сложностью; желательно, чтобы метрика была нормированной, т.е. приведенной к интервалу $[0,1]$; поскольку алгоритмы выделения ХТ и оценки кинематических параметров обладают вычислительными погрешностями, данные содержащиеся в векторах кинематических параметров являются зашумленными, поэтому выбранная метрика должна быть наименее чувствительной к шумам и не требовать дополнительного сглаживания векторов.

Таблица 2.

Количественные кинематические характеристики

Количественные кинематические характеристики	Кадрограмма 1			Кадрограмма 2		
	ХТ 3	ХТ 6	ХТ 9	ХТ 3	ХТ 6	ХТ 9
Максимальный радиус $R_j^{\max}$, пикс	17	42	61	12	40	58
Минимальный радиус $R_j^{\min}$, пикс	15	38	57	10	35	53
Максимальная скорость $v_{\tau}^{\max}$, пикс/с	148	372	561	142	365	528
Минимальная скорость $v_{\tau}^{\min}$, пикс/с	140	365	532	135	358	507
Максимальное ускорение $\varepsilon_{\tau}^{\max}$, пикс/с ²	6	10	18	6	9	17
Минимальное ускорение $\varepsilon_{\tau}^{\min}$, пикс/с ²	5	8	16	5	8	16

Для количественной оценки отличия двух матриц модели исследовались следующие метрики различия векторов $a_{j\text{эм}}^n$ и $b_{j\text{польз}}^n$ (в качестве $a_{j\text{эм}}^n$ и $b_{j\text{польз}}^n$ могут быть использованы вектор-столбцы модели (7) одноименной физической размерности $x_j^n, y_j^n, v_{\tau j}^n, a_{\tau j}^n$) [20]:

- метрика Хаусдорфа: $l_{\text{Haus}}^{ab} = \max \left(\max_i \min_j |a_{i\text{эм}}^n - b_{j\text{польз}}^n|, \max_j \min_i |a_{i\text{эм}}^n - b_{j\text{польз}}^n| \right)$,
- метрика Камберра: $l_{\text{Camb}}^{ab} = \sum_{j=1}^K \frac{|a_{j\text{эм}}^n - b_{j\text{польз}}^n|}{|a_{j\text{эм}}^n + b_{j\text{польз}}^n|}$,
- метрика Минковского: $l_{\text{Mink}}^{ab} = \left(\sum_{j=1}^K |a_{j\text{эм}}^n - b_{j\text{польз}}^n|^p \right)^{1/p}$ для $p = 3, 4, 5$,
- чебышевская мера (представляющая собой предельную меру Минковского для $p = \infty$): $l_{\infty}^{ab} = \max_{\substack{j=1, \dots, K \\ \text{для всех } n}} |a_{j\text{эм}}^n - b_{j\text{польз}}^n|$,
- косинусная мера: $l_{\cos}^{ab} = \frac{a_{j\text{эм}}^n \times b_{j\text{польз}}^n}{|a_{j\text{эм}}^n| \times |b_{j\text{польз}}^n|}$.

В результате исследования всех перечисленных метрик путем программной реализации и применения к экспериментально зарегистрированным кадрограммам установлены их характеристики, приведенные в таблице 3.

В результате исследования по перечисленным выше критериям в качестве методики предлагается следующая двухэтапная процедура. На первом этапе для координатных вектор-столбцов обеих матриц x_j^n, y_j^n находится чебышевская мера различия векторов: $l_{\infty}^x = \max_{\substack{j=1, \dots, K \\ \text{для всех } n}} |x_{j\text{эм}}^n - x_{j\text{польз}}^n|$, $l_{\infty}^y = \max_{\substack{j=1, \dots, K \\ \text{для всех } n}} |y_{j\text{эм}}^n - y_{j\text{польз}}^n|$.

Таблица 3.

Сравнение метрик близости векторов

Наименование метрики	Вычислительная сложность	Необходимость нормирования	Чувствительность к шумам
Хаусдорфа l_{Haus}^{ab}	Высокая	Требуется	Малочувствительна
Камберра l_{Camb}^{ab}	Низкая	Нормирована	Чувствительна
Минковского l_{Mink}^{ab}	Высокая	Требуется	Малочувствительна
Чебышевская l_{∞}^{ab}	Низкая	Требуется	Малочувствительна
Косинусная мера $l_{\cos}^{ab}$	Низкая	Нормирована	Малочувствительна

Если рассчитанные меры близости не превышают допустимых порогов отклонения $l_{\infty}^x \leq Thesh(l_{\infty}^x)$, $l_{\infty}^y \leq Thesh(l_{\infty}^y)$, где $Thesh(l_{\infty}^x)$ и $Thesh(l_{\infty}^y)$ – экспериментально установленные пороги, то движение считается повторенным правильно. При этом чебышевская мера нормируется к максимальному радиусу $R_j^{\max}$ для соответствующей ХТ j . Далее применяется нормированная чебышевская мера близости (НЧМБ). Чебышевская мера практически не требует вычислительных затрат по сравнению с остальными и вынесение решения на первом этапе происходит быстро. В случае невыполнения условий по чебышевскому отклонению быстро устанавливаются номера ХТ тела, координаты которых отличаются от требуемых. На основании первого этапа оценки пользователю выдаются рекомендации первого уровня по координатам движений (например, «правая рука – выше», «наклон головы вправо – ниже»).

На втором этапе для установленного множества ХТ с отклонениями по координатам N_{∞} рассчитывается косинусная мера близости по векторам скорости и ускорения. Напомним, что косинусная мера близости векторов есть отношение скалярного произведения векторов к произведению евклидовых норм этих векторов. Для совпадающих векторов угол между ними равен нулю и соответственно косинусная мера близости равна 1. Косинусные меры близости оцениваются по формулам:

$$l_{\cos}^v = \frac{v_{tj}^n \times v_{tj}^n \text{ польз}}{|v_{tj}^n| \times |v_{tj}^n \text{ польз}|}, \quad l_{\cos}^a = \frac{a_{tj}^n \times a_{tj}^n \text{ польз}}{|a_{tj}^n| \times |a_{tj}^n \text{ польз}|}.$$

для всех $n \in N_{\infty}$

На основании сравнения векторов скорости и ускорения «отклоняющихся точек» формируется второй уровень рекомендаций пользователю: если $1 - l_{\cos}^v \leq Thesh(l_{\cos}^v)$, $1 - l_{\cos}^a \leq Thesh(l_{\cos}^a)$, где $Thesh(l_{\cos}^v)$ и $Thesh(l_{\cos}^a)$ – экспериментально установленные пороги скорости и ускорения соответственно, то движение считается повторенным правильно. В противном случае выдаются рекомендации по коррекции движений пользователя по скорости (например, «правая рука – быстрее», «наклон головы вправо – медленнее») и по ускорению (например, «правая рука – резче», «наклон головы вправо – менее резко»).

Предварительные оценки, полученные в результате тестирования прототипа системы, показывают, что введенные выше пороги отклонения по координатам составляют 8-12% от максимального радиуса вращения, а по косинусной мере лежат в диапазоне абсолютных величин 0.09-0.11.

Пример расчетов по приведенной методике и вынесение решения по коррекции движений для того же видефрагмента приведены в таблицах 4 и 5 соответственно.

Таблиця 4.

Пример обработки видеофрагмента

Номер ХТ	ХТ 3	ХР 6	ХТ 9
НЧМБ по x l_{∞}^x	5/17=0.294	8/42=0.190	16/61=0.262
Порог $Thesh(l_{\infty}^x)$	0.12	0.12	0.12
НЧМБ по y l_{∞}^y	6/17=0.358	9/17=0.542	11/17=0.647
Порог $Thesh(l_{\infty}^y)$	0.12	0.12	0.12
$1-l_{\cos}^v$	1-0.911=0.089	1-0.812=0.188	1-0.678=0.322
Порог $Thesh(l_{\cos}^v)$	0.1	0.1	0.1
$1-l_{\cos}^a$	1-0.945=0.055	1-0.886=0.134	1-0.853=0.147
Порог $Thesh(l_{\cos}^a)$	0.1	0.1	0.1

Таблиця 5.

Пример вынесения решения по коррекции движений

Номер ХТ	Сравнение с порогами	Вынесение решения: корректирующая рекомендация
ХТ 3	$l_{\infty}^x > Thesh(l_{\infty}^x), l_{\infty}^y > Thesh(l_{\infty}^y)$	1 этап – «Голову влево, ниже»
	$1-l_{\cos}^v \leq Thesh(l_{\cos}^v)$ $1-l_{\cos}^a > Thesh(l_{\cos}^a)$	2 этап – По скорости движения головой замечаний нет «Движение головой резче»
ХТ 6	$l_{\infty}^x > Thesh(l_{\infty}^x), l_{\infty}^y > Thesh(l_{\infty}^y)$	1 этап – «Правый локоть правее, выше»
	$1-l_{\cos}^v > Thesh(l_{\cos}^v)$ $1-l_{\cos}^a > Thesh(l_{\cos}^a)$	2 этап – «Движение правым локтем быстрее» «Движение правым локтем резче»
ХТ 9	$l_{\infty}^x > Thesh(l_{\infty}^x), l_{\infty}^y > Thesh(l_{\infty}^y)$	1 этап – «Правая кисть правее, выше»
	$1-l_{\cos}^v > Thesh(l_{\cos}^v)$ $1-l_{\cos}^a > Thesh(l_{\cos}^a)$	2 этап – «Движение правой кистью быстрее» «Движение правой кистью резче»

Анализ полученных результатов показывает принципиальную правильность предложенной проективной модели и разработанной методики выработки корректирующих рекомендаций.

В качестве направления дальнейших исследований укажем следующее. Целесообразно сгруппировать ХТ для отдельных разделов тела человека (левые и правые верхние и нижние конечности, корпус, голова+шея) и выносить корректирующие рекомендации по отдельным разделам тела в целом. Другим направлением совершенствования системы является создание базы данных эталонных обучающих движений для упражнений разного типа, зафиксированных как во фронтальных, так и в профильных ракурсах.

Выводы

В результате классификации и анализа существующих моделей движения тела человека в видеопотоке установлено, что как объемные, так и проективные модели при детальном описании движения требуют вычислительных ресурсов высокой производительности. Упрощенные модели не позволяют достаточно точно описать движения частей тела. Предложена двумерная проективная модель движения тела человека, позволяющая оценить кинематические характеристики набора характерных точек. Предложенная модель ориентирована на применение в дистанционных системах двигательной реабилитации пациентов. Для доступности таких систем алгоритмическое и программное обеспечение рассчитано на обеспечение работы в реальном масштабе времени с бытовой веб-камерой на компьютере средней производительности. Программно реализован прототип системы двигательной реабилитации. Для выработки корректирующих рекомендаций пользователю системы разработана методика количественной оценки мер близости обучающего и пользовательского движений. Предварительное тестирование предложенной модели на уровне ее программной реализации подтвердило ее адекватность и соответствие поставленной задаче.

Список литературы

1. Pawlik, P. Visual Surveillance for Movement Rehabilitation / P. Pawlik, Z. Bublinski // *Image Processing & Communication*. – 2012. – Vol. 17, No. 4. – PP. 173-178.
2. Green, R.D. Video Analysis of Gait for Diagnosing Movement Disorders / R.D. Green, L.J. Guan, A. Burne // *Journal of Electronic Imaging*. – 2000. – Vol.9, No.1. – PP. 16-21.
3. Kannan, P. Development of Human Pose Models for Sports Dynamics Analysis using Video Image Processing Techniques / P. Kannan, R. Ramakrishnan // *International Journal of Sports Science and Engineering*. – 2012. – Vol. 6, No. 4. – PP. 232-238.
4. Вражнов, Д.А. Сравнительный анализ методов повышения устойчивости алгоритмов слежения на видео / Д.А. Вражнов, В.В. Николаев, А.В. Шаповалов // *Вестник Томского государственного университета*. – 2013. – № 4(25). – С. 23-31.
5. Нгуен, Г.К. Применение систем компьютерного зрения в задачах реабилитации пациентов с болезнями опорно-двигательного аппарата / Г.К. Нгуен // *Труды МНТК «Современные информационные и электронные технологии СИЭТ-2013»*. – Одесса, Политехпериодика. – 2013. – Т. 1. – С. 53-54.
6. Mikic, I. Human Body Model Acquisition and Tracking Using Voxel Data / I. Mikic, M. Trivedi, E. Hunter // *International Journal of Computer Vision*. – 2003. – Vol.53, No.3. – PP. 199-223.
7. Shingade, A. Animation of 3D human model using markerless motion capture applied to sports / A. Shingade, A. Ghotkar // *International Journal of Computer Graphics & Animation*. – 2014. – Vol. 4, No. 1. – PP. 27-39.
8. Chang, Y.J. A Kinect-based system for physical rehabilitation: A pilot study for young adults with motor disabilities [Text] / Y.J. Chang, S.F. Chen, J.D. Huang // *Research in Developmental Disabilities*. – 2011. – Vol. 32, No.6. – PP. 2566-2570.
9. Correa, P. Silhouette-based Probabilistic 2D Human Motion Estimation for Real-time Applications / P. Correa, J. Czyz, T. Umeda, F. Marques, X. Marichal, B. Macq // *IEEE International Conference on Image Processing*. – 2005. – Vol.3. – PP. 836-839.
10. Aggarwal, J.K. Human Motion analysis: A Review / J.K. Aggarwal, Q. Cai // *Proceedings of the IEEE Workshop on Motion on Non-Rigid and Articulated Objects*. – 1997. – PP. 90-102.
11. Muthukumar, B. Tracking the Human Motion in Real Time Using Star Skeleton Model / B. Muthukumar, S. Ravi // *International Journal of Engineering and Advanced Technology*. – 2012. – Vol.1, No. 3. – PP. 2249-2958.
12. Win Kong. Essential Human Body Tracking Using Kalman Filter / Win Kong, Aini Hussain, Mohd. Hanif Md Saad // *Proceedings of the World Congress on Engineering and Computer Science IWCECS 2013*. – 23-25 October, 2013, San Francisco, USA. – 2013. – Vol.1. – PP. 23-25.
13. Chang, I.C. Skeleton-based Walking Motion Analysis Using Hidden Markov Model and Active Shape Models/ I.C. Chang, C.L. Huang // *Journal of Information Science and Engineering*. – 2001. – Vol.17. – PP.371-403.

14. Потемкин, С. Восстановление пространственного спортивного движения по его двумерному образу // Труды Междисциплинарного научного семинара «Информатика и спорт». – М.: МГУ. –2010. – С. 132-135.
15. Bartlett, R. Introduction to Sports Biomechanics: Analysing Human Movement Patterns / R. Bartlett. – N.-Y., Routledge. – 2007. – 292 p.
16. Умнов, А.Е. Аналитическая геометрия и линейная алгебра / А.Е. Умнов. – М.: МФТИ, 2011. – 544 с.
17. Open CV: [Электронный ресурс] // Режим доступа: <http://opencv.org> (Дата обращения: 01.09.2014).
18. Болтенков, В.А. Сравнительный анализ алгоритмов скелетизации бинарных изображений / В.А. Болтенков, Д.В. Малявин, Нгуен Гуи Кiong // Труды МНТК «Современные информационные и электронные технологии СИЭТ-2014». – Одесса, Политехперіодика. – 2014. – Т.1. – С. 40-41.
19. Дуда, Р. Распознавание образов и анализ сцен / Р. Дуда, П. Харт. – М.: Мир, 1976. – 512 с.
20. Деза, Е. Энциклопедический словарь расстояний / Е. Деза, М.М. Деза. – М.: Наука, 2008. – 446 с.

ДВОВИМІРНА ПРОЕКТИВНА МОДЕЛЬ РУХУ ТІЛА ЛЮДИНИ ТА ЇЇ ЗАСТОСУВАННЯ В ЗАДАЧАХ ТЕЛЕМЕДИЦИНИ

В.О. Болтъонков, Нгуєн Гуї Кiong

Одеський національний політехнічний університет,
просп. Шевченко, 1, Одеса, 65044, Україна; e-mail: vaboltentkov@mail.ru

Запропоновано двовимірну проективну точкову модель руху тіла людини на підставі аналізу відеопотоку. Модель призначена для побудови системи дистанційної рухової реабілітації пацієнтів із захворюваннями опорно-рухового апарату. Перевірка адекватності моделі проведена на прототипі системи. Розроблено методику вироблення рекомендацій щодо коригування рухів пацієнта на основі мір близькості векторів.

Ключові слова: модель руху тіла людини, аналіз відеопотока, рухова реабілітація, кінематичні параметри, міри близькості векторів

TWO-DIMENSIONAL PROJECTIVE MODEL OF HUMAN BODY MOTIONS AND ITS APPLICATION IN TELEMEDICINE

V.O. Boltentkov, Nhuen Hui Kionh

Odessa National Polytechnical University,
1, Shevchenko ave., Odessa, 65044, Ukraine; e-mail: vaboltentkov@mail.ru

A two-dimensional projective point model of human body motions is proposed based on video stream analysis. The model was designed to develop a system for distant motor rehabilitation of patients with orthopedic injuries. A system prototype was used to test the model for adequacy. A methodology was developed to provide recommendations on corrections in the patient's motions based on vector proximity measures.

Keywords: model of human body motions, video stream analysis, motor rehabilitation, kinematic parameters, and vector proximity measures.

АНАЛІЗ ЗАХИСНИХ ХАРАКТЕРИСТИК СУЧАСНИХ ВИДІВ СКЛА В ШИРОКОМУ ДІАПАЗОНІ ЧАСТОТ ПО АКУСТИЧНОМУ КАНАЛУ ВИТОКУ

В.Б. Дудикевич, І.С. Собчук, П.І. Гаранюк, В.О. Ракобовчук, В.А. Дей

Національний університет «Львівська політехніка»,
вул. С. Бандери, 12, Львів-13, 79013, Україна; e-mail: garanyuk@gmail.com

Досліджено можливості використання захисних характеристик сучасних видів скла в широкому діапазоні частот від акустичних витоків. За допомогою рентгенофлуоресцентного методу проведено аналіз складу хімічних елементів і відповідних їм масових концентрацій з похибкою визначення 0.01% масової частки для скла Saint-Gobain Diamant 6мм та Guardian float Guard 6мм. Проведено аналіз оптичних характеристик сучасних захисних плівок методом спектрофотометрії.

Ключові слова: лазерні системи активної розвідки, скло, захисна плівка, рентгенофлуоресцентний метод, метод спектрофотометрії, оптичні характеристики, склад хімічних елементів скла.

Вступ

Проблема протидії зніманню інформації з використанням лазерного випромінювання залишається актуальною і в той же час однією з найменш вивчених в порівнянні з іншими менш «екзотичними» засобами промислового шпигунства.

Особлива привабливість лазерних систем обумовлена тим, що вони дозволяють знімання мовної інформації максимально безпечно, на відстані, опосередковано, уникаючи необхідності присутності в приміщеннях з метою розміщення там підслуховування, що завжди пов'язане з ризиком. Крім того, і виявлення працюючого лазерного мікрофона дуже складне, а в ряді випадків технічно нездійсненно.

Система SIPE LASER 3-DA SUPER виробництва США використовує в якості джерела випромінювання гелій-неоновий лазер. Наводка приладу на віконне скло здійснюється за допомогою телескопічного візира, а знімання мовної інформації з віконних рам з подвійними склом з гарною якістю забезпечується з відстані до 250 метрів. Лазерний пристрій HPO150 фірми HEWLETT PACKARD забезпечує реєстрацію розмов, що ведуться в приміщеннях, на дальності до 1000 м [1].

Забезпечення захисту мовної інформації від «лазерних мікрофонів» може здійснюватися засобами активного захисту у складі генератора шуму та вібровипромінювача, закріпленого на шибці вікна. Наявність такого вібровипромінювача на вікні розкриває факт застосування засобу захисту від «лазерного мікрофону», що може бути небажано. Таким чином, виникає потреба у приховуванні засобу захисту. Крім того, обмежена маса вібровипромінювача не дає змогу створювати достатню амплітуду коливань шибки на низьких частотах [2,3]. Тому розробка методів захисту від лазерних систем акустичної розвідки (ЛСАР) є актуальною в сфері захисту інформації.

Метою роботи є дослідження використання захисних характеристик сучасних видів скла в широкому діапазоні частот від інформаційних витоків.

Структура та характеристики захисних плівок

Класифікація захисних плівок за технологію виготовлення та прозорістю приведена на рис.1. Найбільш актуальними для цілей захисту інформації слід вважати металізовані та спатерні плівки, які здатні відбивати ближнє та середнє інфрачервоне випромінювання, що може бути застосовано для блокування зчитування вібрацій скла за допомогою лазерного променя. Сучасні системи лазерного зчитування працюють в діапазоні 750 - 840 нм [4].

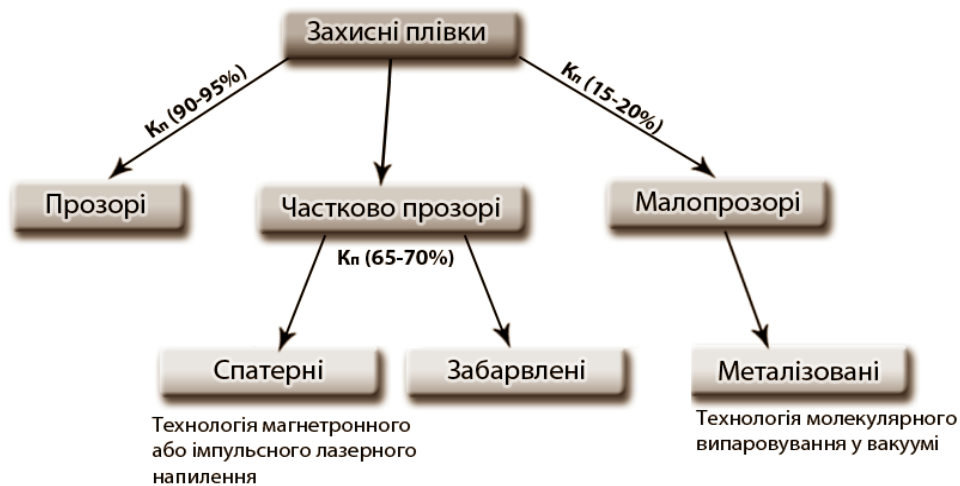


Рис.1. Класифікація захисних плівок за прозорістю та технологію виготовлення, K_p – коефіцієнт прозорості

Плівки «Signals Defenses» – це оптично прозорі, послаблюючі радіочастотні хвилі та інфрачервоне випромінювання віконні плівки. Застосування плівок на склі забезпечує приватність, захист даних та акустичної інформації. При необхідності вони можуть мати ударостійкі та вибухостійкі властивості.

З 2000 року плівки «Signals Defenses» застосовуються урядом США для послаблення радіочастотних сигналів та оптичного випромінювання інфрачервоного спектру з одночасно високим коефіцієнтом пропускання в діапазоні видимого світла і низьким коефіцієнтом відбивання. Це зменшує вплив пристроїв, які працюють в цих діапазонах, зокрема лазерних мікрофонів.

Оскільки плівки забезпечують високе послаблення радіочастотних сигналів та оптичного випромінювання інфрачервоного спектру, це дозволяє встановлювати вікна на об'єктах інформаційної безпеки. Вони встановлені більш як на 400 урядових об'єктах США. Міністерством оборони США було зазначено, що застосування плівки «Signals Defenses» – найдешевший спосіб зменшити велику кількість підслуховуючих та шпигунських засобів[5].

Плівка SD2500 відповідає високим вимогам, встановленим Агентством національної безпеки США, в той час як плівки SD1000 і SD2500 задовольняють вимоги, описані в директивах Розвідувального співтовариства та інші урядові організації США.

Варто зазначити, що плівки «Signals Defenses», за рахунок послаблення радіочастотних сигналів забезпечують захист від бездротових технологій передачі даних включно з Wireless LAN або 802.11, застосовуючи принцип «безпеки за рахунок відмови», а саме унеможлиблюючи проникнення радіочастотних хвиль в приміщення.

У табл.1 наведено дані випробувань з використання у сфері захисту інформації, які підтверджують високу ефективність деяких видів плівок для захисту приміщень від витоку інформації через вікна оптико-електронним каналом.

Таблиця 1.

Оптичні характеристики плівок

Плівка, (фірма, країна)	Назва плівки, марка	Діапазон випромінювання, нм	Кпроп, %	Котр, %	Кпогл, %	Оптична прозорість, %
Signals Defenses (ASTIC Signals Defenses, США) [9]	Signals Defenses, SD2500	800 -2500	<1			53
	SD1000		<3			70
LLumar (CPFilms, США) [10]	R 20 SR CDF	400 - 800	12	55	33	63
	R 15 GO SR HPR					60
Solar Gard (Solar Gard Corporate, США) [11]	4MIL Solar Bronze 175	800 -2500	9	50	41	18
	8MIL Silver 80		10	51	39	14
	4MIL Silver 80		11	52	37	17
	2MIL Clear		83	8	9	89
	8MIL Clear		82	9	9	89
	SD100		10			70

*4MIL – 100 мікрон, 84MIL – 200 мікрон

Для захисту скла від дії ЛСАР була випробувана плівка SMC 12, яка використовується для захисту вікон банківських структур та комерційних підприємств.

SMC 12 – це прозора плівка для захисту скла від руйнування. Вона складається з двох шарів прозорого поліестера. Крім того плівка містять антиподряпинний шар та інсталяційний клей. Інсталяційний клей являє собою стійкий до перепадів температури акриловий шар, що самоклеїться та містить УФ поглиначі і стабілізатори рис.2.

Експериментальні методи

Дослідження оптичних характеристик проводилося за допомогою спектрофотометра Shimadzu UV-3600.

Цей прилад призначений для проведення спектральних досліджень в надзвичайно широкій області спектра. Дозволяє проводити вимірювання поглинання, пропускання і віддзеркалення різних зразків в широкій області спектра, від 185 нм до 3300 нм.

Спектрофотометр компанії Shimadzu модель UV-3600 являє собою прилад, що працює в УФ, в інфрачервоному діапазоні ближнього і видимого спектра. Параметри вимірювальної системи володіють високим ступенем чутливості, малої похибкою вимірювань і мінімальним ступенем розкиду пучків світла[6].

Спектрофотометр укомплектований 3 детекторами: PMT детектор (ФЕУ) для ультрафіолетової і видимої області спектра, *InGaAs* і *PbS* детектори для ближньої ІЧ – області спектра. *InGaAs* автоматично починає працювати в тих областях спектра, в

яких чутливість детекторів PMT – *PbS* дуже низька, що дозволяє досягати вкрай низького рівня розсіяного світла.



Рис.2. Структура плівки SMC 12

Зручне програмне забезпечення UVProbe дає можливість працювати в режимах:

- спектральний – реєстрація поглинання, пропускання або відбиття, сканування по довжині хвилі з можливістю подальшої обробки спектра (визначення положення максимумів і мінімумів, арифметичні операції, розрахунок площі, згладжування, зворотні величини, логарифмування, похідна з 1 до 4 порядку);
- фотометричний (кількісний) – вимірювання на одній або декількох (до 3) обраних довжинах хвиль, побудова градувальної кривої методом К-фактора, однокрапковим або многоточечним;
- кінетичний – реєстрація зміни вимірюваної величини в часі;
- генератор звітів – вільне або за шаблоном розміщення матеріалу (спектри, таблиці, коментарі та ін.).

Всі режими вимірювання програмного забезпечення включають в себе різноманітну обробку отриманих даних і проведення математичних операцій. Поряд зі спектральним і фотометричним можливе вимірювання і в кінетичному режимі.

Елементарний аналіз скла було проведено на рентгенофлуоресценному аналізаторі елементарного складу «EXPERT 3L» [7]

Рентгенофлуоресцентний метод полягає в тому, що на зразок діє первинне рентгенівське випромінювання, під впливом якого виникає вторинне випромінювання зразка, характер якого залежить від якісного та кількісного складу аналізованої речовини. Універсальне градування, яке зберігається на весь період роботи приладу, дає можливість не тільки експлуатувати аналізатор без застосування стандартних зразків, але й без попереднього налаштування і калібрування виконувати багатоелементний якісний і кількісний аналіз зразків будь-якого (зокрема невідомого) складу і довільної форми.

Кожен разок був встановлений у вимірювальну камеру, ми запустили програму і через 40-600 с. отримати його спектр та склад хімічних елементів і відповідних їм масових концентрацій з похибкою визначення 0.01% масової частки.

Результати та їх обговорення

Для досліджень було вибрано найбільш популярні зразки скла ринку України, а саме Saint-Gobain Diamant 6мм [8] та Guardian float Guard 6мм [9].

Після встановлення кожного зразка у вимірювальну камеру рентгенофлуоресцентного аналізатора елементарного складу «EXPERT 3L» і запуску програми, через деякий час ми отримали спектр та склад хімічних елементів і відповідних їм масових концентрацій з похибкою визначення 0.01% масової частки, які можна переглянути в таблиці 2.

Таблиця 2.

Склад хімічних елементів і відповідних їм масових концентрацій скла Saint-Gobain та Guardian

Saint-Gobain 6		Guardian 6	
Елемент	Мас. доля, %	Елемент	Мас. доля, %
14Si	55.248±0.257	14Si	57.349±0.280
20Ca	41.427±0.198	20Ca	37.108±0.185
11Na	2.251±0.428	11Na	2.378±0.400
16S	0.372±0.043	12Mg	2.093±0.226
22Ti	0.101±0.017	16S	0.321±0.044
26Fe	0.476±0.007	22Ti	0.085±0.017
30Zn	0.004±0.001	26Fe	0.482±0.007
33As	0.003±0.001	28Ni	0.004±0.001
38Sr	0.066±0.001	37Rb	0.004±0.001
40Zr	0.027±0.001	38Sr	0.057±0.001
50Sn	0.024±0.003	39Y	0.004±0.001
		40Zr	0.019±0.001
		41Nb	0.005±0.001
		47Ag	0.007±0.002
		50Sn	0.022±0.003
		51Sb	0.023±0.004
		53I	0.039±0.008

При аналізі зразків на домішки, було виявлено, що вміст таких елементів, як Mg, Na, S, Fe, Ti у зразках скла Saint-Gobain та Guardian перевищує 0.1%. (Рис 3).

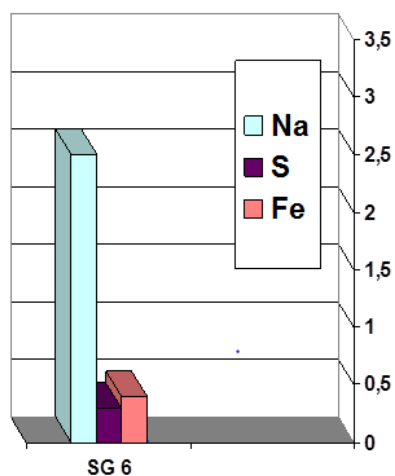
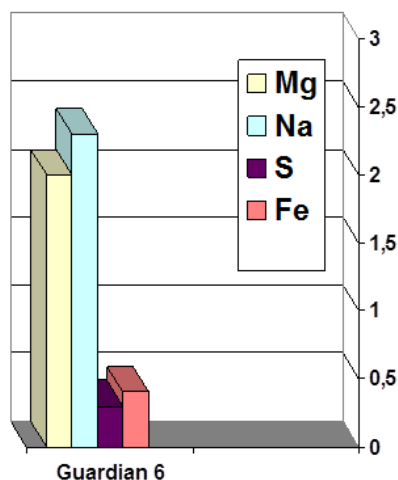
**а****б**

Рис.3. Вміст домішок в склі: а – виробника Saint-Gobain, кількість яких є більшою за 0.1%; б – виробника Guardian, кількість яких є більшою за 0.1%

Як видно з рис. 3, основний вміст домішок складає Na, S, Fe.

Saint-Gobain: Na – 2.251%, S – 0.372%, Fe – 0.476%.

Guardian: Na – 2.378%, S – 0.321%, Fe – 0.482%.

Такий вміст домішок в обох зразках майже однаковий. Відповідно на захисні характеристики може впливати компонент, який присутній в конкретному зразку. При порівнянні даних табл. 2 видно, що в склад скла Guardian входить ще досить велика кількість Mg – 2.093%. Очевидно, що цей елемент має вплив на поведінку зразків при дії випромінювання.

Спектральні характеристики зразків скла подані на рис.4 та рис.5.

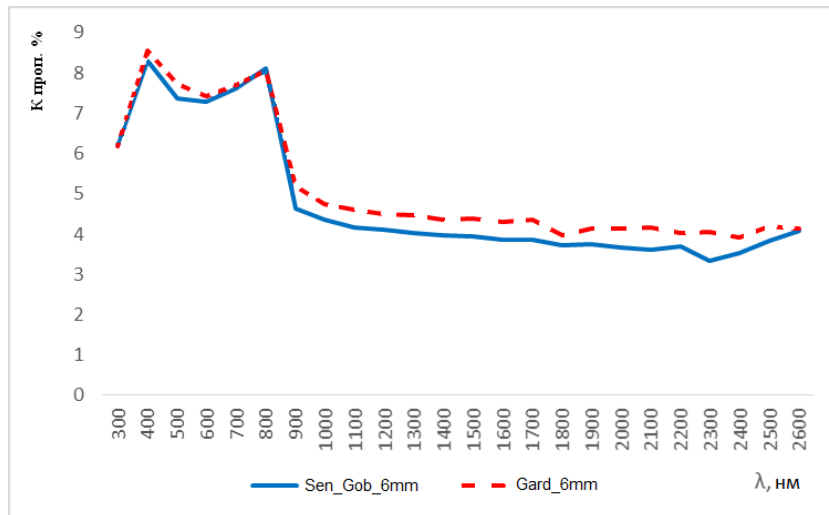


Рис.4. Коефіцієнти відбивання зразків скла в діапазоні частот від 300 до 2600 нм

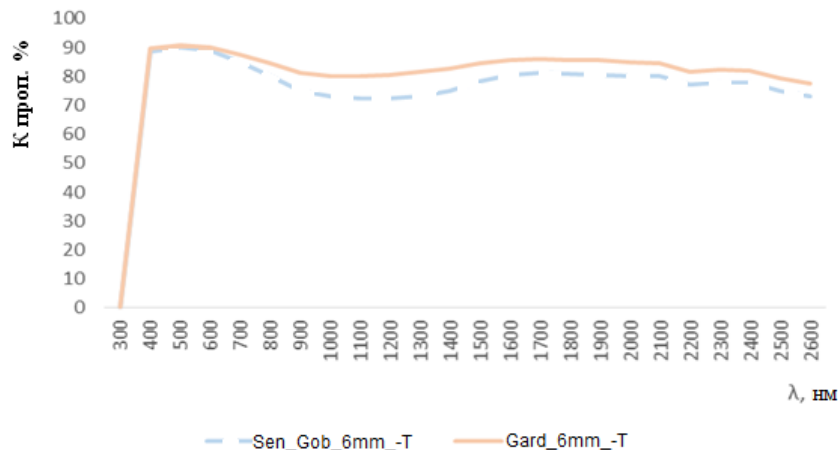


Рис.5. Коефіцієнти пропускання зразків скла в діапазоні частот від 300 до 2600 нм

Як видно, скло Guardian має інші характеристики за коефіцієнтом відбивання в діапазоні частот від 900 до 2500 нм. Тобто можна говорити, що Mg впливає на результативність захищеності в діапазоні від 900 до 2500 нм на 0.5% при його долі в склі 2.093%. Можна зауважити, що цей вплив не значний. Це підтвердило вимірювання коефіцієнтів заломлення зразків скла, що складає $n = 1.52 - 1.53$.

Для скла Guardian коефіцієнт пропускання перевищує коефіцієнт пропускання скла Saint-Gobain на 1 % в діапазоні частот 660-2600 нм. (див. рис.5)

Також проведено дослідження оптичних характеристик плівки SMC 12.

В діапазоні частот 300 до 1800 нм плівка не покращує характеристики скла Guardian, а навіть трохи погіршує рис.6.

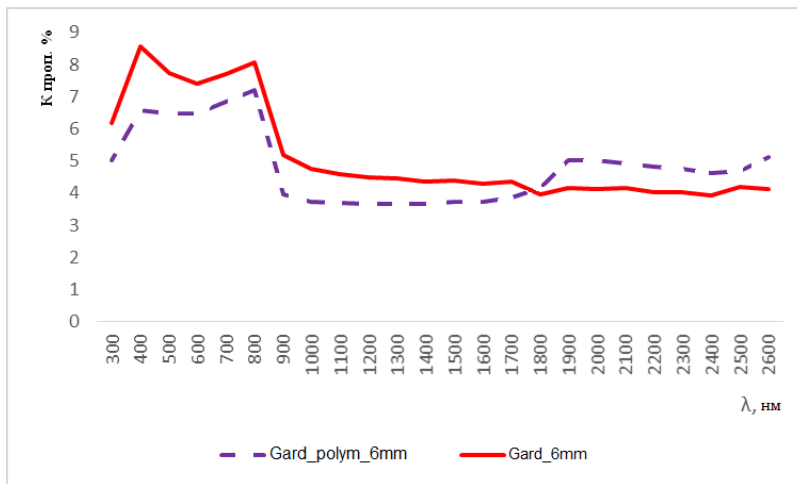


Рис.6. Результати вимірювання коефіцієнта відбивання Guardian із плівкою SMC 12

Висновки

Флуоресцентний аналіз показав, що вміст домішок в обох зразках майже однаковий: Saint-Gobain: Na – 2.251%, S – 0.372%, Fe – 0.476%; Guardian: Na – 2.378%, S – 0.321%, Fe – 0.482%. Відмінність цих зразків - наявність в складі скла Guardian елемента Mg, який очевидно впливає на захисні характеристики самого скла.

Спектральний аналіз показав, що скло Guardian має трохи кращі характеристики за коефіцієнтом відбивання в діапазоні частот від 900 до 2500 нм, проте його коефіцієнт пропускання перевищує коефіцієнт пропускання скла Saint-Gobain на 1 % в діапазоні частот 660-2600 нм. Тобто можна говорити, що Mg покращує результативність захищеності в діапазоні від 900 до 2500 нм на 0.5% при його долі в склі 2.093%. Зауважимо, що цей вплив не значний. Це підтвердило вимірювання коефіцієнтів заломлення зразків скла, що складає $n = 1.52 - 1.53$.

Для захисту скла від дії ЛСАР була випробувана плівка SMC 12. Оскільки сучасні лазерні системи працюють в діапазоні 700-1800 нм, то використання плівки не покращує характеристики скла Guardian, а навіть трохи погіршує в діапазоні частот від 300 до 1800 нм.

Поєднання методів визначення відсоткового складу скла та спектроскопії доцільно використовувати при тестуванні захисних плівок та склопакетів, що використовується в приміщеннях де функціонує інформація з обмеженим доступом.

Список літератури

1. Украинский ресурс по безопасности [Електронний ресурс] / Режим доступу: <http://www.kiev-security.org.ua> (Дата звернення 14.11.2014р.).
2. Дослідження каналу витоку мовної інформації у випадку використання «лазерних мікрофонів»: тези доп. XI Міжнародної науково-практичної конференції «Безпека

- інформації в інформаційно-телекомунікаційних системах» (20-23 травня 2008 р.). – Київ: Державна служба спеціального зв'язку й захисту інформації України, 2008. – 55 с.
3. Хореев, А.А. Способы и средства защиты информации: учеб. пособие / А.А. Хореев. – М.: МО РФ, 2000. – 316 с.
 4. Специальные технические средства негласного получения акустической (речевой) информации. [Електронний ресурс] / Режим доступу: <http://phreaking.ru/printpage.php?s=&pageid=54213> (Дата звернення 14.11.2014р.).
 5. Signal Defense full spectrum security solution [Електронний ресурс] / Режим доступу: <http://www.signalsdefense.com/security-solutions-products.cfm> (Дата звернення 14.11.2014р.).
 6. Спектрофотометр UV-3600, двухлучевой, 185-3300 нм, Shimadzu. [Електронний ресурс] / Режим доступу: <http://www.xn--80ahmr8f.xn--p1ai/lab/spektrofotometry/corningpyrex-uv-3600-spektrofotometr-uv-3600-dvuhluchovoj-185-3300-nm>. (Дата звернення 14.11.2014р.).
 7. Мультиэлементный экспресс-анализатор состава сплавов "EXPERT 3L". [Електронний ресурс] / Режим доступу: <http://www.inam.kiev.ua/Expert3L.html> (Дата звернення 14.11.2014р.).
 8. A building products library for customers industry professionals [Електронний ресурс] / Режим доступу: <http://www.ribaproductselector.com/Product.aspx?ci=20953&pr=saintgobainglassuk-SGGDiamant> (Дата звернення 14.11.2014р.).
 9. Guardian Glass, Automobile, Bilding Products [Електронний ресурс] / Режим доступу: <http://www.gulfguard.com/Products/ClearFloatGlass/> (Дата звернення 14.11.2014р.).

АНАЛИЗ ЗАЩИТНЫХ ХАРАКТЕРИСТИК СОВРЕМЕННЫХ ВИДОВ СТЕКЛА В ШИРОКОМ ДИАПАЗОНЕ ЧАСТОТ ПО АКУСТИЧЕСКОМУ КАНАЛУ УТЕЧКИ

В.Б. Дудикевич, И.С. Собчук, П.И. Гаранюк, В.А. Ракобовчук, В.А. Дей

Национальный университет «Львовская политехника»,
ул. С. Бандеры, 12, Львов 13, 79013, Украина; e-mail: garanyuk@gmail.com

Исследованы возможности использования защитных характеристик современных видов стекла в широком диапазоне частот от акустических утечек. При помощи рентгенофлуоресцентного метода проведен анализ состава химических элементов и соответствующих им массовых концентраций с погрешностью определения 0,01% массовой части для стекла Saint-Gobain Diamant 6мм и Guardian float Guard 6мм. Проведен анализ оптических характеристик современных защитных пленок методом спектрофотометрии.

Ключевые слова: лазерные системы активной разведки, стекло, защитная пленка, рентгенофлуоресцентный метод, метод спектрофотометрии, оптические характеристики, химический состав элементов стекла.

WIDE-BAND ANALYSIS OF PROTECTIVE PERFORMANCE OF MODERN GLASS TYPES WITH REGARD TO ACOUSTIC LEAKAGE PATHS

V.B. Dudykevich, I.S. Sobchuk, P.I. Haranyuk, V.O. Rakobovchuk, V.A. Dej

National University «Lviv Polytechnika»,
12 S.Bandera str., Lviv -13, 79013, Ukraine; e-mail: garanyuk@gmail.com

The potential of utilizing protective performance of modern glass types over a wide frequency band with regard to acoustic leakage was investigated. Two types of glass, 6-mm Saint-Gobain Diamant and 6-mm Guardian float Guard, were subjected to X-ray fluorescence analysis of chemical composition and related mass concentration analysis. Additionally, spectrophotometric analysis of optic characteristics of modern protective films was performed.

Keywords: active laser investigation systems, glass, protective film, X-ray fluorescence analysis, spectrophotometric analysis, optic characteristics, chemical glass composition.

МЕТОДИКА КОЛИЧЕСТВЕННОЙ ОЦЕНКИ НАДЕЖНОСТИ ВОСПРИЯТИЯ ЦИФРОВОГО ИЗОБРАЖЕНИЯ

Е.В. Нариманова, Е.А. Трифонова, А.Е. Килин, М.С. Кучма

Одесский национальный политехнический университет,
пр-т Шевченко, 1, Одесса, 65044, Украина; e-mail: semejka@ua.fm

Работа посвящена исследованию и разработке методики количественной оценки надежности восприятия цифрового изображения при различных возмущающих воздействиях, в том числе при локальном возмущении цифрового изображения, при помощи пикового отношения «сигнал/шум». Приведены результаты вычислительного эксперимента, подтверждающие эффективность предложенной методики, корреляцию результатов, полученных с ее помощью, с результатами субъективного ранжирования.

Ключевые слова: цифровое изображение, оценка надежности восприятия, пиковое отношение сигнал/шум.

Введение

В процессе формирования и передачи стеганографического сообщения требуется оценивать качество получаемого цифрового изображения (ЦИ). При его передаче по каналам связи возможно наложение различных шумов или нанесение локальных изменений. Алгоритмы сжатия с потерями при значительной степени сжатия, как правило, приводят к появлению хорошо заметных человеческому глазу артефактов на ЦИ. Все это порождает необходимость оценки качества цифрового изображения.

На данный момент наиболее распространенной количественной оценкой качества цифрового изображения при анализе уровня его визуальных искажений являются разностные показатели, основывающиеся на различных модификациях отношения «сигнал/шум», в том числе пиковое отношение «сигнал/шум» (peak signal-to-noise ratio – *PSNR*) [1]. Однако, как не раз было отмечено [2], эти показатели слабо коррелируют с субъективными оценками системы человеческого зрения, оценивая ЦИ целиком, что при передаче стеганографического сообщения может привести к противоречию между приемлемой количественной и неприемлемой качественной оценками надежности восприятия изображения, которое имеет явные визуальные искажения, хорошо заметные невооруженным глазом. Чрезвычайно важным здесь является то, что, как правило, такие визуальные искажения носят локальный характер.

Устоявшимся при оценке надежности восприятия ЦИ в стеганографии [1] рекомендованным пороговым значением *PSNR* является значение 40 дБ: значения *PSNR* равное 40 дБ и выше указывают на высокое качество ЦИ. Однако, как показывают многочисленные вычислительные эксперименты [1,2], такой способ количественной оценки искажения, рассматривающий изображение целиком, не является, в общем случае, удовлетворительным для стеганографии.

Цель и задачи исследования

Целью данной работы является разработка методики количественной оценки надежности восприятия ЦИ в результате возмущающих воздействий при помощи пикового отношения «сигнал/шум».

Для достижения цели в работе необходимо:

1. провести искажение ЦИ или его части таким образом, чтобы на основании экспертного оценивания разделить изображения после возмущающего воздействия на разные группы: с сохранением надежности восприятия; с частичным и полным нарушением надежности восприятия;
2. провести вычислительный эксперимент, в котором: разбить ЦИ на непересекающиеся части и провести оценку надежности восприятия по значениям $PSNR$ для каждой из частей ЦИ в сравнении с $PSNR$ для всего изображения.

Изложение основного материала

В данной работе в качестве относительной количественной оценки надежности восприятия ЦИ рассматривается $PSNR$:

$$PSNR = 10 \log_{10} \left(\frac{MAX_I^2}{MSE} \right) = 20 \log_{10} \left(\frac{MAX_I}{\sqrt{MSE}} \right),$$

где MAX_I – это максимальное значение, принимаемое пикселем изображения. Когда пиксели имеют разрядность 8 бит, $MAX_I = 255$; MSE – среднеквадратическая ошибка:

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} |I(i, j) - K(i, j)|^2,$$

где $I(i, j)$ – пиксель с координатами (i, j) исходного изображения; $K(i, j)$ – пиксель с координатами (i, j) измененного изображения, надежность восприятия которого необходимо оценить.

Основным недостатком $PSNR$ для оценки надежности восприятия ЦИ является то, что $PSNR$ мало чувствителен к локальным изменениям изображения. С учетом этого в работе предлагается методика, основные шаги которой следующие:

1. Разбить ЦИ на непересекающиеся части – так называемые подблоки сигнала (ПБС), размер которых сравним с размером 128×128 пикселей, что необходимо для сохранения представительности и информативности блока [3–5];
2. Определить $PSNR$ для каждого ПБС;
3. Количественной оценкой надежности восприятия ЦИ является минимальное значение $PSNR$ среди всех ПБС, поскольку нарушение в любой части изображения является нарушением надежности восприятия всего ЦИ.

В данной работе при проведении вычислительного эксперимента ЦИ разбивалось на 4 ПБС, минимальное значение $PSNR$ среди этих блоков обозначено $PSNR4$.

Результаты вычислительного эксперимента

При проведении вычислительного эксперимента $PSNR$ и $PSNR4$ вычислялись для более чем 100 цветных ЦИ и изображений в градациях серого. На каждую из этих

групп изображений накладывался мультипликативный, гауссовский и пуассоновский шумы. При использовании шумов в качестве возмущающего воздействия на каждое ЦИ или его часть накладывался шум разной интенсивности таким образом, что при помощи экспертного оценивания ЦИ качественно можно было отнести к одной из трех групп: I – «искажения видны хорошо на всем изображении» (рис. 1,б), II – «искажения видны на некоторых частях изображения» (рис. 2,б), III – «искажения не визуализируются» (рис. 3).



а

б

Рис. 1. Изображение I группы качественной оценки: оригинальное изображение (а); измененное изображение (б)



а

б

Рис. 2. Изображение II группы качественной оценки: оригинальное изображение (а); измененное изображение (б)



а

б

Рис. 3. Изображение III группы качественной оценки: оригинальное изображение (а); измененное изображение (б)

При проведении эксперимент для каждой группы качественной оценки фиксировались значения $PSNR$ и $PSNR4$.

Наиболее характерные результаты вычислительного эксперимента приведены в табл. 1. Особый интерес представляют результаты для изображений II группы качественной оценки (в таблице выделено полужирным шрифтом), поскольку разница между значениями $PSNR$ и $PSNR4$ для них больше, чем для изображений других групп. При этом значения $PSNR$ близки к 40 дБ, что является приемлемой количественной оценкой надежности восприятия ЦИ, в то время как значения $PSNR4$ свидетельствуют о нарушении надежности восприятия, что действительно соответствует ЦИ II группы.

Таблица 1.

Результаты оценки надежности восприятия ЦИ при наложении различных шумов

Изображение	$PSNR$	$PSNR4$	Группа качественной оценки визуального восприятия
Гауссовский шум			
В градациях серого	20	19.89	I
	38.2	33.89	II
	39.93	39.87	III
Цветное	20.04	19.76	I
	37.87	28.18	II
	40.07	39.56	III
Мультипликативный шум			
В градациях серого	18.36	18.25	I
	37.02	34.63	II
	43.12	42.92	III
Цветное	19.2	18.98	I
	36.65	33.16	II
	40.87	40.81	III
Пуассоновский шум			
В градациях серого	26.95	23.17	II
Цветное	25.03	22.28	II

Выводы

В работе предложена методика количественной оценки искажений ЦИ, учитывающая возможность их локализации в пределах изображения.

Результаты вычислительного эксперимента показывают, что оценивание надежности восприятия изображения при помощи пикового отношения «сигнал/шум» дает схожие результаты с экспертным оцениванием и может считаться объективным только в том случае, когда возмущение оказывает сравнимые по величине воздействия на все части изображения. При этом рекомендованное в литературе [1] и широко используемое пороговое значение 40 дБ является приемлемым. Все значения $PSNR$ и $PSNR4$ для изображений III группы качественной оценки визуального восприятия оказались близкими (более 39 дБ) или большими 40 дБ.

При выявлении локальных нарушений визуальной устойчивости оценка $PSNR$ оказывается близкой к 40 дБ, в отличие от $PSNR4$ (как видно по результатам для II группы, где наложение шума проводилось и заметно на некоторых частях изображения). В этом случае $PSNR$ и $PSNR4$ отличаются значительно, и в то время как оценка по $PSNR$ свидетельствует скорее о сохранении надежности восприятия,

оценка по $PSNR_4$ и группа качественной оценки визуального восприятия, к которой относятся изображения, указывают на то, что надежность восприятия нарушена.

В связи с этим, при наличии локальных нарушений визуальной устойчивости рекомендуется оценивать отдельные части цифрового изображения, которые их содержат. Такое оценивание цифрового сигнала по частям уже дало хороший результат и активно применяется для выявления областей нарушения целостности малых размеров в различных цифровых сигналах независимо от методов исследования [3–5].

Список литературы

1. Конахович, Г.Ф. Компьютерная стеганография [Текст]: теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. – К.: МК-Пресс, 2006. – 288 с
2. Кобозева, А.А. Учет свойств нормального спектрального разложения матрицы контейнера при обеспечении надежности восприятия стегосообщения / А.А. Кобозева, Е.А. Трифонова // Вестник НТУ «ХПИ». – 2007. – №18. – С.81-93.
3. Нариманова, Е.В. Практическое использование DQ-эффекта для построения универсального метода обнаружения фальсификации ЦС / Е.В. Нариманова // Вісник Східноукр-го нац-го ун-ту ім. В.Даля. – 2010. – С.80-85.
4. Нариманова, Е.В. Проверка целостности цифрового сигнала. – Донецк: Изд. Цифровая типография, 2011. – 180 с.
5. Нариманова, Е.В. Обнаружение области нарушения целостности малого размера в цифровом изображении / Е.В. Нариманова, С.И. Ботнарь // Сучасний захист інформації. – 2013. – Спеціальний випуск. – С.43-48.

МЕТОДИКА КІЛЬКІСНОЇ ОЦІНКИ НАДІЙНОСТІ СПРИЙНЯТТЯ ЦИФРОВОГО ЗОБРАЖЕННЯ

О.В. Наріманова, К.О. Трифонова, А.Є. Кілін, М.С. Кучма

Одеський національний політехнічний університет,
пр-т Шевченка, 1, Одеса, 65044, Україна; e-mail: semejka@ua.fm

Работа посвящена дослідженню і розробці методики кількісної оцінки надійності сприйняття цифрового зображення при різних збурних діях, в тому числі при локальному збуренні цифрового зображення, за допомогою пікового відношення «сигнал/шум». Наведені результати обчислювального експерименту, що підтверджують ефективність запропонованої методики, кореляцію результатів, отриманих з її допомогою, з результатами суб'єктивного ранжування.

Ключові слова: цифрове зображення, оцінка надійності сприйняття, пікове відношення сигнал/шум.

TECHNIQUE OF QUANTITATIVE ASSESSMENT OF DIGITAL IMAGE PERCEPTION RELIABILITY

O.V. Narimanova, K.O. Tryfonova, A.Ye Kilin, M.S. Kuchma

Odesa National Polytechnic University,
1 Shevchenko Ave., Odesa, 65044, Ukraine; e-mail: semejka@ua.fm

Work is devoted to study and development of technique of quantitative assessment of digital image perception reliability at various disturbing effects, including the local perturbation of the digital image, using the peak signal/noise ratio. The results of computational experiments that confirm the effectiveness of proposed technique, the correlation of obtained results with the results of subjective rankings are shown.

Keywords: digital image, assessment of perception reliability, peak signal/noise ratio.

МОДЕЛЬ ПРОЯВЛЕНИЯ И ВЫЯВЛЕНИЯ ВЛИЯНИЯ НЕМОНОТОННОСТИ СТАТИЧЕСКОЙ ХАРАКТЕРИСТИКИ КВАНТОВАТЕЛЯ УРОВНЯ В ВЫХОДНОМ СИГНАЛЕ СИСТЕМЫ АНАЛОГО-ЦИФРО- АНАЛОГОВОГО ПРЕОБРАЗОВАНИЯ

О.В. Рыбальский, В.И. Соловьев

Национальная академия внутренних дел,
пл. Соломенская, 1, Киев, 03035, Украина; e-mail: rybalsky_ol@mail.ru

Предложена модель описания проявления технологических погрешностей квантователя уровня аналогового сигнала на выходе системы аналого-цифро-аналогового преобразования. Показано, что такие проявления могут быть выявлены применением вейвлет-анализа при использовании вейвлета Морле. Показано, что эти проявления носят фрактальный характер. Предложено выявлять их статистические характеристики путем применения известных методов математической статистики.

Ключевые слова: аналого-цифровое преобразование, квантование по уровню, статическая характеристика квантования, немонотонность, нелинейность статической характеристики.

Введение

Широкое использование цифровой аппаратуры звукозаписи привело к началу первых попыток создания инструментария для проведения экспертиз цифровой аппаратуры и материалов видеозвукозаписи. Была создана теория, ставшая основой разработки такого инструментария, и разработаны первые программы и методики, предназначенные для проведения такой экспертизы. Впервые реализация этого инструментария была осуществлена с применением вейвлет-анализа сигналов, что позволило экспертам исследовать паразитные параметры цифровой аппаратуры звукозаписи (ЦАЗЗ) [1–3]. Однако они не удовлетворяли все требования экспертов, что привело к дальнейшей разработке созданного направления использования паразитных параметров ЦАЗЗ. Это потребовало развития теоретической базы, положенной в основу разработки экспертного инструментария. Одной из задач развития теории применения паразитных параметров ЦАЗЗ для экспертных целей была теоретическое осознание процессов проявления и выявления влияния немонотонности статической характеристики квантователя уровня в выходном сигнале системы аналого-цифро-аналогового преобразования. Решению этой задачи и посвящена данная работа.

Основная часть

Известно, что для записи аналогового сигнала (АС) в цифровой форме его необходимо подвергнуть двум операциям – дискретизации во времени и квантованию по уровню [4]. Представим АС на входе аналого-цифрового преобразователя (АЦП) как

$s_1(t) = A_{m1} \cos \omega_0 t$. Этот сигнал на выходе цифро-аналогового преобразователя записывается как

$$s_2(t) = \sum_{n_1=-\infty}^{\infty} \text{rect}\left(\frac{t-n_1 T_1}{T_1}\right) A_{m1} \cos \omega_0(n_1 T_1), \quad (1)$$

где n_1 – номер отсчета (выборки) сигнала на выходе системы аналого-цифро-аналогового преобразования (САЦАП),

T_1 – шаг дискретизации АС в САЦАП,

A_{m1} – амплитуда входного АС [1, 2].

Соотношение (1) описывает сигнал на выходе идеальной САЦАП в виде выборок АС. Спектр сигнала $S_3(j\omega) = \frac{A_{m1}\omega_{Д1}}{\omega} \sin \omega \frac{T_1}{2} \sum_{k_1=-\infty}^{\infty} [\delta(\omega - \omega_0 - k_1\omega_{Д1}) + \delta(\omega + \omega_0 - k_1\omega_{Д1})]$, где

$\omega_{Д1}$ – ЧД в САЦАП, $\omega_{Д1} = \frac{2\pi}{T_1}$ [1, 2].

Также известно, что в общем виде сигнал выборки на выходе квантователя уровня (КУ) записывается как $U = \sum_{i=0}^{2N-1} a_i 2^i U_{0no}$, где a_i – весовые коэффициенты, определяемые соответствующими разрядами двоичного кода, в который преобразован уровень выборки входного АС, i – номер разряда двоичного кода, U_{0no} – уровень младшего разряда преобразования, $2N$ – количество уровней квантования преобразователя [4].

Статическая характеристика (СХ) преобразования АС, соответствующая соотношению (1), показана на рис. 1.

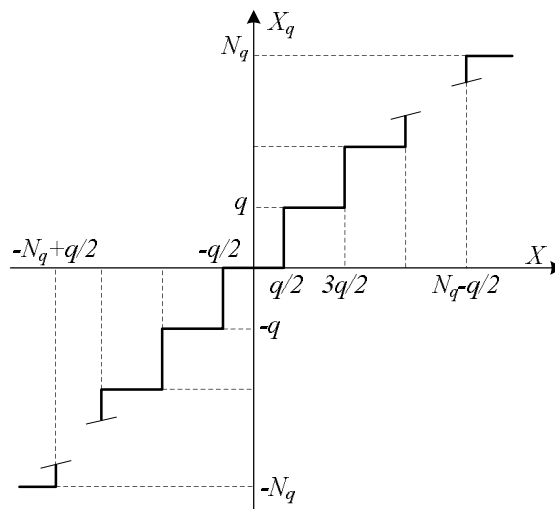


Рис. 1. Статическая характеристика идеального двуполярного квантователя по уровню

Но, как показано в [2, 3], СХ КУ обладает нелинейностью, определяемой несоответствием направления приращения уровня сигнала на определенном такте квантования. В [3] показано, что обычно величина образующегося при этом выброса не превышает значения удвоенной величины уровня младшего разряда, а вероятность совпадения таких мест для двух независимых АЦП определяется как $P = \frac{1}{2^{2i}}$.

Таким образом, для двух 16-разрядных АЦП вероятность совпадения двух мест с немонотонностью СХ (НСХ) преобразования составит $P = 2^{-32}$.

Если входной АС подавался на вход КУ с имеющейся в нем НСХ (а АЦП без НСХ не бывает [5]), то он может рассматриваться с точки зрения принципа «суперпозиции» для безинерционной нелинейной системы, а сигнал на выходе КУ можно записать в виде

$$y(t) = y_1(t) + y_2(t) = \sum_{i=0}^l a_i 2^i U_{0on} + \sum_{i=l+1}^{2N-1} a_i 2^i U_{0on} = a_{l+1} 2^{l+1} U_{0on} + \sum_{i=0}^l a_i 2^i U_{0on} + \sum_{i=l+2}^{2N-1} a_i 2^i U_{0on}, \quad (2)$$

где $y_1(t)$ – отклик системы на воздействие, действующее на участке шкалы, в пределах которого в СХ КУ отсутствует НСХ,

$y_2(t)$ – отклик системы на воздействие, действующее на участке шкалы, в пределах которого в СХ КУ имеется НСХ,

l – номер интервала квантования, до которого НСХ в СХ КУ отсутствует,

$l+1$ – последующий за l номер интервала квантования, на котором в СХ КУ имеется НСХ,

$l+2$ – последующий за $l+1$ номер интервала квантования, на котором отсутствует НСХ в СХ КУ [3].

Соотношение (2) можно проиллюстрировать рис. 2.

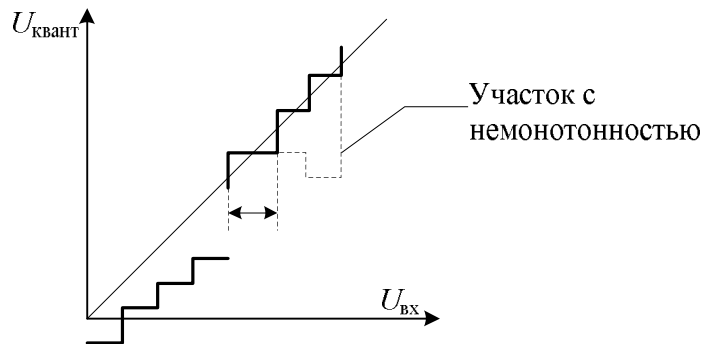


Рис. 2. Фрагмент статической характеристики квантователя уровня, содержащий немонотонность и дифференциальную нелинейность

Для рассмотрения влияния НСХ на выходной сигнал САЦАП вместо значения величины амплитуды сигнала A_{m1} в соотношении (1) подставим соотношение (2). В результате проведенной подстановки получим

$$\begin{aligned} s_2(t) &= \sum_{n_1=-\infty}^{\infty} \text{rect}\left(\frac{t-n_1T_1}{T_1}\right) \left(\sum_{i=0}^l a_i 2^i U_{0on} + \sum_{i=l+1}^{2N-1} a_i 2^i U_{0on} \right) \cos \omega_0(n_1T_1) = \\ &= \sum_{n_1=-\infty}^{\infty} \text{rect}\left(\frac{t-n_1T_1}{T_1}\right) \left(a_{l+1} 2^{l+1} U_{0on} + \sum_{i=0}^l a_i 2^i U_{0on} + \sum_{i=l+2}^{2N-1} a_i 2^i U_{0on} \right) \cos \omega_0(n_1T_1). \end{aligned} \quad (3)$$

Соответственно, спектр этого сигнала запишется как

$$S_2(j\omega) = \frac{\sum_{n_1=-\infty}^{\infty} \text{rect}\left(\frac{t-n_1T_1}{T_1}\right)\omega_{D1}}{\omega} \left(a_{l+1}2^{l+1}U_{0on} + \sum_{i=0}^l a_i2^iU_{0on} + \sum_{i=l+2}^{2N-1} a_i2^iU_{0on} \right) \times \times \sin \omega \frac{T_1}{2} \sum_{k_1=-\infty}^{\infty} [\delta(\omega - \omega_0 - k_1\omega_{D1}) + \delta(\omega + \omega_0 - k_1\omega_{D1})]. \quad (4)$$

Как видно из соотношения (4) в спектре сигнала, прошедшего САЦАП, КУ которой на некоторых уровнях содержит НСХ, проявляются отклонения от идеальной системы, соответствующие величине отклонений на этих уровнях.

Для выявления этих отклонений нами в ряде работ предложено применить вейвлет-анализ, используя для этого вейвлет Морле [6, 7]. Тогда сигнал во временной области, представленный соотношением (3), при проведении такого анализа, является сверткой с вейвлетом Морле, и запишется как

$$s_3(t) = \sum_{n_1=-\infty}^{\infty} \text{rect}\left(\frac{t-n_1T_1}{T_1}\right) \left(a_{l+1}2^{l+1}U_{0on} + \sum_{i=0}^l a_i2^iU_{0on} + \sum_{i=l+2}^{2N-1} a_i2^iU_{0on} \right) \cos \omega_0(n_1T_1) \otimes \otimes \pi^{-\frac{1}{4}} \left(e^{j\omega_c t} - e^{-\frac{\omega_c^2}{2}} \right) e^{-\frac{t^2}{2}}, \quad (5)$$

где $\beta = \frac{1}{\sqrt{2}}$, ω_c – частота (носитель) гетеродинамирования гауссиана, входящего в вейвлет Морле.

С учетом того, что свертка во временной области эквивалентна их произведению в частотной области представления сигналов, спектр сигнала, представленного соотношением (5) запишется как

$$S_3(j\omega) = \frac{\sum_{n_1=-\infty}^{\infty} \text{rect}\left(\frac{t-n_1T_1}{T_1}\right)\omega_{D1}}{\omega} \left(a_{l+1}2^{l+1}U_{0on} + \sum_{i=0}^l a_i2^iU_{0on} + \sum_{i=l+2}^{2N-1} a_i2^iU_{0on} \right) \times \times \sin \omega \frac{T_1}{2} \sum_{k_1=-\infty}^{\infty} [\delta(\omega - \omega_0 - k_1\omega_{D1}) + \delta(\omega + \omega_0 - k_1\omega_{D1})] \sqrt{2\pi}^{\frac{1}{4}} \left(e^{-\frac{(\omega-\omega_c)^2}{2}} - e^{-\frac{\omega^2}{2}} \cdot e^{-\frac{\omega_c^2}{2}} \right). \quad (6)$$

С учетом свойств вейвлет преобразования, можно заключить, что из соотношений (5) и (6) следует возможность выделения локальных максимумов в сигнале, образующихся за счет НСХ КУ. Но такие максимумы фактически всегда будут повторяться в сигнале, прошедшем через САЦАП. При этом они всегда будут повторяться в местах нарушения монотонности СХ преобразования КУ, имеющих строго индивидуальный характер для каждой конкретной системы.

Выводы

1. Исходя из полученных соотношений, можно заключить, что нарушения монотонности СХ преобразования КУ носят фрактальный характер и выделяются из преобразованных сигналов при использовании вейвлета Морле.

2. Для последующей оценки характера выделенных нарушений можно применить методы математической статистики.

Список литературы

1. Рыбальский, О.В. Современные методы проверки аутентичности магнитных фонограмм в судебно-акустической экспертизе / О.В. Рыбальский, Ю.Ф. Жариков. – К.: НАВСУ, 2003. – 300 с.
2. Рибальський, О.В. Застосування вейвлет-аналізу для виявлення слідів цифрової обробки аналогових і цифрових фонограм у судово-акустичній експертизі / О.В. Рибальський. – К.: НАВСУ, 2004. – 167 с.
3. Рыбальский, О.В. Основные положения теории выявления следов цифровой обработки фонограмм и особенности ее программной и методической реализации в экспертизе материалов и средств видеозвукозаписи. Ч. 1. / О.В. Рыбальский // Захист інформації. – 2006. – № 1. – С. 71-76.
4. Баранов, Л.А. Квантование по уровню и временная дискретизация в цифровых системах управления / Л.А. Баранов. – М.: Энергоатомиздат, 1990. – 304 с.
5. Федорков, Б.Г. Микроэлектронные цифро-аналоговые и аналого-цифровые преобразователи / Б.Г. Федорков, В.А. Телец, В.П. Дегтяренко. – М.: Радио и связь, 1984. – 120 с.
6. Соловьев, В.И. Идентификация аппаратуры аудиозаписи по статистическим характеристикам аудиофайлов / В.И. Соловьев // Реєстрація та обробка інформації. – 2013. – Т. 14, № 1. – С. 59-70.
7. Рыбальский, О.В. Применение вейвлета Морле при создании методов и аппаратуры для проведения экспертиз материалов цифровой видеозвукозаписи / О.В. Рыбальский, В.И. Соловьев, В.К. Железняк // Вестник Полоцкого государственного университета. Серия С: Фундаментальные науки. – 2014. – № 3. – С. 3-9.

**МОДЕЛЬ ПРОЯВУ ТА ВИЯВЛЕННЯ ВПЛИВУ НЕМОНОТОННОСТІ СТАТИСТИЧНОЇ
ХАРАКТЕРИСТИКИ КВАНТУВАЧА РІВНЯ У ВИХІДНОМУ СИГНАЛІ СИСТЕМИ АНАЛОГО-
ЦИФРО-АНАЛОГОВОГО ПЕРЕТВОРЕННЯ**

О.В. Рибальський, В.І. Соловйов

Національна академія внутрішніх справ,
пл. Солом'янська, 1, Київ, 03035, Україна; e-mail: rybalsky_ol@mail.ru

Запропонована модель опису прояву технологічних погрешностей квантувача за рівнем аналогового сигналу на виході системи аналого-цифро-аналогового перетворення. Показано, що такі прояви можуть бути виявлені застосуванням вейвлет-аналізу при використанні вейвлета Морле. Показано, що ці прояви носять фрактальний характер. Запропоновано їх статистичні характеристики виявляти шляхом застосування відомих методів математичної статистики.

Ключові слова: аналого-цифрове перетворення, квантування за рівнем, статична характеристика квантування, немонотонність, нелінійність статичної характеристики.

**MODEL TO MANIFEST AND DETECT THE INFLUENCE OF MONOTONICITY OF STATIC
CHARACTERISTIC OF AMPLITUDE QUANTIZER IN OUTPUT SIGNAL OF ANALOG TO
DIGITAL TO ANALOG CONVERSION SYSTEM**

O.V. Rybalsky, V.I. Solovyev

National Academy of Internal Affairs,
1, Solomenskaya sq., Kiev, 03035, Ukraine; e-mail: rybalsky_ol@mail.ru

A model is proposed to define manifestations of instrument inaccuracies of an analog signal amplitude quantizer at the output of analog to digital to analog conversion system. It was shown that these manifestations can be detected by wavelet analysis using Morlet wavelet. Additionally, it was shown that these manifestations are of fractal character. It is proposed to determine their static characteristics using customary methods of mathematical statistics.

Keywords: analog to digital to analog conversion, amplitude quantization, static quantization characteristic, static characteristic nonlinearity.

FACTORIZATION ALGORITHMS FOR CRYPTOGRAPHIC ANALYSIS OF ASYMMETRIC CRYPTO SYSTEMS

L.M. Timoshenko¹, K.V. Verbik¹, Ya.M. Nikolaichuk², S.V. Ivasiev²

¹ Odesa National Polytechnic University,

1 Shevchenko Str., Odesa, 65044, Ukraine; e-mail: lmt0902@gmail.com

² Ternopil national economical university,

1, Lvivska Str., Ternopil, 46020, Ukraine; e-mail: stepan.ivasiev@gmail.com

Improvement of existing factorization methods is one of the most urgent problems of modern asymmetric cryptography. RSA factorization problems (from RSA-968 до RSA-2048) have not been solved yet. Any factorization problem has high computational complexity and requires seeking ways to reduce this complexity for factorization methods, including a well known Fermat's method. This paper shows an approach – using Chrestenson basis and Jacobi symbols – for such a reduction. The basis allows reducing the computational complexity by reducing the length of the numbers subjected to operations.

Keywords: asymmetric cryptography, RSA, factorization, Fermat's factorization method, Chrestenson basis, computational complexity.

Introduction

Currently, asymmetric encryption is used for identification and authentication of users, prevention of data intrusion, and protection of electronic documents against counterfeiting and copying.

RSA system, the most known and popular public-key encryption system, is based on the computational intensiveness of factorization problem for long integers. The cryptographic strength of RSA system is based on the following fact: an encrypted message cannot be easily revealed without knowledge of factors P and Q , and finding these factors and N is considered a hardly solvable problem [1].

Today's computer networks are high speed networks and ensure high capacity for data processing and storage. Therefore, they require more reliable protection than stand-alone computers, since with the increase in network speed, the time for parallel implementation of cryptanalytic algorithms decreases. This gives a chance for unauthorized access to computer networks. Paralleling of cryptanalytic algorithms will allow performing the cryptanalysis of user messages not at the expense of increased capacity of an individual computer, but due to distribution of personal computers and connecting them to computer networks, including Internet.

Extended key length should compensate for any improvement to factorization algorithms. The question of an asymptotic upper bound on the running time of a factorization algorithm remains open. Currently, determining the prime factorization of a number is considered a computationally intensive problem. However, this statement is not proved; and this ambiguity encourages specialists to refine the existing algorithms and to develop the new ones. The potential exists to prove the computational intensiveness of factorization. This would guarantee the security of RSA system within a domain of keys.

Factoring a three hundred digit number is at the limit of current capabilities, whereas factoring a number having more digits is still a task for the future. The problems of factoring RSA-896 to RSA-2048 remain open.

A polynomial-time algorithm for prime factorization on a quantum computer has been already developed. The question of existence of such an algorithm for a common computer remains one of the key open issues in number theory. Therefore, improvement in the speed of existing factoring methods is one of the most urgent tasks in information security [2].

Purpose and tasks of the study

To increase the reliability of data-flow security in computer networks, it is required to increase the cryptographic strength of asymmetric cryptographic security systems. The *purpose* of this paper is to reduce the computational complexity of the factorization algorithm for assessment of cryptographic strength of RSA compatible systems by improvement of Fermat's factorization method. To implement this purpose, the following tasks should be solved:

1. analysis of modern methods of solving cryptanalytic problems,
2. substantiation of the use of the system of remainder classes,
3. improvement of Fermat's factorization method,
4. assessment of computational complexity of the algorithm proposed, and
5. comparative analysis of efficiencies of the improved and common Fermat's factorization methods.

Main Body

Factorization and discrete logarithm approaches are commonly used to solve cryptanalytic problems for public-key encryption systems. They not only present a threat currently, but have a potential for increase in value in the future. In [8], the following methods for factorization of natural numbers have been discussed: Fermat's factorization method, Pollard's rho algorithm, Shanks square forms factorization method, Lehman's method, Dixon's algorithm, continued fraction method, quadratic sieve, elliptic curve method, and number field sieve algorithms (special number field sieve and general number field sieve).

Depending on the complexity, factorization algorithms are generally divided into two groups. The first group comprises exponential algorithms, with their complexity exponentially depending on the lengths of input parameters (i.e., on the length of a binary represented number). To denote their complexity, it is common practice to use «O notation». This notation allows taking into account in function $f(n)$ only the most significant elements and neglecting the less significant elements. The second group comprises subexponential algorithms that run in the time greater than polynomial time but less than exponential time. While studying the operation of the algorithms, the following has been revealed: Fermat's factorization method is the most efficient when near factors are present; elliptic curve method is the most efficient when a relatively small factor is present; Shanks and Pollard's methods are the two most effective methods when the factors are small. Therefore, Fermat's factorization method is the best available for common RSA compatible crypto systems [9].

The emergence of new cryptographic phenomena and methods resulted in the emergence of new cryptographic applications of number theory. Along with elementary and analytic number theory, algebraic number theory and analytic arithmetic geometry are becoming more and more commonly used. Currently, quadratic sieve algorithm is commonly used. It is an exponential and computationally intensive algorithm.

Let us consider the use of Fermat's factorization method for large numbers. As is known, Fermat's factorization method is an odd number factorization algorithm that was proposed by Pierre Fermat as early as 1643. It is effective when N is the product of two integer numbers that are near to each other [3]. The factorization of a natural number into a

product of primes exists and is unique up to rearrangement of the factors, as it follows from a basic theorem of arithmetic.

Fermat's factorization method is based on finding the two integers, x and y , satisfying $x^2 - y^2 = n$, that leads to factorization $n = (x - y)(x + y)$. Encoding schemes are specified by the theoretical-and-numeral bases used for representation.

Commonly used are unitary, Haar, Gray, Rademacher, Chrestenson and Galois bases.

Chrestenson basis produces a system of remainder classes and is successfully used to develop special data compression processors and to implement high-capacity processors in cryptographic security systems [4].

It is well known that parallel processing is the most promising approach to speed up computation [7]. This feature is pertinent to the system of remainder classes (SRC) [2]. Although it has some shortcomings, the system ensures efficient performance of some operations (addition, subtraction, multiplication, and exponentiation for large numbers), which is very important, particularly when solving asymmetric cryptography problems.

Representation of decimal number N in SRC conforms to the least remainders b_i of this number in the system of mutually coprime modules p_i , that is, $b_i = N \bmod p_i$. Here the calculation range should be within $0 \leq N \leq P - 1$, where $P = \prod_{i=1}^n p_i$. SRC-to-decimal

conversion is performed based on the Chinese remainder theorem: $N = \left(\sum_{i=1}^n b_i B_i \right) \bmod P$,

where $B_i = M_i m_i$, $M_i = \frac{P}{p_i}$, and basis numbers m_i are found from $(M_i m_i) \bmod p_i = 1$ [11].

The need for calculating basis numbers $m_i = M_i^{-1} \bmod p_i$ significantly increases the computational complexity of SRC-to-decimal conversion. The complexity of this problem is reduced for a full SRC form (SRC FF), when all $m_i = 1$ [4]. In [5], a modified SRC FF (SRC MFF) has been proposed, with basis numbers $m_i = \pm 1$, which excludes the need of seeking for the reciprocal number. To reduce the computational complexity of Fermat's factorization method, in [10] it has been proposed to use numerical Chrestenson basis that represents a number as the remainder when this number is divided by a fixed module.

We shall apply SRC to equation

$$x^2 = y^2 - n, \quad (1)$$

and perform the following conversion

$$x^2 \bmod p = y^2 - n \bmod p. \quad (2)$$

to get $x^2 \equiv (y^2 - n) \bmod p$. In order to solve this equation, it is advantageous to use Jacobi symbols that allow specifying explicitly whether a square root modulo is computed. This approach reduces the computational complexity of the algorithm.

Let $n \geq 3$ be an odd integer, and it is known that $n = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$, where p_i are prime numbers. Jacobi symbol $\left(\frac{a}{n} \right)$ is defined as follows:

$$\left(\frac{a}{n} \right) = \left(\frac{a}{p_1} \right)^{k_1} \left(\frac{a}{p_2} \right)^{k_2} \dots \left(\frac{a}{p_t} \right)^{k_t}.$$

It follows from the properties of Jacobi symbols [1] that if n is an odd integer, and a is represented as $a = 2^k a_1$, where a_1 is an odd integer, then

$$\left(\frac{a}{n}\right) = \left(\frac{2^k}{n}\right) \left(\frac{a_1}{n}\right) = \left(\frac{2^k}{n}\right) \left(\frac{n \bmod a_1}{a_1}\right) (-1)^{\frac{(a_1-1)(n-1)}{4}}.$$

This formula allows computing the Jacobi symbol without knowing the prime factorization of n .

To find x , we need to perform the following conversion:

$$x \equiv \sqrt{(y^2 - n)} \bmod p. \quad (3)$$

Then the improvement of Fermat method consists in the following: we shall deliberately disregard the values of $(y^2 - n)$ for which the root is not defined, and reduce the resolution at the expense of modulo operation.

The flowchart of the improved factorization algorithm is shown in Fig. 1.

In order to assess the complexity of the algorithm developed, we need to determine the number of basic operations. It is worth to mention that the main computationally complex operations of the algorithm developed are seeking for a Jacobi symbol, computation of a modular square root, and computation of a root of the number. Table 1 presents the estimations of complexity of the basic steps of the multidigit number factorization algorithm developed.

Table 1.

Complexity of the basic operations of the algorithm developed

Basic steps of the multidigit number factorization algorithm developed	Complexity values of the basic operations
sqstart = Sqrt(P0)	n
Difference = (sqstart+1) * (sqstart+1)	$n \log_2 n$
Difference = Difference- P0	n
sqstartm[i] = (sqstartm + 2) mod Prime[i]	$\log_2 n$
If Jacobi symbol (sqstartm[i], Prime[i]) ≠ 1 then Step 8	$\log_2^2 n$
If Jacobi symbol (sqstartm[i], Prime[i]) = 1 then i++, Step 10	$\log_2^2 n$
If Sqrt(Difference) is fractional, then Step 6	n
Output of sqrt(Difference+sqstart*sqstart)+sqrt(Difference)	n

Therefore, the total complexity of the algorithm developed is calculated as $O(n \log_2 n + 2 \log_2^2 n + 4n) \approx O(n \log_2 n)$.

Since conventional Fermat's factorization method is similar to the trial division algorithm, the complexity of this method is estimated as $O(n(\log_2 n)^2)$.

The results of our investigations show that the algorithm developed has lower computational complexity than the conventional one, which is well seen in a graph showing the algorithm complexity versus the length of the input number (Fig. 2).

Since the operating efficiency of a factorization algorithm is estimated through its computational complexity, the improved Fermat's factorization method developed is more efficient than the conventional one.

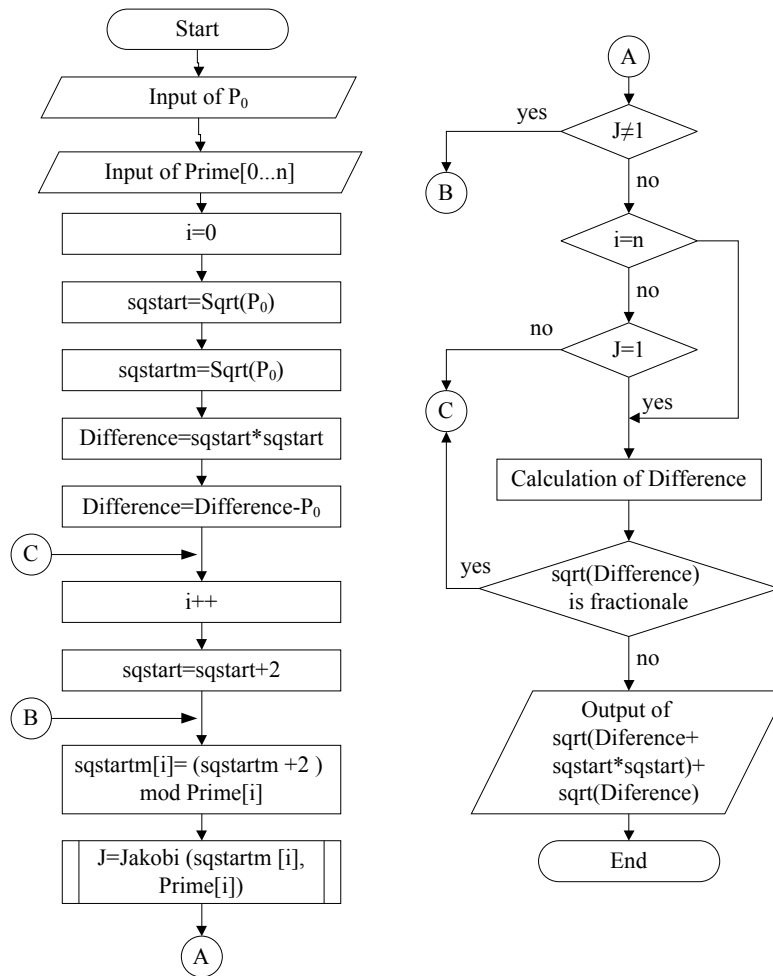


Figure 1. Flowchart of the improved Fermat's factorization algorithm

The operating efficiency gain of the algorithm developed compared to the conventional one is then defined as their computational complexity ratio

$$E(n) = \frac{n(\log_2 n)^2}{n(\log_2 n)} = \log_2 n.$$

Therefore, the efficiency gain of the algorithm developed increases with the increase in the bitlength of the number.

Based on the algorithm proposed and using C++ Builder 6.0 environment, we have developed a software product to perform factorization of multidigit numbers for specified module p .

For operations with extra long variables, a special A. Lenstra's library (involving Lip.h and Lip.c) was used. This library is optimized for use in crypto systems and incorporates a set of functions which we used in the application developed. The results of numerical experiments are in agreement with theoretical calculations and validate the scientific approach proposed.

Therefore, the efficiency of the Fermat's factorization method improved to reduce the computational complexity of factorization has been proved theoretically and experimentally.

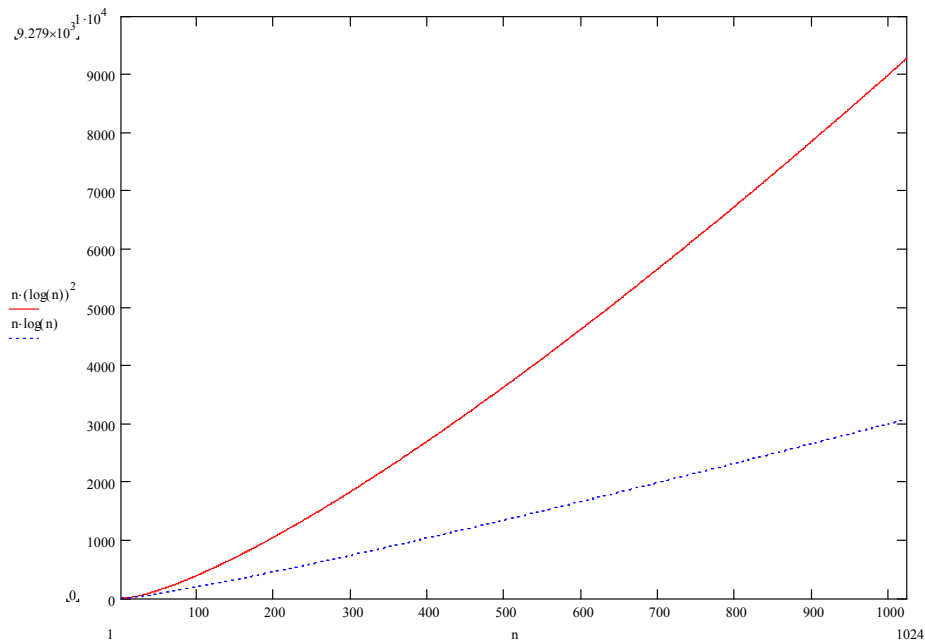


Figure 2. Computational complexity of the algorithm developed compared to that of the conventional one.

Conclusion

The basic factorization methods have been discussed and it has been revealed that Fermat's method is the most efficient when near factors are present. Additionally, the use of Chrestenson basis for the improvement of Fermat's factorization method for multidigit numbers has been substantiated.

Fermat's method has been improved using Chrestenson basis and Jacobi symbols, which allowed reducing its computational complexity.

Chrestenson basis allows reducing the computational complexity by reducing the length of the numbers subjected to operations,

Jacobi symbols allow not to use the numbers for which the square root modulo does not exist.

Thus, the operating efficiency gain of the algorithm developed compared to the conventional one equals $\log_2 n$.

Therefore, the improvement proposed in this paper for Fermat's method is a promising one for the assessment of the cryptographic strength of asymmetric cryptographic security systems.

References

1. Айерлэнд, К. Классическое введение в современную теорию чисел / К. Айерлэнд, М. Роузен. – М.: Мир, 1987. – 416 с.
2. Акушский, И.Я. Машинная арифметика в остаточных классах / И.Я. Акушский, Д.И. Юдицкий. – М: Сов.радио, 1968. – 440 с.
3. Вербіцький, О.В. Вступ до криптології / О.В. Вербіцький. – Львів: ВНТЛ, 1998. – 248 с.

4. Василенко, О.Н. Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко. – М.:МЦНМО, 2003. – 328 с.
5. Касянчук, М.М. Теорія та математичні закономірності досконалої форми системи залишкових класів / М.М. Касянчук // Праці Міжнародного симпозиуму «Питання оптимізації обчислень (ПОО–XXXV)». – Київ–Кацивелі. – 2009.– Т.1. – С. 306-310.
6. Николаенко, О.В. Анализ методов факторизации в криптографических системах защиты информации / О.В. Николаенко, Л.Н. Тимошенко, К.В. Вербик // Матеріали III міжнародної науково-практичної конференції ІУСТ-Одеса-2014. – С. 173-175.
7. Николайчук, Я.М. Теорія джерел інформації / Я.М. Николайчук. – Тернопіль: ТзОВ «Тернограф», 2010. – 536 с.
8. Тимошенко, Л.М. Современные методы решения криптоаналитических задач / Л.Н. Тимошенко, К.В. Вербик // Матеріали ВШСМВС АСІТ'2014. – Тернопіль, 2014. – С. 220-222.
9. Тимошенко, Л.М. Шляхи удосконалення алгоритму факторизації чисел / Л.М. Тимошенко, К.В. Вербик // Тези доповідей Х МНПК «Військова освіта і наука: сьогодення та майбутнє». – Київ, 2014. – С. 220-222.
10. Тимошенко, Л.М. Удосконалений метод Ферма факторизації чисел / Л.М. Тимошенко, К.В. Вербик, С.В. Івасьєв // Всеукраїнської НПК «Проблеми становлення інформаційної економіки в Україні». – Львів, 2014. – С.348-350.
11. Якименко, І.З. Алгоритм знаходження системи модулів модифікованої досконалої форми системи залишкових класів / І.З. Якименко, М.М. Касянчук, Л.М. Тимошенко, С.В. Івасьєв, Я.М. Николайчук // Матеріали МНПК СІЕТ. – Одеса, 2014. – С. 115-117.

АЛГОРИТМИ ФАКТОРИЗАЦІЇ ДЛЯ КРИПТОАНАЛІЗУ АСИМЕТРИЧНИХ КРИПТОСИСТЕМ

Л.М. Тимошенко¹, К.В. Вербик¹, Я.М. Николайчук², С.В. Івасьєв²

¹ Одеський національний політехнічний університет,
просп. Шевченка, 1, м. Одеса, 65044, Україна; e-mail: lmt0902@gmail.com

² Тернопільський національний економічний університет,
вул. Львівська, 1, м.Тернопіль, 46020, Україна; e-mail: stepan.ivasiev@gmail.com

Удосконалення існуючих методів факторизації є однією з найбільш актуальних задач сучасної криптографії. Задачі факторизації RSA від RSA-968 до RSA-2048 залишаються відкритими. На сьогодні задача факторизації має велику обчислювальну складність. Ставиться важливе завдання пошуку шляхів зменшення обчислювальної складності, у тому числі, і відомого методу Ферма. Дане дослідження пропонує один з напрямів його вирішення. Запропоновано скористатися теоретико-числовим базисом Крестенсона, який дозволяє зменшити обчислювальну складність за рахунок зменшення розрядностей чисел, над якими проводяться операції.

Ключові слова: факторизація, метод Ферма, базис Крестенсона, символ Якобі, обчислювальна складність, асиметрична криптографія, RSA.

АЛГОРИТМЫ ФАКТОРИЗАЦИИ ДЛЯ КРИПТОАНАЛИЗА АССИМЕТРИЧНЫХ КРИПТОСИСТЕМ

Л.Н. Тимошенко¹, К.В. Вербик¹, Я.М. Николайчук², С.В. Ивасьев²

¹ Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: lmt0902@gmail.com

² Тернопольский национальный экономический университет,
ул. Львовская, 1, г.Тернополь, 46020, Украина; e-mail: stepan.ivasiev@gmail.com

Усовершенствование существующих методов факторизации является одной из наиболее актуальных задач современной криптографии. Задачи факторизации RSA от RSA-968 до RSA-2048 остаются открытыми. На сегодняшний день задача факторизации имеет большую вычислительную сложность. Ставится важное задание поиска путей уменьшения вычислительной сложности, в том числе, и известного метода Ферма. Данное исследование предлагает одно из направлений его решения. Предложено воспользоваться теоретико-числовым базисом Крестенсона, который позволяет уменьшить вычислительную сложность за счет уменьшения разрядностей чисел, над которыми проводятся операции.

Ключевые слова: факторизация, метод Ферма, базис Крестенсона, символ Якоби, вычислительная сложность, асимметричная криптография, RSA.

КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ КРИТИЧЕСКИХ ПРОСТРАНСТВ СОСУЩЕСТВОВАНИЯ НА ФАЗОВЫХ ДИАГРАММАХ МНОГОКОМПОНЕНТНЫХ ТВЕРДЫХ РАСТВОРОВ

А.И. Казаков, Л.Т. Кваташидзе, Г.В. Шаповалов

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

Эпитаксиальные слои полупроводниковых твердых растворов, выращенные в нестабильных областях, демонстрируют для определенных температур и составов тенденцию к формированию структур с периодическим распределением состава. Рассмотрена методика компьютерного моделирования процесса формирования критических пространств в сложных многокомпонентных системах на основе использования дифференциального топологического подхода. Предложен метод определения полных производных свободной энергии четверных твердых растворов со смешением в двух подрешетках с третьей по восьмую включительно с использованием модели регулярного раствора и стандартных термодинамических функций для бинарных соединений для описания взаимодействия атомов в многокомпонентных твердых растворах. Символьное дифференцирование и численные расчеты производных проводились с использованием системы компьютерной математики *Mathima*. Рассчитаны сечения фазовой диаграммы $In-Ga-As-P$, критические пространства и пространства сосуществования фаз в четырехмерном пространстве для различных температур. Полученные результаты моделирования показывают возможность формирования областей сосуществования фаз различных порядков в твердых растворах $In_xGa_{1-x}As_yP_{1-y}$, что не противоречит имеющимся экспериментальным данным, где наблюдалась пространственная модуляция состава твердого раствора.

Ключевые слова: пространства сосуществования фаз, упорядоченные фазы, многокомпонентные системы, матричные производные.

Введение

В настоящее время значительный интерес вызывают новые функциональные материалы электронной техники. Определенный прогресс достигнут не только в создании и исследовании таких материалов, но и в понимании проблемы самоорганизованного образования упорядоченных структур для современной микро- и нанoeлектроники. Изучение этих явлений имеет важное значение, прежде всего, для современных технологий микроструктур и нанобъектов. Это, в первую очередь, многокомпонентные полупроводниковые твердые растворы с неоднородным распределением концентраций компонентов, такие как периодические структуры, сверхрешетки, системы «квантовых точек» и т.д. [1]. Для анализа процессов получения самоорганизовано образующихся упорядоченных наноструктур возможно использование компьютерного моделирования на основе термодинамических подходов. В подобных случаях необходим расчет многомерных фазовых диаграмм,

учитывающий возможность существования бифуркационных пространств, критических пространств и пространств сосуществования фаз различных порядков.

При термодинамическом описании фазовых переходов уравнение состояния вещества задает некоторое m -мерное многообразие в соответствующем пространстве. Для оценки особенностей потенциальной функции самоорганизующейся системы в случае использования одного параметра порядка можно использовать теорию катастроф, рассматривая ее как обобщенную форму теории фазовых переходов Гинзбурга-Ландау [2]. Однако для оценки составов сосуществующих фаз и описания возможных фазовых переходов в многокомпонентных системах необходимо использование подходов, позволяющих анализировать особенности потенциальных функций нескольких параметров порядка.

Цель работы

Целью работы является разработка методов расчета и анализа высших производных потенциальных функций нескольких параметров порядка в рамках термодинамического моделирования фазовых равновесий в четырехкомпонентных твердых растворах на основе положений теории бифуркаций и теории катастроф.

В качестве объекта исследования были выбраны четырёхкомпонентные твёрдые растворы со смешением атомов в двух подрешётках вида $A_x B_{1-x} C_y D_{1-y}$. Основываясь на дифференциальном топологическом подходе, основные принципы которого изложены в работе [2], можно построить модели процесса формирования критических пространств и пространств сосуществования фаз в многокомпонентных и многофазных системах. Пространство сосуществования фаз возникает, когда одно стабильное состояние сосуществует с другим стабильным состоянием. Появление подобного пространства есть фазовый переход первого рода, определяемый принципом Максвелла, когда два (или более) глобальных минимума потенциальной функции имеют одинаковую глубину. В некоторых точках изучаемого пространства стабильная фаза может становиться нестабильной, образуя бифуркационное подпространство. Две фазы в некоторой области могут быть идентичными при некоторых значениях параметра порядка, образуя критическое пространство порядка 2. При наличии трех или четырех идентичных фаз образуются критические пространства порядка 3 или 4 соответственно. Условие существования стабильных фаз в этом случае имеют вид [2]:

$$\frac{dG}{dx} = 0; \quad \frac{d^2G}{dx^2} > 0. \quad (1)$$

Область нестабильности или бифуркационное пространство:

$$\frac{dG}{dx} = \frac{d^2G}{dx^2} = 0; \quad \frac{d^3G}{dx^3} > 0. \quad (2)$$

Условие существования критического пространства второго порядка:

$$\frac{dG}{dx} = \frac{d^2G}{dx^2} = \frac{d^3G}{dx^3} = 0; \quad \frac{d^4G}{dx^4} > 0. \quad (3)$$

Условие существования критического пространства третьего порядка:

$$\frac{dG}{dx} = \frac{d^2G}{dx^2} = \dots = \frac{d^5G}{dx^5} = 0; \quad \frac{d^6G}{dx^6} > 0. \quad (4)$$

Условие существования критического пространства четвертого порядка:

$$\frac{dG}{dx} = \frac{d^2G}{dx^2} = \dots = \frac{d^7G}{dx^7} = 0; \quad \frac{d^8G}{dx^8} > 0. \quad (5)$$

Изложение основного материала

Обобщение условий (1-5) на случай m -мерного концентрационного пространства позволяет проводить анализ возможных критических пространств и пространств сосуществования фаз в многокомпонентных твердых фазах на основе исследования высших производных потенциальной энергии системы по параметрам порядка x_i . Был проведен анализ существующих принципов использования многомерных матриц и получения соответствующих матричных производных [4]. Также была рассмотрена возможность разложения в многомерный ряд Тейлора свободной энергии многокомпонентных систем. Высшие производные свободной энергии, с третьей по восьмую включительно, по концентрационным параметрам рассматриваемой четырехкомпонентной системы были получены с использованием матрично-векторного дифференцирования многомерных систем с применением метода прямых сумм [5].

Процесс моделирования формирования критических пространств для описания свободной энергии исследуемой системы допускает использование различных термодинамических моделей. Четырехкомпонентные твердые растворы вида $A_xB_{1-x}C_yD_{1-y}$ со смещением атомов, как в катионной, так и в анионной подрешетках представляются как смесь четырех гипотетических бинарных соединений с концентрациями X_{ij} . Свободная энергия $G = G(X_{AC}, X_{BC}, X_{AD}, X_{BD})$ такого твердого раствора будет являться функцией четырех концентрационных параметров $X_{AC}, X_{BC}, X_{AD}, X_{BD}$, а матрица вторых производных свободной энергии по этим параметрам будет иметь размерность 4×4 . В рамках модели строго регулярного раствора, использованной в данной работе, в которой предполагается случайное распределение разнородных атомов по узлам соответствующих подрешеток, выражения для концентраций бинарных компонентов, записанных через концентрационные параметры x и y , имеют вид [3]:

$$X_{AC} = (1-x)(1-y), X_{AD} = (1-x)y, X_{BC} = x(1-y), X_{BD} = xy. \quad (6)$$

Определение высших производных свободной энергии системы в рассматриваемом случае анализа возможности существования критических подпространств проводилось следующим образом. В работе в качестве начальных соотношений были использованы символьные элементы матрицы вторых производных свободной энергии твердого раствора вида $A_xB_{1-x}C_yD_{1-y}$, обусловленной эффектами смешения по концентрациям X_{ij} , полученные с использованием модели регулярного раствора [7]. Для получения третьей производной функции m аргументов были использованы произведения Кроникера матрицы вторых производных свободной энергии на операторы дифференцирования по соответствующим аргументам [6]. Далее, с использованием метода прямых сумм получали блочные матрицы полной третьей

производной, содержащей m блоков частных производных размером $m \times m$. Получение производных свободной энергии многокомпонентной системы высших порядков проводилось с использованием аналогичного алгоритма.

Результаты

Символьное дифференцирование для получения аналитических выражений для частных и полных высших производных путем и численные вычисления производных выполнялись с использованием системы компьютерной математики Maxima [8]. Полученные в работе аналитические выражения для полных производных свободной энергии Гиббса четырехкомпонентных гомогенных твердых растворов типа $A_xB_{1-x}C_yD_{1-y}$, позволили численно определить положения областей существования производных и нулевых контуров производных со второй по восьмую включительно на сечении существования твердых растворов диаграммы состояния исследуемой системы $In_xGa_{1-x}As_yP_{1-y}$ для диапазона температур 773К-1023К. Термодинамические параметры, использованные в расчетах, приведены в таблице 1.

Таблица 1.

Параметры взаимодействия в твердой фазе для квазибинарных систем

Квазибинарная система	Параметр взаимодействия α_{ij-jk}^5 , Дж/моль, [9]
$GaP - InP$	14665
$GaAs - InAs$	12570
$GaP - GaAs$	1676
$InP - InAs$	1676

Далее на основе проведенных вычислений были построены контура областей сосуществования фаз порядков два, три и четыре на сечении существования твердых растворов диаграммы состояния исследуемой системы для различных температур. На рисунках 1-4 представлены полученные результаты расчета положения нулевых контуров производных свободной энергии Гиббса анализируемой системы по концентрационным параметрам, начиная со второй производной и по восьмую производную включительно включительно для температуры 773 К. Темным цветом показана область отрицательных значений производной. Светлым цветом показана область положительных значений производной. Также показаны линии изопериодных составов к подложкам из $GaAs$ и InP и экспериментальные составы эпитаксиальных слоев $In_xGa_{1-x}As_yP_{1-y}$, в которых наблюдалось формирование периодических модулируемых структур, полученных с помощью жидкофазной эпитаксии на подложках из InP [10,11] и на подложках из $GaAs$ [12,13] и полученных с помощью газотранспортной эпитаксии на подложках из InP [14]. В этих работах описаны случаи образования структур с простой одномерной модуляции [10,11], так и сложной модуляции состава, таких как наличие двух различных длин концентрационных волн в различных кристаллографических направлениях [11], и формирование системы чередующихся доменов твердого раствора двух различных составов [12,13]. В работе [14] приведены результаты исследования структуры эпитаксиальных слоев $In_xGa_{1-x}As_yP_{1-y}$, полученных осаждением из газовой фазы на подложках из InP при температуре 973 К. Образование квазипериодических структур концентраций состава с длиной волны модуляции от 10-20 нм вдоль направления $[110]$ до 80 нм вдоль направления $[001]$ наблюдалось для диапазонов концентраций получаемых твердых

растворов $0.2 < x < 0.53$ и $0.37 < y < 1$. В результате проведения дополнительных экспериментальных исследований было показано, что эти модуляции состава не являются следствием неустойчивости процесса роста [13]. Также было показано, что условия роста эпитаксиальных слоев не влияют на период модуляции состава [10].

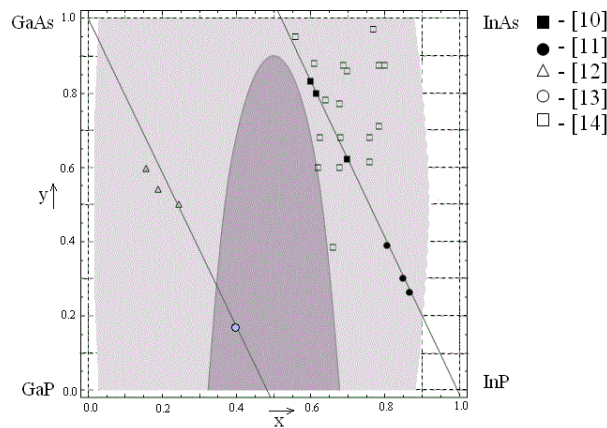


Рис.1. Сечение существования твердых растворов диаграммы состояния системы $In-Ga-As-P$. Приведены результаты численных расчетов второй производной свободной энергии системы

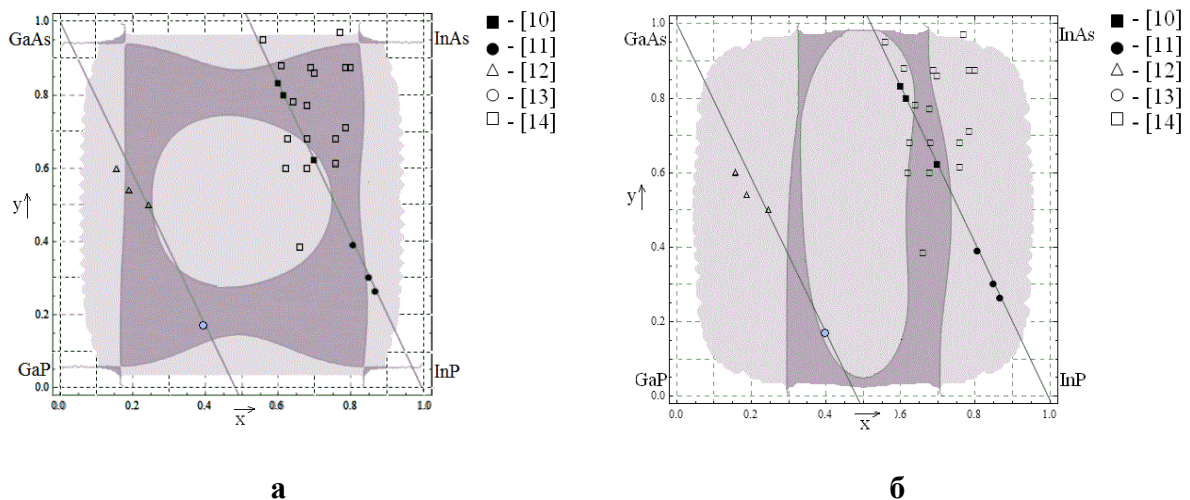


Рис.2. Сечения существования твердых растворов диаграммы состояния системы $In-Ga-As-P$. Результаты численных расчетов: а – третьей; б – четвертой производных свободной энергии системы.

Полученные в работе положения нулевых контуров для третьей и четвертой производных свободной энергии системы по концентрациям бинарных компонентов для твердого раствора $In_xGa_{1-x}As_yP_{1-y}$ (рис.2) показывают, что большинство экспериментальных точек, для которых наблюдается модуляция состава, попадают в область отрицательных значений третьей производной и находятся в области положительных значений четвертой производной, что соответствует выполнению условий формирования пространств сосуществования фаз порядка два и позволяет построить эти пространства на сечении диаграммы состояния.

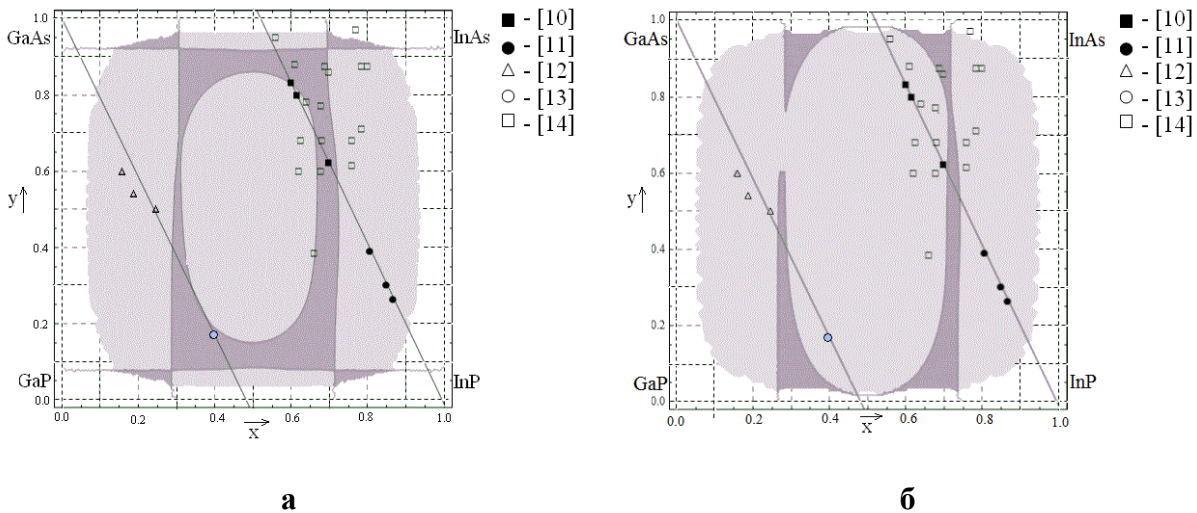


Рис.3. Сечения существования твердых растворов диаграммы состояния системы $In - Ga - As - P$. Результаты численных расчетов: а – пятой; б – шестой производных свободной энергии системы

На рисунке 4 представлены результаты моделирования областей на сечении существования твердых растворов диаграммы состояния системы $In - Ga - As - P$, где возможно сосуществование двух твердых фаз для различных температур. Темным цветом показаны области выполнения условий формирования пространств сосуществования фаз порядка два для температуры а) 773 К, б) 1050 К. Показаны изопериодные линии для подложек из $GaAs$ и InP . Для построения этих областей были использованы результаты численных расчетов производных со второй по четвертую включительно свободной энергии системы. Как видно из приведенных рисунков, большинство экспериментальных составов эпитаксиальных слоев, полученных в работах [10-14], в которых наблюдалось образование модулированных периодических структур, попадает в расчетные области сосуществования фаз. Таким образом, полученные результаты компьютерных расчетов областей сосуществования фаз показывают возможность использования предложенного подхода для описания процесса формирования модулированных структур в многокомпонентных твердых растворах.

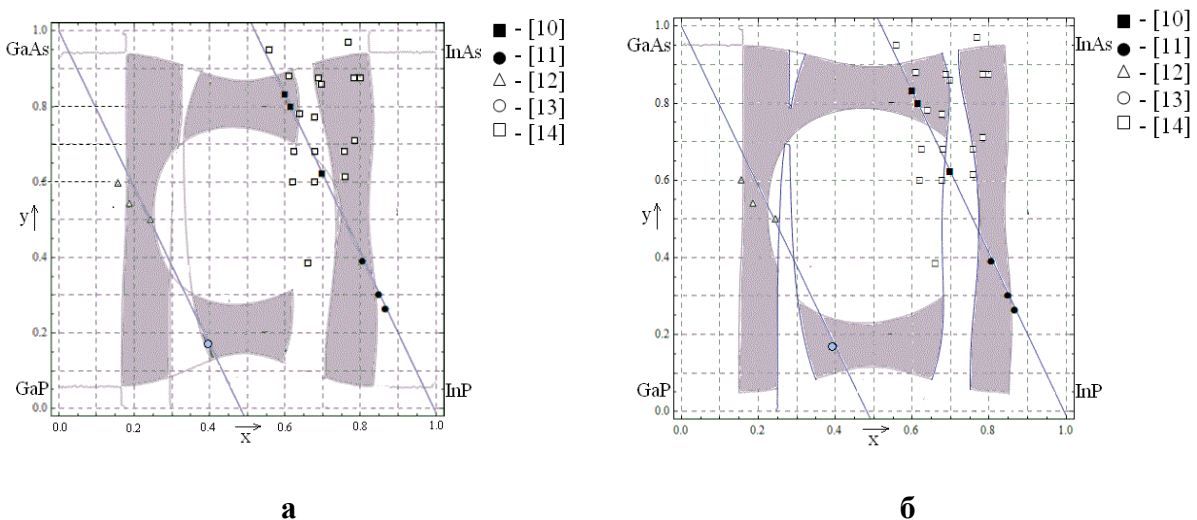


Рис.4. Сечения существования твердых растворов диаграммы состояния системы $In - Ga - As - P$. Показаны области выполнения условий формирования пространств сосуществования фаз порядка два и изопериодные линии для подложек из $GaAs$ и InP

Выводы

Полученные результаты моделирования критических пространств во многокомпонентных системах на основе предложенного дифференциального топологического подхода позволяют объяснить имеющиеся экспериментальные данные по спонтанному формированию двухфазных модулированных структур в эпитаксиальных слоях твердого раствора $In_xGa_{1-x}As_yP_{1-y}$. Показано, что использованная модель регулярного раствора для свободной энергии Гиббса твердого раствора позволяет проводить достаточно корректную оценку положения пространств сосуществования порядка 2 на фазовых диаграммах. Увеличение температуры системы приводит к уменьшению полученной области сосуществования пространств. Исходя из полученных результатов моделирования положения областей сосуществования фаз порядка 2, можно предположить, что предложенная модель может быть использована для прогнозирования пространства возможного образования периодических модулированных структур на фазовых диаграммах многокомпонентных систем также для случаев двух- и трехмерной модуляции состава твердых растворов.

Список литературы

1. Малинецкий, Г.Г. Математические основы синергетики: Хаос, структуры, вычислительный эксперимент / Г.Г. Малинецкий. – Москва: ЛКИ, 2007. – 312 с.
2. Okada, K. Classical calculations on the phase transition I. Phase diagram in four-dimensional space for the system with one order parameter / K. Okada, I. Suzuki // J. Phys. Soc. Jap. – 1982. – Vol. 51, No.10. – PP. 3250-3257.
3. Onabe, K. Thermodynamics of the type $Al_{1-x}BxC_1-yD_y$, III-V quaternary solid solutions / K. Onabe // J.Phys.Chem.Solids/ – 1982. –V.43, No.11. – PP. 1071-1086.
4. Муха, В.С. Анализ многомерных данных: проблемы, состояния, перспективы / В.С. Муха // Доклады БГУИР. – 2004. – №1. – С.38-49.
5. Корн, Г. Справочник по математике / Г. Корн, Т. Корн. – М.: Наука, 1974. – 832 с.
6. Traat, I. Matrix calculus for multivariate distributions / I. Traat // Уч. зап. Тарт. гос. ун-та. – 1986. – Вып.733. – С. 64-85.
7. Kazakov, A. Computer simulation for stability of quaternary solid solutions / A. Kazakov, I. Kishmar // J. Crystal Growth. – 1991. – Vol.110. – PP. 803-814.
8. Система компьютерной алгебры Maxima [Электронный ресурс] / Режим доступа: <http://maxima.sourceforge.net>. (Дата обращения 05.11.2013).
9. Расчет фазовых равновесий в многокомпонентных системах / А.И. Казаков, В.А. Мокрицкий, В.Н. Романенко и др. – М.: Металлургия, 1987. – 136 с.
10. Composition modulation in liquid phase epitaxial $In_xGa_{1-x}As_yP_{1-y}$ layers lattice matched to InP substrates / P. Henoc, A. Izrael, M. Quillec, H. Launois // Appl. Phys. Let. – 1982. – Vol. 40. – PP. 951-963.
11. Spinodal decomposition in InGaAsP epitaxial layers / S. Mahajan, B.V. Dutt, H. Temkin, and others // J. Crystal Growth. – 1984. – Vol.68, No.2. – PP. 589-595.
12. Electron microscope study of modulated structures and heterointerfaces in LPE-grown GaInAsP layers lattice matched on GaAs / N. Kuwano, K. Funuka, Oki K. and others // J. Crystal Growth. – 1989. – Vol.98. – PP. 82-89.
13. Спонтанно формирующиеся периодические InGaAsP-структуры с модулированным составом / Л.С. Вавилова, В.А. Капитонов, А.В. Мурашева и др. // Физика и техника полупроводников. – 1999. – Т. 33, № 9. – С. 1108-1110.
14. Chu, S. Surface layer spinodal decomposition in $In_{1-x}Ga_xAs_{1-y}Py$ and $In_{1-x}Ga_xAs$ grown by hybrid transport vapor phase epitaxy / S. Chu, S. Nakahara, K. Strege, W. Johnston // J.Appl.Phys. – 1985. – Vol.57. – PP. 4610-4616.

КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ КРИТИЧНИХ ПРОСТОРІВ СПІВІСНУВАННЯ НА ФАЗОВИХ ДІАГРАМАХ БАГАТОКОМПОНЕНТНИХ ТВЕРДИХ РОЗЧИНІВ

А.И. Казаков, Л.Т. Кваташидзе, Г.В. Шаповалов

Одесский национальный политехнический университет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: anatkaz@mail.ru

Епітаксiальні шари напівпровiдникових твердих розчинiв, вирощенi у нестабiльних областях демонструють для певних температур i складiв тенденцiю до формування структур з перiодичним розподiлом складу. Розглянуто методику комп'ютерного моделювання процесу формування критичних просторiв у складних багатокомпонентних системах на основi використання диференцiального топологiчного пiдходу. Запропоновано метод визначення повних похiдних вiльної енергiї четвертих твердих розчинiв зi змiшанням в двох пiдгратках з третього по восьмий включно з використанням моделi регулярного розчину i стандартних термодинамiчних функцiй для бiнарних сполук для опису взаємодiї атомiв в багатокомпонентних твердих розчинах. Символьне диференцiювання та чисельнi розрахунки похiдних проводилися з використанням системи комп'ютерної математики Maxima. Розрахованi перерiзи фазової дiаграми $In-Ga-As-P$, критичнi простори i простори спiвiснування фаз в чотиривимiрному просторi для рiзних температур. Отриманi результати моделювання показують можливiсть формування областей спiвiснування фаз рiзних порядкiв у твердих розчинах $In_xGa_{1-x}As_yP_{1-y}$, що не суперечить наявним експериментальним даним, де спостерiгалася модуляцiя складу твердого розчину.

Ключові слова: простори спiвiснування фаз, впорядкованi фази, багатокомпонентнi системи, матричнi похiднi.

COMPUTER MODELING OF CRITICAL COEXISTENCE SPACES AT PHASE DIAGRAMS OF MULTICOMPONENT SOLID SOLUTIONS

A.I. Kazakov, L.T. Kvatahidze, G.V. Shapovalov

Odesa National Polytechnic University,
1 Shevchenko Str., Odesa, 65044, Ukraine; e-mail: anatkaz@mail.ru

Epitaxial layers of semiconductor solid solutions grown in unstable areas tend to form structures with periodic composition distribution under certain temperatures and compositions. A methodology is discussed for computer modeling of formation of critical coexistence spaces in complex multicomponent systems based on a differential topological approach. A method is proposed to determine total derivatives of the free energy of quaternary solid solutions with mixing on two sublattices (from the third to the eighth inclusive) using a regular solution model and standard thermodynamic functions for binary systems to define atomic interaction in multicomponent solid solutions. Symbolic differentiation and numerical calculation of derivatives were performed using the computer algebra system Maxima. The following was calculated: sections of $In-Ga-As-P$ phase diagram, critical spaces and phase coexistence spaces in the four-dimensional space under different temperatures. The modeling results obtained show the potential to form coexistence spaces for phases of different orders in solid $In_xGa_{1-x}As_yP_{1-y}$ solutions. This is not in disagreement with the experimental evidence available, where spatial modulation of solid solution composition has been observed.

Keywords: phase coexistence spaces, ordered phases, multicomponent systems, matrix derivatives.

АНАЛІЗ СТАТИСТИЧНОЇ БЕЗПЕКИ КРИПТОАЛГОРИТМІВ АСИМЕТРИЧНОГО ШИФРУВАННЯ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

Ю.Є. Яремчук

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

Проведено аналіз статистичної безпеки криптоалгоритмів асиметричного шифрування інформації на основі рекурентних U_k та V_k -послідовностей у порівнянні з відомим алгоритмом Ель-Гамала для довжини ключа 4096 розрядів. За результатами аналізу найвищий рівень статистичної безпеки показав криптоалгоритм на основі V_k -послідовностей.

Ключові слова: криптографія, асиметричне шифрування, криптостійкість, статистична безпека, рекурентні послідовності.

Вступ

На сьогодні задача забезпечення конфіденційності інформації ефективно вирішується за допомогою криптоалгоритмів [1], серед яких асиметричні [1–4] володіють перевагою відсутності необхідності фізичного розподілу ключів секретним каналом зв'язку або наявності третьої сторони для реалізації цього. Найбільш відомими асиметричними криптоалгоритмами є RSA [3] та Ель-Гамала [4]. У роботах [5] та [6] представлено асиметричні криптоалгоритми, що базуються відповідно на основі рекурентних U_k - та V_k -послідовностей. У порівнянні з відомими криптоалгоритмами вони забезпечують за певних умов можливість спрощення обчислень. Актуальним при цьому залишається аналіз криптографічної стійкості цих криптоалгоритмів у порівнянні з відомими аналогами.

У роботі [7] проведено дослідження статистичної безпеки представлених у [5] та [6] криптоалгоритмів, однак актуальним залишається питання більш детального аналізу статистичної безпеки цих криптоалгоритмів для великих розмірів ключа, зокрема у 4096 розрядів, оскільки розвиток обчислювальної техніки для збільшення стійкості вимагає постійного збільшення розміру чисел, над якими виконуються криптографічні перетворення.

Метою роботи є проведення аналізу статистичної безпеки запропонованих у [5] та [6] асиметричних криптоалгоритмів на основі рекурентних U_k - та V_k -послідовностей для розміру ключа у 4096 розрядів у порівнянні з відомим криптоалгоритмом Ель-Гамала.

Оцінювання статистичної безпеки асиметричних криптоалгоритмів для довжини ключа у 4096 розрядів

Для дослідження статистичної безпеки асиметричних криптоалгоритмів використано пакет NIST STS [8], який включає у себе набір з 16 статистичних тестів.

У таблиці 1 наведено дані про проходження результуючих послідовностей криптоалгоритмами на основі рекурентних U_k - та V_k -послідовностей та Ель-Гамалю для довжини ключа 4096 бітів.

Таблиця 1.

Кількість тестів, що пройшли успішне тестування для ключа у 4096 бітів

Метод	для $\alpha = 0.01$		для $\alpha = 0.001$	
	більше 99% послідовностей	більше 96% послідовностей	більше 99% послідовностей	більше 98% послідовностей
Ель-Гамалю	61 (32.45%)	160 (85.11%)	149 (79.26%)	162 (86.17%)
U_k	56 (29.79%)	160 (85.11%)	145 (77.13%)	161 (85.64%)
V_k	57 (30.32%)	156 (82.98%)	142 (75.53%)	162 (86.17%)

З таблиці 1 видно, що відсоток проходження тестів послідовностями на основі V_k - та U_k -послідовностей гірший, ніж за методом Ель-Гамалю (30.32% та 29.79% порівняно з 32.45%) при найжорсткішому порозі проходження (проходженням 99% послідовностей тестів при $\alpha = 0.01$).

У таблиці 2 наведено відсотки проходження кожного з 16 тестів для $\alpha = 0.001$ та $\alpha = 0.01$ для довжини ключа 4096 розрядів.

Як видно з результатів, наведених у таблиці 2, найкращі результати $\alpha = 0.001$ має криптоалгоритм на основі V_k -послідовностей. Також видно, що криптоалгоритми на основі V_k - та U_k -послідовностей зберігають показники 99-100% за іншими тестами, в той час як алгоритм Ель-Гамалю має нижчі показники на рівні 83-94%. Це дає підстави говорити, що методи на основі V_k - та U_k -послідовностей у цілому є більш статистично безпечними, ніж метод Ель-Гамалю. Порівнюючи результати для рівня значимості $\alpha = 0.01$, слід відзначити, що алгоритм на основі U_k -послідовностей має дещо вищі відсотки проходження за алгоритм на основі V_k -послідовностей.

На рисунках 1-3 представлено статистичні портрети криптоалгоритмів асиметричного шифрування для довжини ключа 4096 бітів.

Як видно з рисунків 1-3, статистичні портрети результатів тестування методів знаходяться на високому рівні, виключення становлять тести 161-186, яким відповідають тести на перевірку випадкових відхилень. Ці тести є найжорсткішими порівняно з іншими, тому ці показники є очікуваними. З рисунків видно, що частка проходження 90% тестів для послідовностей за методами шифрування на основі V_k - та U_k -послідовностей вища за 0.98, порівняно з методом Ель-Гамалю (0.94), що свідчить про вищу статистичну безпеку цих методів.

На рисунку 4 показано узагальнені графіки за кожним тестом для кожного методу шифрування для довжини ключа 4096 розрядів.

Результати тестування на рис. 4 показують, що послідовності за алгоритмом Ель-Гамалю мають гірші показники (на 0.03) порівняно з алгоритмами на основі V_k - та U_k -послідовностей у тесті на перевірку шаблонів, які перекриваються.

Таблиця 2.

Відсотки проходження кожного з 16 тестів для довжини ключа 4096 бітів

№ тесту	Назва статистичного тесту	для $\alpha = 0.001$			для $\alpha = 0.01$		
		Е-Г	U_k	V_k	Е-Г	U_k	V_k
1	Частотний (монобітний) тест	100%	100%	100%	100%	100%	99%
2	Частотний тест всередині блоку	98%	100%	99%	98%	100%	98%
3	Послідовний тест	83%	100%	100%	98%	98%	100%
4	Перевірка максимальної довжини серії в блоці	96%	100%	100%	99%	99%	98%
5	Перевірка рангу двійкової матриці	100%	100%	100%	100%	100%	98%
6	Спектральний тест на основі дискр. перетв. Фур'є	100%	100%	100%	100%	98%	99%
7	Перевірка шаблонів, які не перекриваються	100%	100%	100%	99%	99%	99%
8	Перевірка шаблонів, які перекриваються	94%	100%	100%	95%	98%	99%
9	Універсальний тест Маурера	100%	99%	100%	99%	99%	99%
10	Перевірка лінійної складності	99%	100%	100%	98%	97%	99%
11	Перевірка серій	93%	100%	100%	100%	98%	100%
12	Ентропійний тест	91%	100%	100%	100%	99%	98%
13	Перевірка накоплених сум	100%	100%	100%	100%	99%	99%
14	Перевірка випадкових відхилень	51%	64%	67%	60%	63%	57%
15	Перевірка випадкових відхилень (модифікація)	51%	64%	67%	61%	63%	56%
16	Перевірка стиснення по алгоритму Лемпеля-Зіва	100%	100%	100%	100%	100%	99%

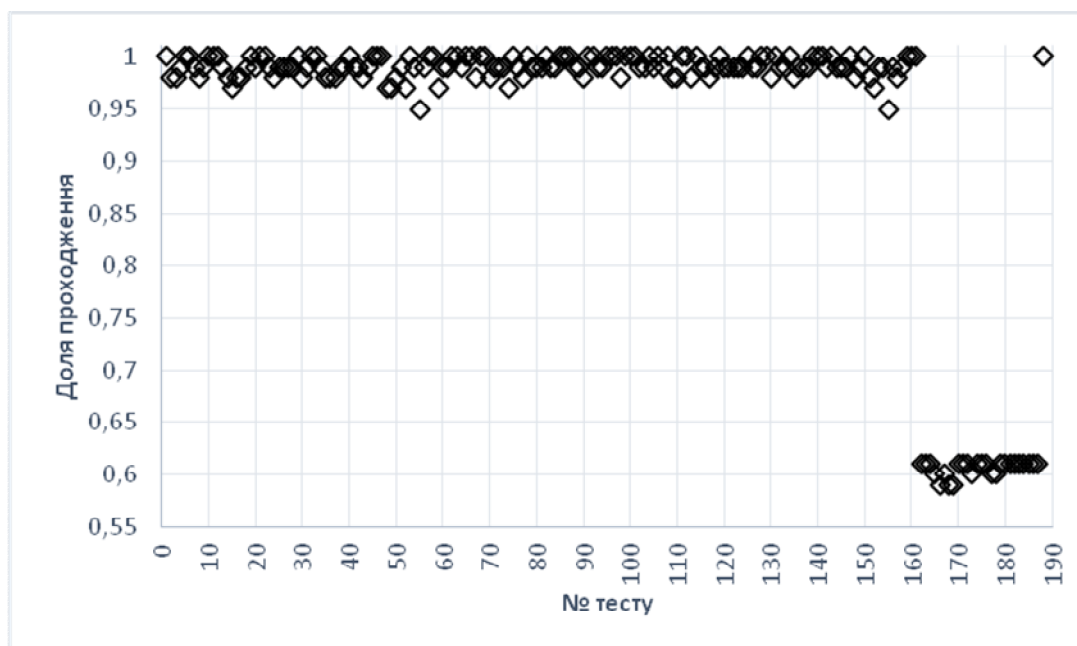


Рис. 1. Результати тестування алгоритму Ель-Гамала з розміром ключа 4096 бітів

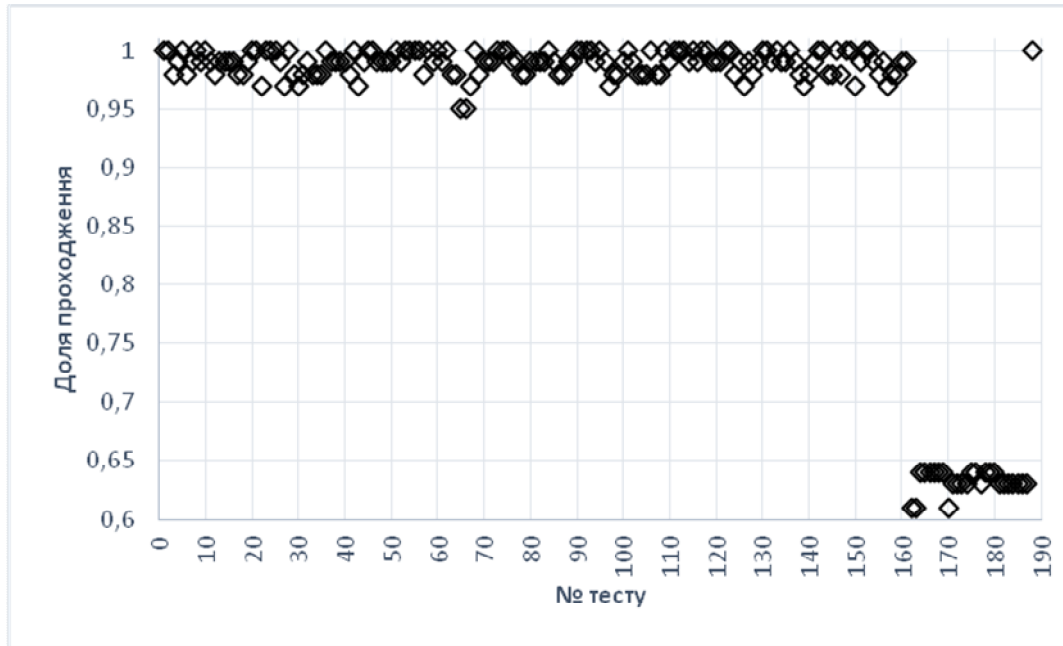


Рис. 2. Результати тестування алгоритму шифрування на основі U_k -послідовностей з розміром ключа 4096 бітів

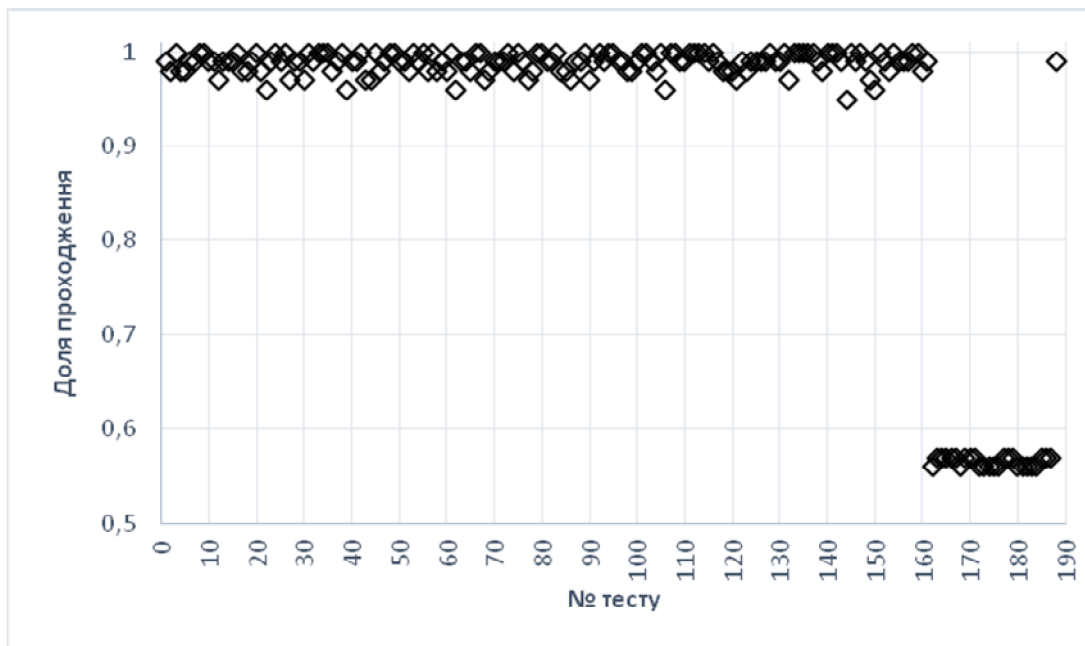


Рис. 3. Результати тестування алгоритму шифрування на основі V_k -послідовностей з розміром ключа 4096 бітів

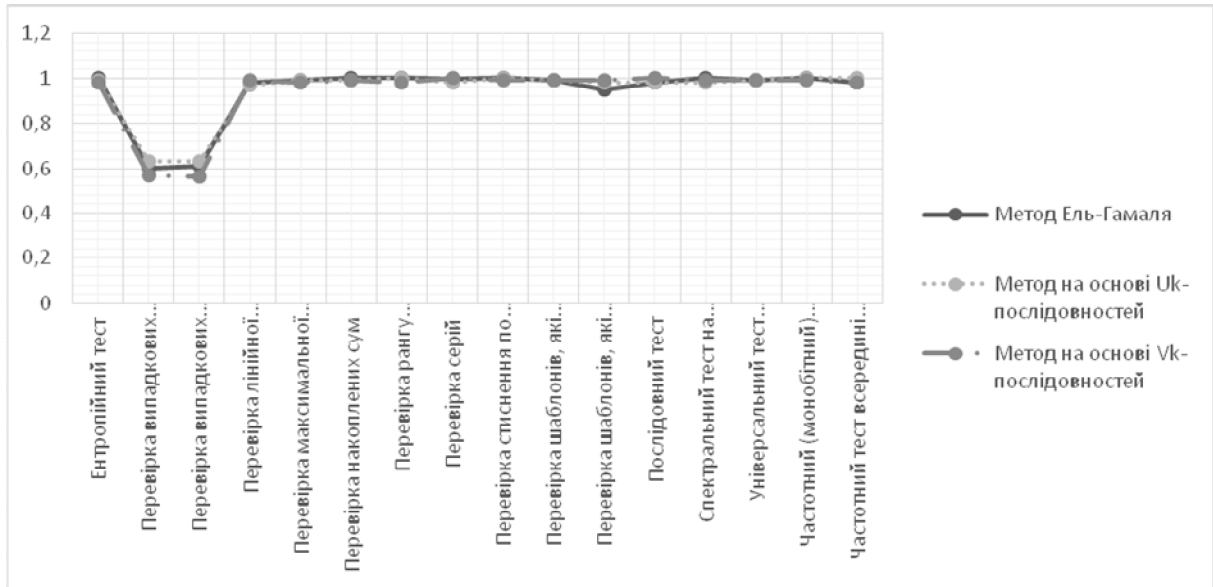


Рис. 4. Частка проходження тестів для послідовностей з розміром ключа 4096 біт

Висновки

Дослідження запропонованих у [5] та [6] методів асиметричного шифрування відповідно на основі U_k - та V_k -послідовностей порівняно з відомим методом асиметричного шифрування Ель-Гамалю показало, що для довжини ключа у 4096 розрядів, показники тестування послідовностей за алгоритмом Ель-Гамалю майже зрівнюються з показниками методів основі V_k - та U_k -послідовностей. При розмірі ключа 4096 біт 100% проходження майже усіх тестів отримали алгоритми на основі V_k - та U_k -послідовностей. Порівнюючи результати тестування з рівнем значимості $\alpha = 0.01$, найкращі показники показав алгоритм на основі V_k -послідовностей. У цілому запропоновані алгоритми на основі V_k - та U_k -послідовностей мають високі показники статистичної безпеки порівняно з Ель-Гамалю, але при найжорсткішому тестуванні найвищий рівень статистичної безпеки показав саме алгоритм на основі V_k -послідовностей, отримуючи найвищі показники за усіма тестами, випереджаючи результати тестування послідовностей за алгоритмом на основі U_k -послідовностей.

Порівняння отриманих результатів для розміру ключа у 4096 розрядів з результатами, отриманими у роботі [7] для менших розмірів ключа, показує, що у цілому із збільшенням розміру ключа показники статистичної безпеки відомого криптоалгоритму вирівнюються з показниками криптоалгоритмів, що базуються на рекурентних послідовностях.

Список літератури

1. Menezes, A.J. Handbook of Applied Cryptography [Текст] / A.J. Menezes, P.C. van Oorschot, S.A. Vanstone. – CRC Press, 2001. – 816 p.
2. Саломая, А. Криптография с открытым ключом: Пер. с англ [Текст] / А. Саломая. – М.: Мир, 1995. – 318 с.

3. Rivest, R.L. A method for obtaining digital signatures and public-key cryptosystems [Текст] / R.L. Rivest, A. Shamir, L.M. Adleman // Communications of the ACM. – 1978. – Vol.21, No.2. – PP. 120-126.
4. Elgamal, T. A public key cryptosystem and a signature scheme based on discrete logarithms [Текст] / T. Elgamal // IEEE Intern. Symp. Informat. Theory. – 1985. – Vol.31. №4. – PP. 469-472.
5. Яремчук, Ю.Є. Метод асиметричного шифрування інформації на основі рекурентних послідовностей [Текст] / Ю.Є. Яремчук // Сучасна спеціальна техніка. – 2012. – №4. – С. 79-87.
6. Яремчук, Ю.Є. Метод шифрування інформації з відкритим ключем на основі рекурентних послідовностей [Текст] / Ю.Є. Яремчук // Інформаційна безпека. – 2013. – №3. – С. 123-129.
7. Яремчук, Ю.Є. Дослідження статистичної безпеки методів асиметричного шифрування інформації на основі рекурентних послідовностей / Ю.Є. Яремчук // Сучасний захист інформації. – 2014. – №2. – С. 64-72.
8. NIST SP 800-22 Rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications [Текст] / A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo. – National Institute of Standards and Technology, 2010. – 131 p.

АНАЛИЗ СТАТИСТИЧЕСКОЙ БЕЗОПАСНОСТИ КРИПТОАЛГОРИТМОВ АССИМЕТРИЧНОГО ШИФРОВАНИЯ НА ОСНОВЕ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Ю.Е. Яремчук

Винницкий национальный технический университет,
ул. Хмельницьке шосе, 95, Винница, 21021, Украина; e-mail: yurevyar@vntu.net

Проведено аналіз статистическої безпеки криптоалгоритмів асиметричного шифрування інформації на основі рекурентних U_k - і V_k - послідовностей по порівнянню з відомим алгоритмом Ель-Гамала для довжини ключа 4096 разрядів. По результатам аналізу найбільш високий рівень статистическої безпеки показав криптоалгоритм на основі V_k - послідовностей.

Ключевые слова: криптография, асимметричное шифрование, криптостойкость, статистическая безопасность, рекуррентные последовательности.

STATISTICAL SECURITY ANALYSIS OF ASYMMETRIC CRYPTO ALGORITHMS BASED ON RECURRENT SEQUENCES

Yu.E. Yaremchuk

Vinnytsia National Technical University,
95 Khmelnytske shose, Vinnytsia, 21021, Ukraine; e-mail: yurevyar@vntu.net

Statistical security analysis was performed for asymmetric crypto algorithms based on recurrent U_k - and V_k sequences and compared with that for the El Gamal algorithm for 4096-bit key. A crypto algorithm based on recurrent V_k sequences was shown to have the highest level of statistical security.

Keywords: cryptography, asymmetric encryption, cryptographic strength, statistical security, recurrent sequences.

ХАРАКТЕРИСТИКА И ЗНАЧЕНИЕ МЕЖДУНАРОДНОЙ СТАТИСТИКИ КИБЕРПРЕСТУПНОСТИ

В.И. Трапезников

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: comandor1949@yandex.ua

Рассматривается статистика киберпреступности на материалах США с точки зрения ее необходимости для оценки состояния, динамики изменения в количественных и других характеристиках для определения проблемных направлений организации противостояния этому виду преступления. Показана невозможность организации, правильной постановки задачи решения вопроса искоренения киберпреступности для всех участников этой сложной работы без серьезного изучения конкретной статистики этого вида преступления.

Ключевые слова: киберпреступность, статистическая классификация преступлений, латентность киберпреступлений, виктимизация киберпреступлений

Введение

Если количество радиослушателей во всем мире достигло 50 млн. человек только через 38 лет после изобретения радио, а для телевидения этот срок составил 13 лет, то количество пользователей всемирной сети Internet превысило полсотни миллионов всего через 4 года после ее появления. Эффект формирования глобального информационного пространства, придавший мощнейший импульс человеческому прогрессу, одновременно (как, впрочем, и всегда) имел и негативную сторону.

Во второй половине истекшего века развитие общественных и экономических отношений привело к огромному увеличению перерабатываемой информации, вследствие чего возникла необходимость в поиске новых и более эффективных средств хранения, учета, поиска и переработки этой информации, поскольку прежние формы пользования информацией уже не удовлетворяли потребности общества.

Внедрение в управленческие процессы и другие сферы жизни общества электронно-вычислительной техники позволило успешно решить эту задачу, способствовало стремительному развитию научной мысли и успешному решению многих технических и социальных проблем. Но это достижение человечества стало использоваться не только в полезных для общества целях.

Фактически развитие научно-технического прогресса, связанное с внедрением современных информационных технологий, привело к появлению новых видов преступлений, в частности, к незаконному вмешательству в работу ЭВМ, систем и компьютерных сетей, хищению, присвоению, вымогательству компьютерной информации, опасному антисоциальному явлению, получившему распространенное название – киберпреступность.

«Киберпреступность не имеет государственных границ, – следовательно, и усилия по противодействию ей – дело не одного государства. Нужное плодотворное международное сотрудничество многих стран мира, как на государственном уровне, так и на уровне сотрудничества между правительственными организациями и представителями бизнеса в сфере распространения IT-технологий», – цитирует пресс-

центр СБУ слова руководителя отдела кибернетической защиты Директората новых вызовов безопасности Международного секретариата НАТО Сулеймана Анила.

Определения киберпреступности

Большая часть отчетов, рекомендаций и публикаций по вопросам киберпреступности начинаются с определения термина «киберпреступность». Одно общепринятое определение описывает киберпреступность как любое деяние, в котором инструментом, целью или местом преступных действий являются компьютеры или сети. Одним из примеров международного подхода является Статья 1.1 Проекта Международной Конвенции по улучшению защиты от киберпреступности и терроризма (CISAC), которая отмечает, что киберпреступностью называются действия в отношении кибернетических систем [1].

В некоторых определениях предприняты попытки учесть цели, намерения при определении киберпреступности как «действий посредством компьютеров, которые либо являются незаконными, либо считаются противоправными некоторыми сторонами и которые могут быть совершены при помощи глобальных электронных сетей» [2]. Эти более точные описания исключают те случаи, когда физическое оборудование используется для совершения обычных преступлений, но они рискуют исключить преступления, которые считаются киберпреступлениями в международных соглашениях, например в «Конвенции о киберпреступности». Например, человек, который создает USB85-устройства, содержащие злонамеренные программы, которые разрушают информацию в компьютере, если устройство к нему присоединено, совершает преступление, которое определяется Статьей 4 Конвенции о киберпреступности Совета Европы. Однако действие по удалению данных с использованием физического устройства для копирования злонамеренного кода не совершается по глобальным электронным сетям и не может быть квалифицировано как киберпреступление в соответствии с вышеприведенным узким определением. Это действие было бы квалифицировано как киберпреступление только в соответствии с определением, основанным на более широком описании, включающем такие действия как незаконное искажение информации. Это показывает, что определение термина «киберпреступность» встречает заметные трудности [1].

Термин «киберпреступность» используется для описания широкого спектра правонарушений, включая традиционные компьютерные преступления, а также сетевые преступления. Поскольку эти преступления во многом отличаются друг от друга, не существует единого критерия, который может включать в себя все действия, упомянутые в проекте Стэнфордской конвенции и Конвенции о киберпреступности, исключая при этом традиционные преступления, которые совершаются с использованием только оборудования. Тот факт, что не существует единого определения «киберпреступности», не должен быть очень важным до тех пор, пока этот термин не используется в качестве юридического термина [1].

Типология киберпреступности

Термин «киберпреступность» включает в себя большое разнообразие преступлений. Признанные преступления охватывают широкий спектр правонарушений, что усложняет разработку системы типологии или классификации для киберпреступности. Одна интересная система приводится в Конвенции о киберпреступности Совета Европы. Конвенция о киберпреступности различает *четыре типа правонарушений*:

- преступления против конфиденциальности, целостности и доступности компьютерных данных и систем;
- преступления, связанные с компьютерами;
- преступления, связанные с контентом;
- преступления, связанные с правами собственности.

Эта типология не является полностью последовательной, поскольку она не основана на едином базовом критерии, который бы определял различия между категориями. Три категории сфокусированы на объекте юридической защиты: «Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем»; преступлениях, связанных с контентом; и преступлениях, связанных с правами собственности. Четвертая категория «преступления, связанные с компьютерами» сфокусирована не на объекте юридической защиты, а на методе. Эта непоследовательность приводит к некоторому пересечению между категориями [1]. Кроме того, некоторые термины, которые используются для описания преступных действий (например, «кибертерроризм» или «фишинг»), охватывают действия, которые попадают в несколько категорий. Тем не менее, категории, приведенные в Конвенции о киберпреступности, являются полезной основой для обсуждения явления киберпреступности. [1]

Характеристика статистики киберпреступлений

Борьба с киберпреступностью требует всестороннего подхода. Учитывая, что одни технические меры не могут предотвратить преступлений, важно чтобы органы правопорядка имели право эффективно расследовать и наказывать киберпреступления. Очень трудно количественно оценить влияние киберпреступности на общество. Финансовые потери, обусловленные киберпреступностью, а также число правонарушений оценить очень трудно. Согласно некоторым источникам, потери из-за киберпреступности для предприятий и организаций в Соединенных Штатах Америки достигают 67 миллиардов долларов США (2011г.); однако неясно, оправдана ли экстраполяция примерных результатов исследований. Эта методологическая критика применима не только к потерям, но также и к известным правонарушениям [1].

Трудно измерить число киберпреступлений, поскольку их жертвы могут не всегда сообщать о правонарушениях. Тем не менее, исследования могут помочь в понимании влияния киберпреступности. Более важно, что точное число киберпреступлений в каждый отдельно взятый год – это тенденция, которую можно определить путем сравнения результатов за последние несколько лет.

Одним из примеров является обзор компьютерных преступлений и безопасности 2007 г., выполненный ЦРУ в Соединенных Штатах Америки, в котором помимо иных тенденций анализируется число совершенных преступлений, связанных с компьютерами. Оно основано на ответах, полученных от 494 практикующих экспертов в области компьютерной безопасности из корпораций США, правительственных органов и финансовых организаций США. В исследовании задокументировано множество правонарушений, о которых сообщили респонденты с 2000 по 2007 год. В нем показано, что с 2001 года уменьшился процент респондентов, которые испытывали или видели вирусные атаки или несанкционированный доступ к информации, или проникновение в систему. В исследовании не объяснено, почему такое уменьшение происходит. Однако это снижение числа распознанных правонарушений указанных категорий подтверждается также исследованиями других организаций (в противовес тому, что иногда предполагают средства массовой информации). Аналогичное развитие наблюдается и при анализе статистики преступности, например, статистика преступности Германии показывает, что после пика в 2004 г. количество преступлений, связанных с компьютерами, уменьшилось вплоть до уровня 2002 года [1].

Статистические данные по киберпреступности не позволяют предоставить надежную информацию о масштабе или размерах правонарушений. Эта неуверенность относительно размеров правонарушений, о которых сообщают их жертвы, а также факт невозможности найти объяснение снижению уровня киберпреступности, делают эти статистические данные открытыми для различных интерпретаций [1].

В настоящее время нет достаточного числа доказательств, для того чтобы предсказывать будущие тенденции и ход развития.

Глобальная картина статистики киберпреступности

В 2011 году по меньшей мере 2.3 миллиарда человек или более одной трети от общей численности населения планеты имели доступ к Интернету. Более 60 процентов всех пользователей Интернета находятся в развивающихся странах, причем 45 процентов всех пользователей Интернета составляют лица в возрасте до 25 лет. По оценкам, к 2017 году доступ к мобильному широкополосному Интернету получают до 70 процентов от общей численности населения мира. К 2020 году количество сетевых устройств («Интернет вещей») будет в шесть раз превосходить численность населения, что полностью изменит нынешнее представление об Интернете. В сверхподключенном к сети мире будущего будет трудно представить себе какое-либо «компьютерное преступление», а, возможно, и вообще любое преступление, которое не сопровождалось бы электронными доказательствами, связанными с подключением к интернет-протоколу (IP) [3].

Во многих странах резкий всплеск в количестве подсоединений к глобальной сети совпал по времени с экономическими и демографическими преобразованиями, ростом разрыва в доходах, сокращением расходов в частном секторе и снижением финансовой ликвидности. На общемировом уровне правоохранительные органы в своих ответах на вопросник отмечают рост уровня киберпреступности в связи с тем, что и частные лица, и организованные преступные группы используют новые возможности для совершения преступлений, руководствуясь стремлением к извлечению прибыли и получению личной выгоды. По оценкам, свыше 80 процентов киберпреступлений совершаются в той или иной форме организованной деятельности, со сложившимися черными рынками киберпреступности в области цикла создания вредоносных программ, компьютерных вирусов, управления бот-сетями, сбора персональных и финансовых данных, продажи данных и получения денег за финансовую информацию. Для совершения киберпреступлений более не требуется обладание сложными навыками или знание сложных методов. Особенно в контексте развивающихся стран появилась субкультура молодых людей, занимающихся финансовым мошенничеством при помощи компьютеров, многие из которых начинают заниматься киберпреступностью в конце подросткового возраста [3].

В глобальном плане наблюдается широкий диапазон киберпреступлений, которые включают преступления, совершаемые в целях получения финансовой выгоды, преступления, связанные с использованием содержащейся в компьютере информации, а также преступления, направленные против конфиденциальности, целостности и доступности компьютерных систем. Однако государственные органы и предприятия частного сектора по-разному воспринимают относительный риск и угрозу. В настоящее время статистические данные о преступности, регистрируемые полицией, не являются собой прочной основой для сравнений между странами, хотя такие статистические данные часто важны для разработки политики на национальном уровне. Две трети стран считают свои системы полицейской статистики недостаточными для того, чтобы регистрировать киберпреступность. Показатели киберпреступности, регистрируемые полицией, зависят не столько от непосредственного уровня преступности, сколько от уровня развития страны и специализированных возможностей полиции [3].

Деятельность правоохранительных органов и проведение расследований

Свыше 90 процентов стран-респондентов сообщают, что правоохранительным органам становится известно о деяниях в области киберпреступности из сообщений частных лиц или организаций, ставших жертвами такой деятельности. По оценкам стран-респондентов, полиция получает сообщения о виктимизации в результате киберпреступности в одном проценте случаев или более. В одном глобальном обследовании частного сектора указано, что 80 процентов частных лиц, ставших жертвами киберпреступности, в полицию о преступлении не сообщают. Тот факт, что люди редко обращаются в полицию, объясняется тем, что они не знают о виктимизации и о механизмах сообщения информации, ощущают стыд или неловкость в связи с тем, что они стали жертвами преступников, а корпорации опасаются возможного репутационного риска.

Государственные органы стран всех регионов мира сообщают об инициативах, направленных на повышение уровня представления информации о совершении преступлений, в том числе о системах, позволяющих сообщать о преступлениях по Интернету и горячим телефонным линиям, кампаниях по повышению информированности общественности, контактах с частным сектором и активизации информационно-пропагандистской деятельности полиции и обмену информацией. Однако меры борьбы с киберпреступностью, принимаемые в порядке реагирования на совершенные преступления, должны сопровождаться среднесрочными и долгосрочными тактическими расследованиями в отношении рынков преступности и разработчиков преступных схем.

Виктимизация – это сложный процесс, который может включать в себя несколько этапов. Первый из них – первичная виктимизация, включает в себя взаимодействие между преступником и жертвой в процессе совершения преступления, а также последствия этого взаимодействия или самого преступления. Второй этап – реакция жертвы на преступление, в том числе возможные изменения в самовосприятии, а также формальные меры, которыми жертва может отреагировать на преступление. Третий этап – последующие взаимодействия жертвы с другими людьми, в том числе с представителями правоохранительных органов, к которым она может обратиться. Если это взаимодействие тоже оказывает негативный эффект на жертву, его называют повторной виктимизацией [4].

Правоохранительные органы развитых стран работают в этой области, в том числе используя действующие под прикрытием подразделения по выявлению правонарушителей на сайтах социальных сетей, в чатах и при обмене мгновенными сообщениями и пользовании материалами совместного пользования. Трудности при расследовании киберпреступлений связаны с использованием преступниками новаторских преступных методов, сложностями в получении доступа к электронным доказательствам и с внутренними ограничениями в отношении ресурсов, потенциала и материально-технических возможностей. Подозреваемые часто используют технологии анонимизации и запусков следов, и новые технологии быстро получают распространение в преступном мире благодаря онлайн-преступным рынкам.

Выводы. Зачем нужна статистическая классификация преступлений?

Классификация преступлений для статистических целей, в первую очередь, необходима для организованного сбора данных о преступлениях в рамках информационно-аналитической работы. Классификация преступлений позволяет эффективно и упорядоченно структурировать данные по всем видам преступлений, подразделяя их на несколько категорий, что отчасти напоминает концептуально-аналитическую деятельность и работу, связанную с вопросами политики [5].

Стандартная классификация преступлений для статистических целей является важным инструментом для улучшения сопоставимости и повышения качества данных на национальном и международном уровнях [5].

На национальном уровне классификация данных позволяет лучше систематизировать информацию об отдельных правонарушениях, предусмотренных нормативно-правовыми документами, которую обычно трудно использовать в аналитических целях. Классификация также может служить важнейшим средством согласования деятельности по сбору и распространению данных, проводимой различными органами уголовного правосудия (полицией, прокуратурой, судами и тюрьмами) и органами субнационального уровня, которые могут использовать различные нормативно-правовые базы и организационные принципы, а также деятельности по сбору и распространению данных из различных источников (административных документов и статистических обследований). Благодаря общей классификации данных о преступности и уголовном правосудии уровень согласованности национальных данных повышается [5].

На международном уровне использование статистической классификации преступлений необходимо для улучшения сопоставимости данных о преступности по странам, что имеет важность для повышения эффективности анализа тенденций и ситуации в целом на глобальном и региональном уровнях. Несмотря на то, что на пути обеспечения высокой степени сопоставимости данных по странам сохраняются другие проблемы (различия в методах регистрации преступлений, правилах учета, технических и организационных возможностях и т.д.), использование согласованных подходов, общей терминологии и единых критериев является важным шагом в сторону улучшения сопоставимости статистических данных.

Было отмечено, что есть с трудом поддающиеся статистическому учету преступления, в их числе киберпреступность, или компьютерные преступления, которые охватывают различные правонарушения, такие как незаконный доступ к компьютерным данным и системам (хакерство), размещение запрещенного контента (например, детской порнографии или ксенофобских материалов), нарушение авторских прав и другие компьютерные правонарушения (такие как интернет-мошенничество в целях хищения личных данных или кража цифровых персональных данных). Во всех случаях качество данных, полученных из административных документов, страдает из-за низкого уровня их регистрации и выявления по таким причинам, как отсутствие прямых жертв (как в случае с нарушением авторских прав), существование современных систем для сокрытия следов преступления и личности преступников, нежелание жертв сообщать о преступлении из-за опасения возможных негативных последствий (как, например, в случае хакерской атаки против какого-либо финансового учреждения) [5].

Говорить о статистике киберпреступности в Украине на уровне международных требований к сожалению невозможно, так как ее латентность (*латентная преступность* (от лат. *latens* / *latentis* - скрытый; англ. *latens criminality*) - уголовно наказуемые деяния, не ставшие известными государственным правоохранительным органам в течение определенного периода времени на определенной территории и не отраженные в официальной уголовной статистике).

Наказуемые деяния, которые не были зафиксированы вообще, относятся к *абсолютной латентной преступности*. Относительную латентную преступность составляют уголовно наказуемые деяния, которые жертва, преступник или третье лицо воспринимают как преступление, но не заявляют о нем в правоохранительные органы [6] практически достигает 90%, а то и более. Это серьезное упущение в работе всех правоохранительных органов нашего государства, которое не дает возможность увидеть все проблемы киберпреступности.

Спеціалісти НАТО вважають, що Україна є вразливою не тільки зовні, внутрішня небезпека також існує. Спеціалісти відзначають, що для ефективної боротьби з кібер-загрозами в Україні спочатку необхідно прийняти відповідні закони [7].

Список литературы

1. Понимание киберпреступности: Руководство для развивающихся стран // Отдел приложений ИКТ и кибербезопасности. Департамент политики и стратегии. Сектор развития электросвязи МСЭ. – Проект. Апрель 2009 г. – 228 с.
2. Hale, C. Cybercrime: Facts & Figures Concerning this Global Dilemma [Электронный ресурс] / C. Hale // CJL. – 2002. – Vol. 18. Режим доступа: <http://www.cjimagazine.com/archives/cji4411.html?id=37>
3. Осипенко, А. Л. Борьба с преступностью в глобальных компьютерных сетях: международный опыт: монография / А.Л. Осипенко. – М.: Норма, 2004. – 432 с.
4. Криминология: учебник / под ред. В.Н. Булгакова и Н.М. Кропачева. – СПб.: Изд-во СПбГУ, 2005. – 520 с.
5. E/CN.3/2013/11. Доклад Национального института статистики и географии Мексики и Управления Организации Объединенных Наций по наркотикам и преступности о программе по повышению качества и доступности статистических данных о преступности на национальном и международном уровнях: Пункт 3(j) предварительной повестки дня: Пункты для обсуждения и принятия решения: статистика преступности [Электронный ресурс]/ Записка Генерального секретаря // Организация Объединенных наций. Экономический и социальный совет. – Сорок четвертая сессия 26 февраля - 1 марта 2013 года. – 40 с. Режим доступа: <http://unstats.un.org/unsd/statcom/doc13/2013-11-CrimeStats-R.pdf>
6. Українські реферати [електронний ресурс]. Режим доступу: refine.org.ua/pageid-11300-1.html
7. СБУ отработывает с НАТО механизмы борьбы с киберпреступностью [Электронный ресурс]. Режим доступа: <http://za.zubr.in.ua/2011/10/18/13536/>

ХАРАКТЕРИСТИКА ТА ЗНАЧЕННЯ МІЖНАРОДНОЇ СТАТИСТИКИ КІБЕРЗЛОЧИННОСТІ

В.І. Трапезніков

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: comandor1949@yandex.ua

Розглядається статистика кіберзлочинності на матеріалах США з точки зору її необхідності для оцінки стану, динаміки зміни у кількісних та інших характеристиках для визначення проблемних напрямів організації протистояння цьому виду злочину. Показано неможливість організації, правильної постановки задачі вирішення питання викорінення кіберзлочинності для усіх учасників цієї складної роботи без серйозного вивчення конкретної статистики даного виду злочину.

Ключові слова: кіберзлочинність, статистична класифікація злочинів, латентність кіберзлочинів, віктимізація кіберзлочинів

CHARACTERISTIC AND IMPORTANCE OF INTERNATIONAL CYBER CRIME STATISTICS

V.I. Trapeznikov

Odesa National Polytechnic University,
1 Shevchenko Str., Odesa, 65044, Ukraine; e-mail: comandor1949@yandex.ua

Cyber crime statistics is discussed based on the sources from the USA from the standpoint of its importance in assessing the crime status and trends (involving quantitative and other indicators) and to determine the most problematic areas in combating these crimes. It is shown that without thorough investigation of the statistics of cyber crimes, it is impossible to organize the participants of combat actions and to state their tasks in a proper way for elimination of these crimes.

Keywords: cyber crimes, statistical classification of crimes, latency of cyber crimes, victimization of cyber crimes.

ОРГАНИЗАЦИЯ ВОЗМОЖНОСТИ САМОВЫРАЖЕНИЯ СТУДЕНТОВ ПРИ ИЗУЧЕНИИ ДИСЦИПЛИНЫ «ПРОГРАММИРОВАНИЕ И ПОДДЕРЖКА ВЕБ- ПРИЛОЖЕНИЙ»

Л.В. Скакун

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

В статье рассматриваются вопросы, связанные с возможностью самовыражения студентов при изучении дисциплины «Программирование и поддержка веб-приложений» для повышения эффективности обучения.

Ключевые слова: самовыражение, веб-программирование, веб-дизайн, обучение веб-программированию.

Введение

Дисциплина «Программирование и поддержка веб-приложений» является одной из нормативных учебных дисциплин учебно-профессиональной программы подготовки бакалавров отраслевого стандарта высшего образования Украины по направлению подготовки «Информатика». Задачи изучения дисциплины достаточно обширны и включают в себя формирование и обобщение специальных знаний и навыков студентов по вопросам создания приложений для глобальной сети Интернет, что обобщенно принято называть веб-программированием. В статье будут рассмотрены составляющие процесса обучения дисциплине «Программирование и поддержка веб-приложений», дающие студентам возможность полноценного самовыражения, что существенно повышает эффективность изучения этой дисциплины.

Основная часть

Веб-программирование – частный случай программирования клиент-серверного приложения, в котором клиентом выступает Интернет-браузер, а сервером – веб-сервер. От обычного программирования веб-программирование отличается, в первую очередь, контекстом исполнения, а также взаимодействием различных компонентов.

В качестве составляющих веб-программирования обычно выделяют: веб-дизайн, кодирование страниц и программирование на стороне клиента или сервера. Процесс кодирования и программирования полностью стандартизован, при изучении данного материала, в большинстве случаев, теряется личность студента, его особенности, предпочтения, увлечения, у него нет возможности выразить себя [1]. Веб-дизайн – эта составляющая веб-программирования, в процессе изучения и реализации которой учащиеся получают возможность для полноценного самовыражения.

Проблема самовыражения анализируется, например, в работах А. С. Косоговой, которая рассматривает этот вопрос в контексте выделения процессов самовыражения личности как значимого фактора в ее личностном и профессиональном становлении.

Под самовыражением она понимает стремление человека (студента) передать другим то, что значимо и ценно для него самого. Это стремление «всегда было объективно необходимым условием его жизни как на уровне физического выживания, так, позднее, и в решении им задач духовного плана» [2, с.6]. Оно является неотъемлемой характеристикой человека, сопровождающей его на протяжении всей жизни и демонстрирующейся вовне с помощью самопрезентаций и самопроявлений. При этом для самопроявлений характерна внешняя направленность, основанная на внутренней сущности человека, и неотделимая от нее.

Одной из задач преподавателя для эффективного обучения веб-программированию является возможность создания условий, позволяющих студенту относиться к программированию веб-приложений как к процессу, осуществление которого приносит, с одной стороны, вполне конкретные, а с другой – личностно-значимые результаты.

Простор для самовыражения при работе над дизайном веб-приложений, проектируемых при изучении дисциплины «Программирование и поддержка веб-приложений», очень широк. Под понятием «веб-дизайн» понимают вид графического дизайна, направленного на разработку и оформление объектов информационной среды интернета, призванного обеспечить им высокие потребительские свойства и эстетические качества. Подобная трактовка отделяет веб-дизайн от веб-программирования, подчеркивает специфику предметной деятельности веб-дизайнера, а также позиционирует веб-дизайн как вид графического дизайна [3]. Тем не менее, несмотря на то, что веб-дизайн имеет в своей основе графическую составляющую, он существенно отличается от полиграфического дизайна. В первую очередь, это обусловлено динамичностью и интерактивностью визуального образа веб-страницы. Любая веб-страница содержит гиперссылки, меню навигации и прочие элементы, обеспечивающие узлы перехода между единицами информации. Эти интерактивные элементы отличают электронные интерфейсы от изданий на бумажных носителях.

Процесс обучения веб-дизайну требует непрерывного отслеживания изменений тенденций в области информационных технологий. Существует постоянная необходимость изучения современных как технических, так и программных средств, применяемых в веб-программировании.

Теоретические и практические основы веб-дизайна освещаются в работах Д.Кирсанова, который обозревает этот процесс в контексте «философии дизайна» [4]. Автор рассматривает процесс веб-дизайна как работу с абстрактными материалами, такими как размер, форма, цвет, текстура и шрифт с помощью принципов единства, баланса, контраста, динамики и нюансировки. В своей книге «Веб-дизайн» Кирсанов акцентирует внимание на необходимости для разработчика веб-проекта проведения самостоятельного теоретического анализа, критики и разбора чужих работ. Согласно ему, обладая определенными знаниями, веб-разработчику необходимо постоянно экспериментировать как с чужими работами, так и с собственными проектами для развития художественных способностей. Д.Кирсановым был введен термин «информационный дизайн», определяющийся как сочетание дизайна полиграфической продукции (книг и журналов), дизайна интерактивных компьютерных программ, дизайна рекламы, теле- и видеопродукции. Его главное назначение – помогать потребителю воспринимать и усваивать некую информацию. Отличие же дизайна от других визуальных искусств заключается в том, что дизайнер использует в своей работе, а нередко и кладет в ее основу, не им созданные художественные ценности. В профессиональном дизайне используются покупные фотографии, заказная графика, шрифты и т.п. Как и в других областях массового производства, разделение труда дает наилучшие результаты: скомпоновав работу профессионального фотографа, профессионального художника и профессионального автора текста, дизайнер обычно получает лучший результат, чем если бы всем от начала до конца пришлось заниматься

ему одному. Помимо информационного дизайна, освещаемого в работе Кирсанова, в задачу веб-дизайнера входит проектирование интерфейса веб-приложения, что подразумевает проектирование взаимодействия. Ниже приведено подробное раскрытие этого понятия.

В современном информационном мире люди постоянно работают с программным обеспечением. Исторически так сложилось, что сложные механические устройства требовали серьезной подготовки операторов для управления ними. Большие машины надежно охранялись, и доступ к ним имели только подготовленные профессионалы. Информационная эра изменила такой подход, и сегодня рядовой пользователь может справиться со сложнейшими технологиями. Одним из самых ярких примеров этого является Интернет, когда посетитель сайта может пользоваться сайтом совершенно без предварительной подготовки. Именно такой подход к разработке интерфейса веб-приложений требуется от веб-разработчика: посетитель веб-сайта должен понять, как пользоваться веб-приложением, как взаимодействовать с ним, всего через несколько секунд после первого посещения веб-страницы.

Современные инженеры впервые столкнулись с проблемой, которая качественно отличается от всех проблем индустриальной эры. За неимением лучшего термина, эта проблема получила название «когнитивное сопротивление». Когнитивное сопротивление – это сопротивление, с которым сталкивается человеческий интеллект, пытаясь разобраться в сложной системе динамически изменяющихся правил. Взаимодействие с программами имеет высокий показатель когнитивного сопротивления по сравнению с взаимодействием человека с физическими устройствами, которые, несмотря на свою сложность, имеют ограниченное количество состояний в сравнении с количеством внешних действий.

Хотя система World Wide Web имеет достаточно простые интерфейсы, тем не менее, они вынуждают пользователей затрачивать больше энергии на восприятие информации с экрана, чем любой механизм. В информационной сети, основанной на гипертексте, каждая ссылка является переходом в другое место в сети, и когнитивное сопротивление возникает именно благодаря гиперсвойствам WWW. Следовательно, одной из основных задач веб-разработчика является создание веб-интерфейсов, обладающих высоким уровнем юзабилити. Юзабилити – это комбинация факторов, влияющих на удобство пользования веб-сайтом. При хорошем юзабилити снижается уровень когнитивного сопротивления, и пользователь при серфинге по сайту чувствует себя комфортно и не допускает ошибок. Важность юзабилити можно определить цитатой из книги признанного во всем мире специалиста в области интерфейсов и удобства эксплуатации Якоба Нильсена: «Изучение поведения пользователей в вебе показывает, что они плохо воспринимают медленные сайты и сайты со сложным дизайном. Люди не хотят ждать. Также они не хотят изучать, как пользоваться домашней страницей. Не существует таких вещей, как обучение веб-сайту или инструкции по веб-сайта. Люди хотят ухватить функциональность сайта сразу же после беглого сканирования страницы, то есть за несколько секунд». Именно таким принципом должны руководствоваться веб-разработчики при проектировании интерфейсов будущего веб-приложения.

Весь процесс создания программного обеспечения пронизан проектированием, и именно при проектировании интерфейса разработчик передает свое личностное отношение к тому, как именно будет выглядеть и работать приложение.

Задачей преподавателя при обучении веб-дизайну является указать студенту, какие элементы интерфейса должны присутствовать в проектируемой системе в соответствии с существующими стандартами. Задачей же студента является самостоятельное проектирование элементов программы, которые должны действовать и передавать информацию, и определение того, как они будут реализованы в том или ином приложении. Самовыражение студентов происходит с помощью отражения их

представления о будущем приложении с учетом требований, предъявляемых к информационному дизайну и юзабилити веб-проекта.

Процесс проектирования веб-приложения, как и любой другой информационной системы, осуществляется поэтапно, и включает в себя, в общем случае, такие шаги:

- Определение цели веб-сайта. Рамки будущего проекта определяются стратегией сайта. На этом этапе определяется не только то, что получают от веб-сайта его владельцы, но также то, что должны получить пользователи;
- Описание вариантов использования сайта. На этом этапе создается список и описание персонажей (моделей пользователей) и действий, которые будут выполняться персонажами на сайте;
- Описание сценариев. На этом этапе определяется бизнес-логика веб-проекта, необходимо описать сценарии для персонажей, для программного обеспечения;
- Определение информационной структуры. Информационная структура определяет, каким образом различные функции и материалы сайта, наличие которых определялось на предыдущих этапах проектирования, будут соотноситься между собой.
- Разработка схемы. На этом этапе определяется конкретное изображение абстрактной структуры сайта;
- Определение внешнего вида сайта. Здесь определяется, какую функциональность будут нести отображаемые на страницах сайта изображения и текст;
- Подготовка текстового и другого наполнения сайта. На этом этапе осуществляется подготовка текстовых, графических, видео- и аудио-материалов, которые будут использоваться для наполнения веб-сайта;
- Кодирование и программирование. На этом этапе разработчик, имея проект веб-сайта, определенного всеми предыдущими этапами, создает HTML-код, программный код и шаблоны веб-сайта.

Проектирование веб-сайта – процесс творческий. На каждом из перечисленных этапов, за исключением последнего, от разработчика требуется креативный подход. От разработчика зависит выбор поведения, назначения, информации, предназначенного для пользователей представления этих аспектов. Благодаря возможности выбора, необходимости принятия решения касательно каждого этапа проектирования веб-приложения, отсутствия готовых шаблонов для принятия решений у разработчика (студента) появляется возможность самовыражения при разработке веб-проекта.

При изучении особенностей веб-технологий в задачу преподавателя входит объяснение учащимся, что при проектировании информационной структуры веб-приложения следует придерживаться наличия определенных обязательных и второстепенных элементов. Возможностью для самовыражения обладает осуществление выбора студентами элементов информационной структуры разрабатываемого ими веб-сайта. Студент сам определяет, какие из этих элементов он будет использовать, какое графическое оформление он выберет для используемых элементов, каким будет расположение этих элементов. Студент самостоятельно решает, каков будет объем, детальность информации, каково будет оформление, расположение отдельных элементов интерфейса, руководствуясь своим личностным восприятием.

К примеру, при визуальном оформлении навигационной структуры студент должен выбрать, будет ли меню в горизонтальном или вертикальном исполнении, будут ли ссылки статичными или в виде выпадающих ссылок, будут ли ссылки простыми текстовыми или графическими. Также студент может решить использовать вместо обычного меню навигацию, выполненную в виде ярлыков, переключателей, кнопок, а также определить глубину навигации. Таким образом, созданное веб-приложение будет результатом творческой деятельности студента, в которой он получает возможность раскрыться, выразить самого себя, предъявить другим людям (пользователям веб-приложения) свои ценности и предпочтения. С точки зрения эффективности обучения, предоставление возможности самовыражения студентов при

выполнении поставленных задач побуждает студента к активности. Проектирование веб-приложения осуществляется через развертывание, развитие и совершенствование качеств и способностей личности [5]. Кроме того, для наиболее успешного выполнения поставленных задач, а именно разработки веб-приложения, студенту необходимо в самовыражении ориентироваться не только на себя, но и на других людей, что формирует культуру самовыражения в профессиональной деятельности.

Вывод

Таким образом, можно сделать вывод, что при изучении дисциплины «Программирование и поддержка веб-приложений» у студентов появляется возможность продемонстрировать свою внутреннюю позицию по отношению к себе, по отношению к другим людям (пользователям веб-приложения), то есть имеются возможности и условия для самовыражения. Задачей преподавателя является лишь направление деятельности студентов. Возможность самостоятельного выбора пути реализации своей деятельности способно привлечь интерес студентов к разработке веб-приложений и повысить качество соответствующих работ.

Список литературы

1. Омельченко, Е.А. Возможности самовыражения студентов в ходе научно-исследовательской деятельности / Е.А. Омельченко // Международный журнал экспериментального образования. – 2010. – №11. – С. 126-128.
2. Косонова, А.С. Становление педагога: монография / А.С. Косонова. – Иркутск: Изд-во Иркут. Гос. Пед. Ун-та, 2001. – 178 с.
3. Бородаев, Д.В. Веб-сайт как объект графического дизайна: монография / Д.В. Бородаев. – Х.: «Септима ЛТД», 2006. – 288 с.
4. Кирсанов, Д. Веб-дизайн / Д. Кирсанов. – СПб: Символ-Плюс, 1999. – 376 с.
5. Абульханова-Славская, К.А. Типология активности личности в социальной психологии / К.А. Абульханова-Славская // Психология личности и образ жизни / Е.В. Шорохова. – М.: Наука, 1987. – 220 с.

ОРГАНІЗАЦІЯ МОЖЛИВОСТІ САМОВИРАЖЕННЯ СТУДЕНТІВ УНІВЕРСИТЕТУ ПРИ ВИВЧЕННІ ДИСЦИПЛІНИ «ПРОГРАМУВАННЯ ТА ПІДТРИМКА ВЕБ-ЗАСТОСУВАНЬ»

Л.В. Скакун

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: lor-chik@list.ru

У статті розглядаються питання, пов'язані з можливістю самовираження студентів при вивченні дисципліни «Програмування та підтримка веб-застосувань» для підвищення ефективності навчання.

Ключові слова: самовираження, веб-програмування, веб-дизайн, навчання веб-програмуванню.

ORGANIZATION OF OPPORTUNITY FOR STUDENT SELF-EXPRESSION WHEN STUDYING «WEB APPLICATION PROGRAMMING AND SUPPORT» DISCIPLINE

L.V. Skakun

Odesa National Polytechnic University,
1 Shevchenko Str., Odesa, 65044, Ukraine; e-mail: lor-chik@list.ru

The paper discusses the issues related to opportunities for student self-expression when studying Web Application programming and Support to improve the study efficiency.

Keywords: self-expression, Web Application programming, web design, web programming teaching.

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ФІЛЬТРАЦІЙНИХ ПРОЦЕСІВ ГАЗОНАСИЧЕНИХ НЬЮТОНІВСЬКОЇ ТА НЕНЬЮТОНІВСЬКОЇ РІДИН В ЗОНІ ТИСКУ НАСИЧЕННЯ

В.С. Савіч, О.О. Ошовська

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: savichsp@gmail.com

Виконано теоретичні дослідження умов тотожності фільтраційних процесів в пористих середовищах ньютонівських та неньютонівських газонасичених рідин. Отримано вирази, що визначають масові витрати вказаних рідин при гомогенному та гетерогенному механізмах фільтраційного плинку.

Ключові слова: пористе середовище, фільтрація, ньютонівська рідина, не ньютонівська рідина, газонасиченість, витрата газонасиченої рідини.

Вступ

Аналіз літератури [1-4], присвяченої питанням дослідження процесу фільтрації газованої рідини, дозволяє зробити наступні висновки: газувана рідина при тиску вище тиску насиченості має нелінійну стискуваність; при стаціонарній фільтрації газованої рідини у пористому середовищі спостерігається значне збільшення витрати рідини неподалік (вище) тиску насичення; ефект збільшення витрати рідини зменшується з ростом проникності (або середнього радіусу капіляра) пористого середовища; залежність рухомості рідини та витрати рідини, приведеного до витрати за Дарсі (відносна витрата) від рівня тиску вище тиску насичення, має немонотонний характер; із зростанням газонасиченості рідини ефект збільшення витрати зростає; основні закономірності стаціонарного плинку газуваних ньютонівських рідин справедливі також і для не ньютонівських.

В даному випадку спостерігається ефект наближення властивостей плинку ньютонівської та неньютонівської рідин при фільтрації у пористому середовищі, що потребує дослідження меж даної тотожності.

Мета роботи

Теоретичне дослідження умов тотожності фільтраційних процесів ньютонівської та неньютонівської рідин, зумовлених явищем газонасиченості рідини при наближенні до тиску насичення.

Основна частина

Для пояснення зазначених висновків аналізу дослідимо механізм утворення зародків, а саме: гомогенний або гетерогенний.

1. Гомогенний механізм. Будемо вважати, що утворення зародків відбувається, в основному, у всьому об'ємі рідкої фази.

Дослідимо за даних умов тотожність фільтраційних плинів ньютонівської та неньютонівської рідин. Сліди поверхнево-активних речовин (ПАР), які майже завжди присутні при фільтраційному русі [1], та поверхневий електричний заряд [2] стабілізують зародок газу, однак поверхня розділу «рідина – зародок газу» ще зберігає рухомість [3] (тобто зародки є такими, що деформуються), в результаті чого газувана рідина набуває стискуваності, яка зростає з наближенням до тиску насиченості, зважаючи на зростання об'ємного вмісту зародків. З примусовим додаванням ПАР її кількість на поверхні зародка зростає, з огляду на що рідина втрачає рухомість [4], а стискуваність системи при інших рівних умовах стає меншою.

Розглянемо тепер як наявність нелінійної стискуваності відбивається на характеристиках витрати при фільтрації газуваної рідини в пористому середовищі. За визначенням [5] коефіцієнт стискуваності $\beta(P)$ віднаходиться з рівняння

$$\frac{1}{\rho} \frac{d\rho}{dP} = \beta(P), \quad (1)$$

де ρ – густина рідини, що фільтрується (з урахуванням обох фаз: газової та рідинної); P – внутрішньо пластовий тиск, який спричиняє фільтраційний рух.

Приймемо, що в першому наближенні, функція стискуваності може бути представлена у адитивній формі

$$\beta(P) = \beta_1 + (\beta_c - \beta_1) \exp[-\alpha(P - P_c)], \quad (2)$$

де β_1 та β_c відповідно мінімальне (при $P \gg P_c$) і максимальне (при $P = P_c$) значення коефіцієнта стискуваності.

Підставляючи в (1) форму (2), отримаємо

$$\rho = \rho_c \exp[\beta_1(P - P_c)] \exp\{[(\beta_c - \beta_1)/\alpha][1 - \exp(\alpha(P - P_c))]\}, \quad (3)$$

де ρ_c – густина газуваної рідини при P_c . Підекспоненціальний вираз другої експоненти при підстановці наступних експериментальних даних: $\alpha = 10^{-6} \text{ 1/Па}$, $P - P_c = 10^6 \text{ Па}$, $\beta_c - \beta_1 = 5 \cdot 10^{-6} \text{ 1/Па}$ стає близьким до нуля ($\approx 10^{-4}$), тому (3) може бути спрощено:

$$\rho = \rho_c \exp[\beta_1(P - P_c)]. \quad (4)$$

Формула (4) показує, що для плин у газуваної рідини можна використовувати модель «надстислої» рідини Маскета [6], яка вміщує поряд з (4) ще й наступне

рівняння: $\frac{\partial^2 P}{\partial x^2} = \frac{m \beta_1 \eta}{k} \frac{\partial \rho}{\partial t}$, де m – пористість, η – в'язкість, k – проникність.

Для стаціонарного плин у газуваної рідини при постійному перепаді тиску масова витрата має вигляд:

$$Q = Q_c ((\rho_0 - \rho_c) / \beta_1 \rho_c (P_0 - P_c)), \quad (5)$$

де ρ_0 та ρ_c – густина газуваної рідини відповідно на вході та виході пористого середовища; Q_c – масова витрата рідини, яка не стискається, з густиною ρ_c , яка

(витрата) визначається з виразу $Q = Q_c(k \rho_c F / (\eta l))(P_0 - P_c)$, де F, l – відповідно площа поперечного перетину та довжина зразку пористого середовища.

Після перетворень (при $P_0 - P_c \ll (1/\beta_1)$), формулу (5) можна привести до виду $Q = Q_c[1 + \beta_1(P_0 - P_c)]$, де $P = (P_0 - P_c)/2$. Приймаючи за результатами експерименту для $\beta_1 = 5 \cdot 10^{-10}$ 1/Па, а для $P - P_c \approx 2 \cdot 10^6$ Па, отримаємо $\beta_1(P - P_c) \approx 10^3$.

Таким чином, стискуваність практично не впливає на витратні характеристики при фільтрації газованої рідини в пористому середовищі.

2. Гетерогенний механізм. Відомо, що зародки нової фази, в основному, утворюються на існуючих поверхнях [7]. У випадках, які розглядаються, цю роль виконує, наприклад, геометрична структура пористого середовища. Дійсно, роботу гетерогенного утворення зародків може бути визначено із співвідношення [8, 9]

$$W_h/W = f(\theta), \quad (6)$$

де W – робота гомогенного утворення зародків газової фази, $f(\theta)$ – функція крайового кута змочування рідиною твердої поверхні [8]:

$$f(\theta) = 0.25 \cdot (1 + \cos \theta)^2 (2 - \cos \theta). \quad (7)$$

Підставляючи (7) в (6), після перетворення, отримаємо: $W_h/W = 0.5 + 0.75 \cdot \cos \theta - 0.25 \cdot \cos^3 \theta$.

Із наведеного рівняння видно, що при $0^\circ < \theta \leq 180^\circ$ робота гетерогенного процесу завжди менше роботи гомогенного процесу. З покращенням змочуваності, що може досягаться додаванням, зокрема аніонної ПАР, робота гетерогенного утворення зародків збільшується, тобто зменшується ймовірність їх утворення.

Прийmemo, що зародки газу, які утворюються (суть – адсорбуються [10]) на поверхні капілярів, рухомі. В результаті пристінний шар рідини, який насичено зародками газу, має меншу в'язкість, аніж центральний. Природно уявити, що при зниженні тиску до тиску насичення, з огляду зменшення роботи утворення зародків, об'ємний вміст їх збільшується, що може привести до збільшення товщини пристінного шару зниженої в'язкості.

Розглянемо рух газорідинної системи в одиничному капілярі та скористаємося результатами робіт [11, 12], в яких, на основі принципу максимуму Понтрягіна отримано функцію $h(c) = [\rho(c)/2\eta(c)] + [A/(1-r^2)]c$, де $\rho(c)$, $\eta(c)$ – відповідно функції густини та в'язкості від концентрації газу. Відшукується такий розподіл концентрації по радіусу капіляра $c(r)$, який забезпечує максимум функції $h(c)$ та, відповідно, витрати рідини. Враховуючи [12], A – постійна, причому $A \in [0; \infty)$, $r \in [0; 1]$, $c \in [0; 1]$.

Для функції густини від концентрації $\rho(c)$ можна прийняти відоме співвідношення $\rho(c) = 1 - c$. Для функції в'язкості від концентрації $\eta(c)$ відповідно до [13], приймаємо $\eta(c) = c(1 - \lambda)$ ($1/3 < \lambda < 1$) – для високих та середніх концентрацій, та $\eta(c) = c\lambda$ ($0 < \lambda < 1/6$) – для відносно низьких концентрацій.

Вочевидь, для розподілу концентрації, який доставляє максимум витраті рідини:

$$c_m(r) = \begin{cases} 0, & 0 \leq r < \sqrt{1 - 2A/(1-\lambda)}, \\ \frac{1}{\lambda} - \frac{1}{\lambda} \sqrt{(1-\lambda)(1-r)^2(2A)^{-1}}, & \sqrt{1 - 2A/(1-\lambda)} < r < 1. \end{cases} \quad (8)$$

Середня концентрація газу, відповідно до [12], визначається із співвідношення

$$F = \int_0^1 c_m(r) r dr = \frac{A}{3\lambda(1-\lambda)}.$$

Вказаний розподіл концентрації за перетином (8) буде мати місце при $A \in (0; (1-\lambda)/2)$ та $F \in (0; 1/6\lambda)$.

Зазначимо, що при відносно високих концентраціях газу, коли має місце двофазний плин, можливо, як показано в [12], утворення пристінного газового шару.

Таким чином, максимізація витрати відбувається при розшаруванні газорідинної системи, коли в центрі плине чиста рідина, а біля стінок рідина із зародками газу (тобто система з меншою в'язкістю аніж у центрі потоку). Очевидно, що відносно малий пристінний шар, насичений гетерогенними зародками газу, який виділився, буде мати значно меншу в'язкість, ніж чиста рідина, в той час як об'ємна в'язкість газованої рідини при наявності зародків газу, відповідно до [1], зменшується лише на (10...15)%.

3. Кільцева схема плин у капілярі. Розглянемо особливості плин у пористому середовищі ньютонівської та не ньютонівської рідин.

Ньютонівська рідина. Для визначення витрати в теоретичних підрахунках можна застосувати кільцеву схему руху в капілярі, запропоновану в [14]. Тоді швидкість стаціонарного плин флюїдів в капілярі визначиться з рівняння

$$v_i = -(\Delta P / (4l \eta_i)) r^2 + a_{1i} \ln r + a_{2i}, \quad (9)$$

де $\Delta P / l$ – градієнт тиску, η_i – в'язкість флюїда (для центрального флюїда приймемо індекс 1, для пристінного – індекс 2). Постійні a_{1i} та a_{2i} визначаються з наступних

граничних умов: $v_2 = 0$, $r = R$, $\eta_2 \frac{dv_2}{dr} = \eta_1 \frac{dv_1}{dr}$, $v_1 = v_2$, $r = R_0$, $\frac{dv_1}{dr} = 0$, $r = 0$.

З (9) при вказаних граничних умовах визначається швидкість

$$v_1 = \left(\Delta P R^2 / (4 \eta_1 l) \right) \left[(R_0/R)^2 - (r/R)^2 + \varepsilon (1 - R_0^2/R^2) \right] \quad (10)$$

та відносна витрата рідини $Q_1 = Q/Q_0 = S^4 \left[1 + (2\varepsilon/S^2)(1-S^2) \right]$, або

$$Q_1 = (1-\xi)^4 \left[1 + 2\varepsilon \xi (2-\xi) / (1-\xi)^2 \right], \quad (11)$$

де $S = R_0/R = 1-\xi$, $\xi = \delta/R$, $\varepsilon = \eta_1/\eta_2 > 1$, Q_1 – витрата для рідини з в'язкістю η_1 . Перехід до пористого середовища в даному випадку не змінить результату, якщо прийняти (11) як відносну проникність, виражену у термінах витрати. Аналіз виразу (11) показує, що залежність витрати рідини від товщини пристінного шару має немонотонний характер, причому максимум витрати настає при

$$\xi = 1 - \sqrt{\varepsilon(2\varepsilon - 1)}^{-1}. \quad (12)$$

Немонотонність витрати визначається добутком $(1-\xi)^4 \times [2\varepsilon \xi (2-\xi) / (1-\xi)^2]$. Перший множник характеризує площину поперечного перетину потоку рідини, другий – внесок пристінного шару зниженої в'язкості у збільшення витрати рідини. За відносно низької товщини пристінного шару переважає другий множник, і витрата рідини збільшується. За відносно високої товщини пристінного шару переважає перший множник, і витрата рідини зменшується.

Неньютонівська рідина. Розглянемо кільцевий плин в капілярі неньютонівської (степеневі) рідини з пристінним шаром газу. Швидкість руху рідини в капілярі, враховуючи, що при $r=0$ напруження τ повинно бути кінцевою величиною, визначається з рівняння [6]:

$$v_1 = -(n/(n+1))(\Delta P/(2\eta_0 l))^{1/n} r^{(1/n)+1} + a_{2i}, \quad (13)$$

а швидкість плинну пристінного шару газу з рівняння

$$v_2 = -(\Delta P/(4\eta_2 l))r^2 + a_{1i} \ln r + a_{2i}, \quad (14)$$

де η_0 – постійна величина ($\eta_0 = \tau/\gamma^n$). Постійні інтегрування визначаються із наступних граничних умов: $v_2 = 0$, $r = R$, $\tau_1 = \tau_2$, $v_1 = v_2$, $r = R_0$.

Тоді з (13) та (14) визначається швидкість плинну

$$v_1 = (n/(n+1))(\Delta P/(2\eta_0 l))^{1/n} R_0^{(1/n)+1} \left[1 - (r/R_0)^{(1/n)+1} \right] + ((\Delta P R^2)/(4\eta_2 l)) \left[1 - (R_0/R)^2 \right], \quad (15)$$

а з (15) відносно витрату рідини

$$Q_1 = Q/Q_0 = (1-\xi)^{(1/n)+3} \left[1 + (3(n+1)/(2n)) \cdot (\varepsilon \xi (2-\xi)/(1-\xi)^2) \right], \quad (16)$$

$$\varepsilon = \eta_1/\eta_2, \quad \eta_1 = \eta_0 ((\Delta P R_0)/(2\eta_0 l))^{1-(1/n)}, \quad (17)$$

де η_1 – в'язкість рідини при $r = R_0$, тобто на межі поділу рідини та газу,

$$Q_0 = \frac{\pi n}{3n+1} \left(\frac{\Delta P R_0}{2\eta_0 l} \right)^{1/n} R^{(1/n)+3} - \text{витрата степеневі рідини з в'язкістю } \eta_1 = \eta_0 \left(\frac{dv_1}{dr} \right)^{n-1}.$$

При $n=1$ рівняння (15) та (16) переходять відповідно в рівняння (10) та (11). Аналіз виразу (16) показує, що залежність витрати рідини від товщини пристінного шару також має немонотонний характер, причому максимум витрати настає при

$$\xi = 1 - \sqrt{((n+1)\varepsilon)/((3n+1)\varepsilon - 2n)}. \quad (18)$$

При $n=1$ рівняння (18) переходить в рівняння (12). Аналіз виразу (18) показує, що зі зростанням n (за інших рівних умов) ξ зростає.

Немонотонність витрати за вище описаних причин визначається добутком $(1-\xi)^{(1/n)+3} \times \left[1 + (3(n+1)/(2n)) \cdot ((\varepsilon \xi (2-\xi))/(1-\xi)^2) \right]$, причому «внесок» кожного із добутоків аналогічний відповідному як і у випадку ньютонівської рідини.

Висновок

Отримано і досліджено умови тотожності фільтраційних процесів ньютонівської та неньютонівської рідин, зумовлених явищем газонасиченості рідини в зоні, наближеній до тиску насичення. Запропоновано вирази, які описують витрату рідини при зародках газової фази у пристінковому шарі для гомогенного та гетерогенного механізмів фільтраційного плинну.

Список літератури

1. Бувейч, Ю.А. О докритическом образовании зародышей в жидкости с поверхностно-активным веществом (ПАВ) / Ю.А. Бувейч // Инженерно-физический журнал. – 1987. – Т. 52, № 5. – С. 394-402.
2. Сулейманов, Б.А. Влияние поверхностно-активного вещества на неравновесные эффекты в газожидкостных системах в докритической области / Б.А. Сулейманов, Ф.Б. Нагиев // Инженерно-физический журнал. – 1995. – Т. 68, № 6. – С. 968-974.
3. Сиротюк, М.Г. Стабилизация газовых пузырьков в воде / М.Г. Сиротюк // Акустический журнал. – 1970. – Т. 16, № 4. – С. 567-569.
4. Dammer, S.M. Gas enrichment at liquid-wall interfaces / S.M. Dammer, D. Lohse // Physical Review Letters. – 2006. – Vol. 96. – PP. 2257-2264.
5. Бернадинер, М.Г. Гидродинамическая теория фильтрации аномальных жидкостей / М.Г. Бернадинер, В.М. Ентов. – М.: Наука, 1979. – 199 с.
6. Tretheway, D. Effects of absolute pressure on fluid-solid interface / D. Tretheway // Physical Review Letters. – 1999. – Vol. 82. – PP. 1671-1674.
7. Фольмер, М. Кинетика образования новой фазы / М. Фольмер. – М.: Мир, 1986. – 208 с.
8. Корнфельд, М. Упругость и прочность жидкостей / М. Корнфельд. – М.-Л.: Энергия, 1975. – 108 с.
9. Хирс, Д. Испарение и конденсация / Д. Хирс, Г. Паунд. – М.: Metallurgia, 1966. – 200 с.
10. Михайлов, Д.Н. О влиянии адсорбции-десорбции микророзышей газа на характер фильтрации газированной жидкости / Д.Н. Михайлов, Г.С. Степанова // Изв. РАН. Механика жидкости и газа. – 2003. – № 5. – С. 106-114.
11. Павловский, Ю.Н. О пристеночном эффекте / Ю.Н. Павловский // Изв. АН СССР. Механика жидкости и газа. – 1967. – № 2. – С. 160-165.
12. Эфрос, Д.А. Исследование фильтрации неоднородных систем / Д.А. Эфрос. – Л.: Энергия, 1978. – 351 с.
13. Сатаров, Р.М. Исследование движения газожидкостных систем с учетом образования микророзышей / Р.М. Сатаров, П.Я. Фарзани // Инженерно-физический журнал. – 1987. – Т. 52, № 5. – С. 765-771.
14. Blake, T.D. Slip between a liquid and a solid theory reconsidered / T.D. Blake // Colloids and Surfaces. – 1990. – Vol. 47. – P. 135-145.

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ФИЛЬТРАЦИОННЫХ ПРОЦЕССОВ ГАЗОНАСЫЩЕННЫХ НЬЮТОНОВСКОЙ И НЕНЬЮТОНОВСКОЙ ЖИДКОСТЕЙ В ЗОНЕ ДАВЛЕНИЯ НАСЫЩЕНИЯ

В.С. Савич, О.А. Ошовская

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: savichsp@gmail.com

Выполнены теоретические исследования условий тождественности фильтрационных процессов в пористых средах ньютоновских и неньютоновских газонасыщенных жидкостей. Получены выражения, определяющие массовые расходы указанных жидкостей при гомогенном и гетерогенном механизмах фильтрационного течения.

Ключевые слова: пористая среда, фильтрация, ньютоновская жидкость, неньютоновская жидкость, газонасыщенность, расход газонасыщенной жидкости.

MATHEMATICAL MODELING OF FILTRATION PROCESSES OF GAS-SATURATED NEWTONIAN AND NON-NEWTONIAN LIQUIDS IN SATURATION PRESSURE REGION

V.S. Savich, O.O. Oshovska

Odesa National Polytechnic University,
1 Shevchenko Str., Odesa, 65044, Ukraine; e-mail: savichsp@gmail.com

The conditions of identity of filtration of gas-saturated Newtonian and non-Newtonian liquids through porous media were theoretically investigated. The expressions determining mass flow rates of these liquids for homogeneous and heterogeneous filtration were obtained.

Keywords: porous medium, filtration, Newtonian liquid, non-Newtonian liquid, flow rate of gas-saturated liquid.

Алфавітний покажчик авторів
Том 4, 2014

Author Index
Volume 4, 2014

Банах, Р.І.	137	Banach, R.	137
Баранов, П.С., <i>д.т.н.</i>	99	Baranov, P., <i>EngD</i>	99
Бодарев, Д.О.	68	Bodarev, A., <i>PhD</i>	68
Бодарев, О.Д., <i>к.т.н.</i>	68	Bodarev, D.	68
Болтъонков, В.О., <i>к.т.н.</i>	201, 312	Boltenkov, V., <i>PhD</i>	201, 312
Боровік, Б., <i>к.т.н.</i>	111	Borowik, B., <i>PhD</i>	111
Боряк, К.Ф., <i>д.т.н.</i>	126	Boryak, K., <i>EngD</i>	126
Браїловський, М.М., <i>к.т.н.</i>	304	Brailovsky, N., <i>PhD</i>	304
Вербик, К.В.	342	Chaikivska, Iu.	272
Вичужанін, В.В., <i>д.т.н.</i>	225	Chechelnitsky, V., <i>EngD</i>	57; 210
Гайша, О.О., <i>к.т.н.</i>	158	Cicarev, V., <i>PhD</i>	126
Гаранюк, П.І., <i>д.т.н.</i>	324	Contreras, D., <i>PhD</i>	250
Григоренко, Ю.В.	85; 180	Dej, V.	324
Гришин, С.І., <i>к.т.н.</i>	68	Diachenko, P.	239
Дей, В.А.	324	Dudikevich, V., <i>EngD</i>	137, 324
Дудікевич, В.Б., <i>д.т.н.</i>	137, 324	Fomin, A., <i>PhD</i>	219
Дяченко, П.В.	239	Gaisha, A., <i>PhD</i>	158
Єнікєєв, Р.І.	201	Grigorenko, Yu.	85; 180
Зибін, С.В., <i>к.т.н.</i>	304	Grishin, S., <i>PhD</i>	68
Іванченко, Є.В., <i>к.т.н.</i>	256	Haranyuk, P., <i>EngD</i>	324
Івасьєв, С.В.	342	Hochlacheva, Yu.	256
Казаков, А.І., <i>д.т.н.</i>	349	Ivanchenko, Ye., <i>PhD</i>	256
Карпінський, В.М., <i>к.т.н.</i>	111	Ivasiev, S.	342
Кваташидзе, Л.Т.	349	Karpinskyi, V., <i>PhD</i>	111
Кілін, А.С.	332	Kazakov, A., <i>EngD</i>	349
Кобозєва, А.А., <i>д.т.н.</i>	99	Khoroshko, V., <i>EngD</i>	137; 195; 256, 304
Козіна, Ю.Ю., <i>к.т.н.</i>	120	Kilin, A.	332
Кононович, І.В.	35	Kobozeva, A., <i>EngD</i>	99
Контрєрас, Д.Е., <i>к.т.н.</i>	250	Kononovich, I.	35
Кучма, М.С.	332	Kozina, Yu., <i>PhD</i>	120
Кушніренко, Н.І.	210	Kuchma, M.	332
Лебєдєва, О. Ю., <i>к.т.н.</i>	76; 278	Kushnirenko, N.	210
Лєнков, Є.С.	158	Kvatashidze, L.	349
Лєнков, С.В., <i>д.т.н.</i>	126; 158	Lebedeva, H., <i>PhD</i>	76; 278
Мазурков, М.І., <i>д.т.н.</i>	5	Lenkov, E.	158
Мельник, М.О., <i>к.т.н.</i>	44; 99	Lenkov, S., <i>EngD</i>	126; 158
Микитин, Г.В., <i>д.т.н.</i>	137	Mazurkov, M., <i>EngD</i>	5
Мокріцький, В.А., <i>д.т.н.</i>	165	Melnyk, M., <i>PhD</i>	44; 99
Молдавська, О.В.	149	Mikitin, G., <i>EngD</i>	137
Наріманова, О.В., <i>к.т.н.</i>	332	Mokritskyi, V., <i>EngD</i>	165
Нгуєн Гуї Кіонг	312	Moldavskaya, A.	149
Николайчук, Я.М., <i>д.т.н.</i>	342	Narimanova, O., <i>PhD</i>	332
Орєхов, А.М.	195	Nhuen Hui Kionh	312
Ошовська, О.О.	375	Nikolaichuk, Ya., <i>EngD</i>	342
Павленко, В.Д., <i>к.т.н.</i>	14; 105	Orehov, A.	195
Павлов, І.М., <i>к.т.н.</i>	263	Oshovska, O.	375
Пасічник, Р.М., <i>к.ф.-м.н.</i>	272	Pasichnyk, R., <i>PhD in Physics</i>	272
Паулін, О.М., <i>д.т.н.</i>	50	Paulin, O., <i>EngD</i>	50
Положаєнко, С.А., <i>д.т.н.</i>	219; 250, 291	Pavlenko, V., <i>PhD</i>	14; 105
Ракобєвчук, В.О.	324	Pavlov, I., <i>PhD</i>	263
Ребєць, А.І.	137	Polozhaenko, S., <i>EngD</i>	219; 250, 291
Рибальський, О.В., <i>д.т.н.</i>	337	Rakobovchuk, V.	324
Рувінська, В.М., <i>к.т.н.</i>	149	Rebets, A.	137
Рудніченко, Н.Д.	225	Rudnichenko, N.	225

Савіч, В.С.	375	Ruvinskaya, V., <i>PhD</i>	149
Сиропятов, О.А.	57	Rybalsky, O., <i>EngD</i>	337
Скакун, Л.В.	370	Savich, V.	375
Собчук, І.С., <i>к.ф.-м.н.</i>	324	Shapovalov, G.	349
Соколов, А.В.	5	Siropyatov, O.	57
Соловійов, В.І., <i>к.т.н.</i>	337	Skakun, L.	370
Сперанський, В.О.	14	Sobchuk, I., <i>PhD in Physics</i>	324
Тимошенко, Л.М., <i>к.е.н.</i>	165, 342	Sokolov, A.	5
Трапезніков, В.І., <i>к.ю.н.</i>	363	Solovyev, V., <i>PhD</i>	337
Трифонов, К.О.	332	Speransky, V.	14
Турченко, І.В., <i>к.т.н.</i>	173	Timoshenko, L., <i>PhD in Economics</i>	165, 342
Фомін, А.А., <i>к.т.н.</i>	219	Trapeznikov, V., <i>PhD in Law</i>	363
Хорошко, В.О., <i>д.т.н.</i>	137; 195; 256, 304	Trifonova, K.	332
Хохлачова, Ю.Є.	256	Turchenko, I., <i>PhD</i>	173
Цицарєв, В.М., <i>к.т.н.</i>	126	Verbik, K.	342
Чайківська, Ю.М.	272	Vychuzhanin, V., <i>EngD</i>	225
Чечельницький, В.Я., <i>д.т.н.</i>	57; 210	Yakimenko, I., <i>PhD</i>	165
Шаповалов, Г.В.	349	Yaremchuk, Yu., <i>PhD</i>	26, 357
Юхименко, Б.І., <i>к.е.н.</i>	233	Yenikyeyev, R.	201
Якименко, І.З., <i>к.т.н.</i>	165	Yukhimenko, B., <i>PhD in Economics</i>	233
Яремчук, Ю.Є., <i>к.т.н.</i>	26, 357	Zybin, S., <i>PhD</i>	304

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

Том 4, номер 4, 2014. Одеса – 97 с., іл.

ИНФОРМАТИКА И МАТЕМАТИЧЕСКИЕ МЕТОДЫ В МОДЕЛИРОВАНИИ

Том 4, номер 4, 2014. Одесса – 97 с., ил.

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Volume 4, No. 4, 2014. Odesa – 97 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 №4 від 23.12.2014)

Адреса редакції: Одеський національний політехнічний університет,
проспект Шевченка, 1, Одеса, 65044 Україна

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

E-mail: immm.ukraine@gmail.com

Автори опублікованих матеріалів несуть повну відповідальність за підбір, точність наведених фактів, цитат, економіко-статистичних даних, власних імен та інших відомостей. Редколегія залишає за собою право скорочувати та редагувати подані матеріали

© Одеський національний політехнічний університет, 2014