

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеський національний політехнічний університет

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ
МЕТОДИ В МОДЕЛЮВАННІ

INFORMATICS AND MATHEMATICAL
METHODS IN SIMULATION

Том 7, № 3

Volume 7, No. 3

Одеса – 2017
Odesa – 2017

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:

О.Ю. Козлова

Редакційна колегія:

*Т.О. Банах, П.І. Бідюк, Н.Д. Вайсфельд,
А.Ф. Верлань, Г.М. Востров, В.Б. Дудикевич,
М.Б. Копитчук, С.В. Ленков, І.І. Маракова,
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,
С.В. Філіппова, 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 - 6460Р of 04.04.2011

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

Associate editor:

A.A. Kobozeva

Executive editor:

O.Yu. Kozlova

Editorial Board:

*T. Banakh, P. Bidyuk, V. Dudykevich,
V. Khoroshko, N. Kopytchuk,
S. Lenkov, I. Marakova, S. Nesterenko,
N. Nikitchenko, S. Philippova, 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, 2017

ЗМІСТ / CONTENTS

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ
БАГАТОЧАСТОТНОГО ФАЗОВОГО
МЕТОДУ ДАЛЬНОМЕТРІЇ
В.Р. Любчик, А.В. Клепіковський,
Ю.О. Бабій, Є.С. Ленков, В.О. Ковальов

156

MATHEMATICAL MODELLING OF
DISTANCE MEASURING
MULTIFREQUENCY PHASE METHOD
Liubchik V., Klepikovskiy A., Babiy Yu.,
Lenkov E., Kovalev V.

ТЕОРЕТИЧНИЙ РОЗВИТОК
ЗАГАЛЬНОГО ПІДХОДУ ДО
ПРОБЛЕМИ ВИЯВЛЕННЯ
ПОРУШЕНЬ ЦІЛІСНОСТІ ЦИФРОВИХ
КОНТЕНТІВ, ЗАСНОВАНОГО НА
АНАЛІЗІ ПОВНОГО НАБОРУ ЇХ
ФОРМАЛЬНИХ ПАРАМЕТРІВ
І.І. Бобок

170

THEORETICAL DEVELOPMENT OF
THE GENERAL APPROACH TO
SOLVING THE PROBLEM OF
DETECTING THE INTEGRITY
VIOLATIONS OF DIGITAL CONTENT
BASED ON THE ANALYSIS OF A
COMPLETE SET OF FORMAL
PARAMETERS
Bobok I.

ЕКСПЕРИМЕНТАЛЬНЕ
ДОСЛІДЖЕННЯ ПРОГРАМНОЇ
РЕАЛІЗАЦІЇ МЕТОДІВ ПОШУКУ
ОБЕРНЕНОГО ЕЛЕМЕНТА ЗА
МОДУЛЕМ
М.М. Касянчук, І.З. Якименко,
С.В. Івасьєв, О.В. Момотюк

178

EXPERIMENTAL RESEARCH OF
PROGRAM IMPLEMENTATION OF
METHODS OF THE INVERSE
ELEMENT SEARCH BY MODULE
Kasianchuk M., Yakymenko I., Ivasiev S.,
Momotjuk O.

УДОСКОНАЛЕННЯ
СТЕГАНОАНАЛІТИЧНОГО МЕТОДУ
ВИЯВЛЕННЯ ВКЛАДЕНЬ
ДОДАТКОВОЇ ІНФОРМАЦІЇ В
ЦИФРОВИХ ЗОБРАЖЕННЯХ,
ЗАСНОВАНОГО НА АНАЛІЗІ
ПОСЛІДОВНИХ ТРІАД КОЛІРНИХ
ТРИПЛЕТІВ
Г.В. Ахмаметьєва, В.В. Мурова

187 IMPROVEMENT OF THE
STEGANALYTIC METHOD FOR
DETECTING THE ADDITIONAL
INFORMATION ATTACHMENTS IN
DIGITAL IMAGES, BASED ON THE
ANALYSIS OF SEQUENTIAL TRIADS
OF COLOR TRIPLETS
Akhmametieva A., Murova V.

ПРОГНОЗУВАННЯ НАДІЙНОСТІ
ПРОЦЕСУ ФУНКЦІОНУВАННЯ
СКЛАДНИХ СИСТЕМ ТА РИЗИК ЇХ
ВІДМОВИ
В.О. Хорошко, Ю.Є. Хохлачова

195 FORECASTING THE RELIABILITY OF
THE PROCESS OF FUNCTIONING OF
COMPLEX SYSTEMS AND RISK OF
THEIR DISCLAIMER
Khoroshko V., Hohlachova Yu.

ДИНАМІЧНІ ВЛАСТИВОСТІ
ПРОЦЕСІВ ЗАБЕЗПЕЧЕННЯ
КІБЕРБЕЗПЕКИ НА ПРИКЛАДІ
АУДИТУ КІБЕРБЕЗПЕКИ
О.Ю. Козлова, В.Г. Кононович,
І.В. Кононович, М.Г. Романюков,
Л.М. Тимошенко

205 DYNAMIC PROPERTIES OF
PROVIDING OF CYBERSECURITY ON
THE EXAMPLE OF CYBERSECURITY
AUDIT
Kozlova O., Kononovich V.,
Kononovich I., Romanukov M.,
Timoshenko L.

ЗАСТОСУВАННЯ КЛАСТЕРНОГО
АНАЛІЗУ ДАНИХ ДЛЯ ВИДІЛЕННЯ
МІРИ СХОЖОСТІ ФАКТОРІВ
ВПЛИВУ НА ПРАЦЕЗДАТНІСТЬ
СКЛАДНИХ ТЕХНІЧНИХ СИСТЕМ
В.В. Вичужанін, Д.С. Шибасєв,
М.Д. Рудніченко

213 CLUSTER DATA ANALYSIS FOR THE
SIMILARITY MEASURE IDENTIFY OF
THE COMPLEX TECHNICAL
SYSTEMS OPERABILITY FACTORS
Vichuzhanin V., Shibaev D.,
Rudnichenko N.

СИНТЕЗ І МОДЕЛЮВАННЯ
ЦИФРОВОГО ПРИСТРОЮ
УПРАВЛІННЯ ДЛЯ
НЕСТАЦІОНАРНОГО ОБ'ЄКТУ
С.О. Бобріков, Є.Д. Пічугін, М.М. Дикий

220 SYNTHESIS AND SIMULATION OF
DIGITAL
MANAGING DEVICE FOR NON-
STATIONARY OBJECT
Bobrykov S., Pichugin E., Dikiy N.

УПРАВЛІННЯ РИЗИКАМИ ВТРАТ
КОНТРОЛЮ НАД СКЛАДНИМИ
ТЕХНІЧНИМИ СИСТЕМАМИ
В.Д. Бойко

228 RISK MANAGEMENT FOR
SCENARIOS OF LOSS CONTROL
OVER COMPLEX TECHNICAL
SYSTEMS
Boyko V.

ПАРАЛЕЛЬНІ АЛГОРИТМИ
РОЗВ'ЯЗАННЯ ПРОСТОРОВОЇ
ЗАДАЧІ ЦИФРОВОЇ ФІЛЬТРАЦІЇ
ДАНИХ
М. С. Яджак

234

PARALLEL ALGORITHMS FOR
SOLVING THE SPATIAL PROBLEM
OF DATA DIGITAL FILTERING
Yadzhak M.

СЕРВІС-ОРІЄНТОВАНИЙ
ІНФОРМАЦІЙНИЙ РЕСУРС
КАФЕДРИ ВНЗ В ГІБРИДНІЙ
ХМАРНІЙ ІНФРАСТРУКТУРІ
В.Є. Малахов, Л.А. Волощук

240

SERVICE - ORIENTED INFORMATION
RESOURCE OF THE UNIVERSITY
CHAIR IN THE HYBRID CLOUD
INFRASTRUCTURE
Malakhov V., Voloshchuk L.

MATHEMATICAL MODELLING OF DISTANCE MEASURING MULTIFREQUENCY PHASE METHOD

V. Liubchyk¹, A. Klepikovskiy², Yu. Babiy³, E. Lenkov⁴, V. Kovalev⁵

¹ Khmelnytsky National University,

11, Institutskaya Str., Khmelnytsky, 29000, Ukraine; e-mail: vitaly1612@gmail.com;

² Bukovinian state medical university,

2, Theatralna Str., Chernivtsi-city, 58002, Ukraine; e-mail: andrei.klepikovskiy@gmail.com;

³ The National Academy of State Border Guard Service of Ukraine named after Bohdan Khmelnytsky,

46, Shevchenko Str., Khmelnytsky, 29000, Ukraine; e-mail: julscorpio@gmail.com;

⁴ Military Institute of Telecommunications and Informatization,

45/1, Moscow Str., Kyiv, 01011, Ukraine;

⁵ Odessa research institute of television technology,

132, Mechnikova Str., Odessa, 65028, Ukraine

The article is developed algorithm of mathematical modelling of the formation process of the reflected monophonic signal in the presence of several reflection objects has been worked out. The algorithm consists of the following phases: setting the initial values, calculating the vectors values of the monophonic signals as a sum of signals reflected from each object, the vectors change by taking into account the amplitude error, the phase shift and the frequency of the probing signal. The mathematical modelling of the process of the objects distance measuring using multi-frequency phase method has been performed. In the process of modeling we have changed the basic parameters of the probing signal and the monophonic reflected signal, namely: initial frequency, frequency incremental step, frequency instability, amplitude designation error and monophonic signal phase shift error. Monte Carlo method has been applied in the process of modelling. Frequency instability was set according to normal distribution, and the amplitude and phase error were set with uniform distribution. The mathematical modelling of distance measuring using multi-frequency phase method has shown that distance measuring error is decreased if the probing signal frequency instability and the monophonic signal vectors measurement error are reduced. With regard to the abovementioned the mean square deviation of the distance is decreased. Calculations of the distance error coincide with the data obtained by the mathematical modelling. It has been found that it is appropriate, in the process of the objects probing at the depth of 50 meters, to use the frequency incremental step of 4 MHz, where the signal generator frequency instability is at least $10^{-6} f$, the amplitude measurement error is $1/1024 a_{\Sigma max}$, the phase shift measurement error does not exceed 0.1° . In this case, the distance measurement error does not exceed 0.6 m.

Keywords: mobile target, range, radar system, probe signal, rangometry, phase method.

Introduction

The problem of high-precision measurement of distance and radial velocity of moving targets such as surface, air and sea ones is not new. Various radars are used to solve the problem. Different types and kinds of problems can be distinguished depending on the problem to be solved by the radar station. Protection of the state borders turns out the most acute problem. In this case, identification of pinpoint targets at close distances from each other and their identification at considerable distances is undoubtedly a critical task.

The known methods for measuring distances in radar-location mainly use impulse-type signals and signal separation reflected from each object at time of their arrival. In this connection the probing signals which provide sufficient accuracy occupy a significant

frequency range. This creates problems when constructing units of distance-measurement radar systems [1, 2].

The phase methods of distance measuring are the most accurate ones. They allow precision of the target distance measuring provided that the frequency range of probing signals is strictly limited, by virtue of the fact that we use harmonic signals and multi-scale approach [1].

Recently developed distance measuring multi-frequency phase methods allow to separate the signals reflected from many objects using limited frequency range of probing signals and measurements of the reflected signals vectors [1].

The theoretical material and methods of radar measurements can be used to develop fundamentally new radio systems of distance measuring, to measure the radial velocity of targets and conduct radar observation in the military sphere. This is especially true concerning development of radar systems which are to identify targets from each other at short distances in a single line. In order to set the limits of the distance measuring multi-frequency phase method using we have to perform mathematical modelling and specify major dependencies between the probing signals parameters and the parameters of accuracy and discrimination power.

Main body

Determining accuracy and discrimination power of the method is a multidimensional problem, in other words these values depend on many input parameters, namely: initial frequency, spectrum width, frequency incremental step, distance between adjacent objects, amplitude error, phase error. Let us consider the most important parameters that influence the potential accuracy and discrimination power of the method, namely initial frequency and frequency incremental step. The accuracy and discrimination power are important characteristics of distance measuring. They allow, knowing the results permissible accuracy, to set requirements for the measurement conditions, namely frequencies and instruments error. In this case, we consider the error as the difference between the true distance d and the measured one l with reference to the true distance, viz relative error:

$$\delta l = \frac{|d - l|}{d}, \quad (1)$$

where d – true distance; l – measured distance.

Discrimination power is the minimum distance between two adjacent objects Δd , wherein the method allows their identification as two separate objects, rather than as a single one. This can be expressed by the equation:

$$\Delta d = d_2 - d_1, \max(\Delta l_1, \Delta l_2) < \Delta d, \quad (2)$$

where $\Delta l_1, \Delta l_2$ – absolute errors of distances; d_1, d_2 – true distances to the objects.

The formula on the right side is the separability condition: if all absolute errors are less than the real distance between the adjacent objects then we separate them. Let us use mathematical modelling to determine the dependence character of accuracy and discrimination power on the initial frequency and frequency incremental step. To do this we must have the values of the "measured" vectors $\overrightarrow{B}_k$ at each probing frequency. Therefore, we will calculate these vectors analytically, setting the true values of the distances to the objects and the amplitudes of each reflected signal. These operations can be represented in the shape of the flow chart (Fig. 1).

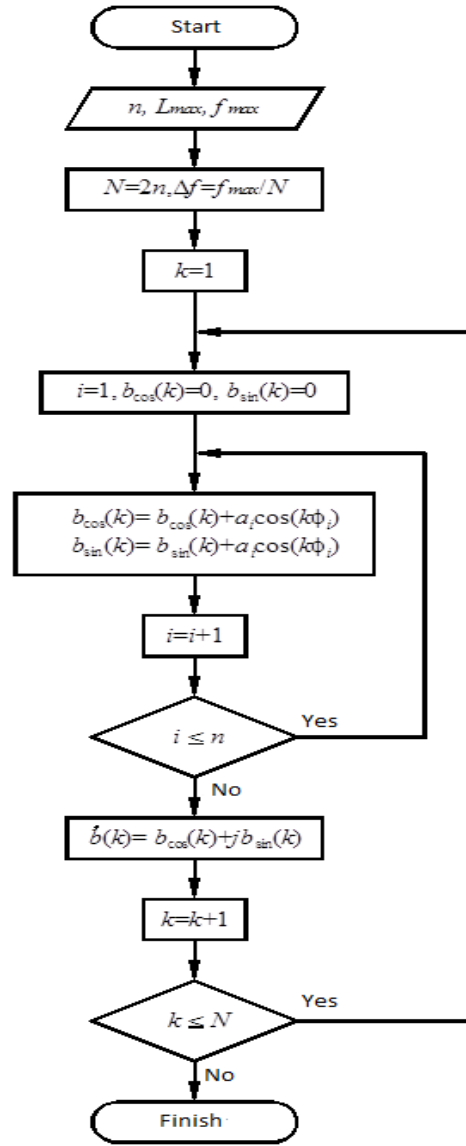


Fig. 1. Control flow chart for calculating vectors $\dot{b}(k)$ for mathematical modelling

According to the flow chart Fig. 1 we calculate the phase shifts of harmonic signals reflected from each object using the following expression:

$$\phi_k = \frac{4 \cdot \pi \cdot d_k \cdot f}{c}, k = 1 \dots n, \quad (3)$$

where n – number of objects; d_k – true distances; f – initial frequency; c – wave-propagation velocity.

Calculation of the vectors of monophonic signals in the complex form is done in the following manner:

$$\dot{b}(k) = \sum_{i=1}^n a_i \cdot \left(\cos(k \cdot \phi_i) + j \cdot \sin(k \cdot \phi_i) \right), k = 1 \dots N, \quad (4)$$

where a_i – true amplitudes of the vectors reflected from each object; inc – frequency incremental step; N – required number of frequencies.

We must take into account the fact that the calculation of the distance will depend on both the initial frequency and the incremental step of probing frequencies variation. The initial frequency is taken into account in the expression (4) by putting it in the calculation of the phase shift.

We use the following expression to take into account the incremental step of frequencies variation:

$$\dot{b}(k) = \sum_{i=1}^n a_i \cdot e^{j \cdot k \cdot inc \cdot \phi_i}, k = 1 \dots N, \quad (5)$$

where *inc* - frequency increment which takes the values from 0 to 1.

So, we have considered all the mathematical operations required for modelling. Before we start modelling, it should be noted that the characteristics under research, namely accuracy and discrimination power, can be divided into potential and real. Potential characteristics are the maximum characteristics that can be provided by the method not taking into account the errors of real devices. In this case the computation error (it cannot be excluded) is taken into account only. But this error can be minimized by increasing the capacity of calculations. The real characteristics take into account the errors of the real devices, namely the voltmeter and the phase meter (of course the computation error is present in this case). The reasons and nature of the device errors were discussed above. The research of potential accuracy and discrimination power of the distance measuring multi-frequency phase method was carried out in the preceding chapter. So let us not dwell on the conditions of the experiments performance but let's consider only the obtained results.

The accuracy and discrimination power is affected by the following parameters: initial frequency f , frequency incremental step Δf , measurement error of amplitude of monophonic signal Δa_Σ , measurement error of phase shift of monophonic signal $\Delta \phi_\Sigma$, instability of probing signal frequency δf . During the measurements this means that the objects probing frequencies are changed with a specific constant incremental step (increment) to be expressed in fractions of a unit and we will denote it by *inc*. The analysis of the determined parameters indicates that a number of parameters which influence the accuracy of measurement have determined character, and the rest of them are random in character. The first group includes initial frequency and incremental step of probing frequency variation. The second group includes the errors of amplitude and phase shift measurements and also instability of frequency of the probing harmonic signal. When performing the modelling it is necessary to take into account the determined nature of the first group of parameters and random nature of the second group.

Modelling of the determined parameters influence is carried out by their change from the initial value to the final value in some incremental steps. As a rule the initial value is taken at zero level. The upper value is limited by the capacity of receiving and transmitting equipment, measurement units, etc. By virtue of the fact that terminable parameters include frequency, then it is necessary to rely on the capability of harmonic signals generators, frequency range of transceivers, measuring devices of phase shifts and amplitudes. Since the harmonic signals can be generated, transmitted and received within a wide range of frequencies, then the measuring devices of the phase shifts and amplitudes are characterised by the limited frequency range. Thus, namely the frequency parameters will determine the modelling. The most common are the methods and technical means of measuring amplitude and phase shifts that are effective in the frequency range of 10 MHz [1-4]. Parameters that are random in character should be set given that they have their own probability characteristics i.e. distribution law, expectation function and mean square expectation.

To study the impact of various factors upon the accuracy of the distance measuring using the multi-frequency phase method with regard to their random nature it is necessary to

develop appropriate mathematical models with introduced probability distributions. Let us consider the influence of each factor separately.

It is possible to use frequency generator with control option or frequency synthesizer to set the frequency grid. In both cases taking into account the impact of various factors frequency generation occurs with some instability i.e. long-term or short-term. The probability of frequency occurrence has normal distribution law that must be considered in the process of mathematical model development. Wherein the expectation function has the value of the required frequency, and the mean square expectation depends on the instability value of the generator. A quartz-crystal generator is characterised by a typical value of frequency instability, which vary from 10^{-4} до 10^{-8} . Taking into account the mathematical expression for the phase shift calculation of the harmonic signal reflected from the object located at some distance (3) we must introduce a random frequency value with provision for probability distribution:

$$\phi_k = \frac{4 \cdot \pi \cdot d_k \cdot \text{normald}[f + inc \cdot \Delta f, \sigma_f]}{c}, k = 1 \dots n. \quad (6)$$

where $\text{normald}[f + inc \cdot \Delta f, \sigma_f]$ is a coversine that sets the random value of the probing signal frequency with expectation function $f + inc \cdot \Delta f$ and mean square deviation σ_f .

To calculate the vectors of monophonic signals the resulting expression must be substituted in the expression (5). Frequency instability is changed through the values of 10^{-5} до 10^{-8} . We use Monte Carlo method to carry out mathematical modelling. We produce at least 1000 calculations for adequate modelling. After calculating we perform statistical processing of the received values of the objects distance. We construct histogram of the frequency of the data occurrence, reveal the nature of the distribution function, find expectation function, and values dispersion.

The results of mathematical modelling of the impact of the frequency instability upon the measurement result of the objects distance are shown in Table 1.

Fig. 2 and 3 show the dependence of the distance measuring error on the frequency instability.

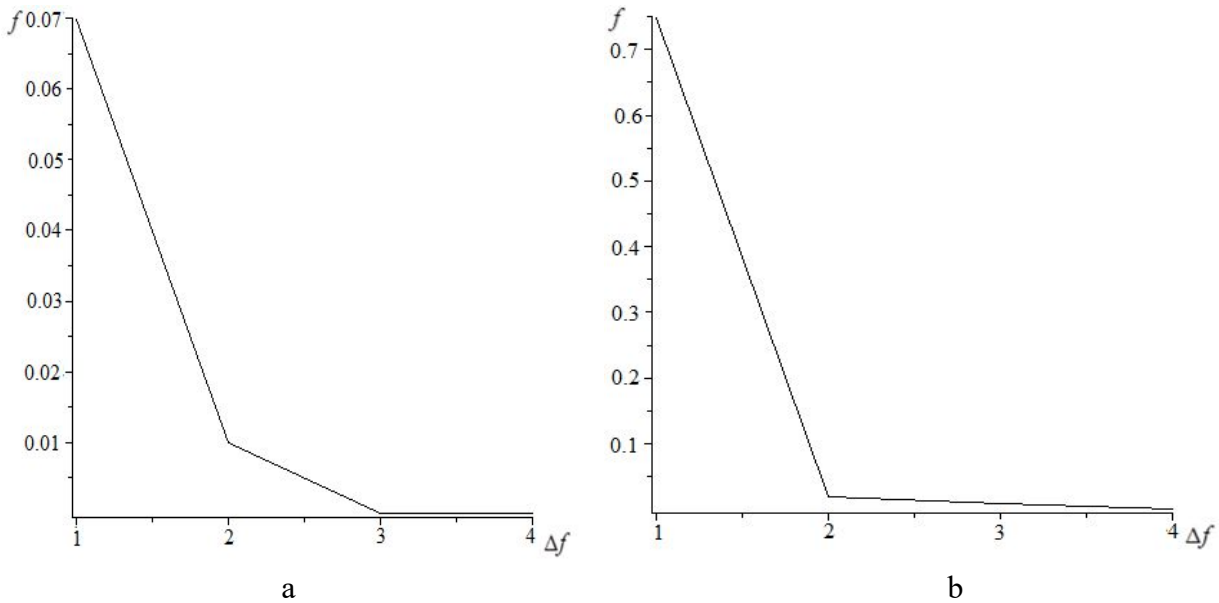


Fig. 2. Dependence of the distance measuring error on the frequency instability for:
a – $\Delta f/f = 10^{-5}$; b – $\Delta f/f = 10^{-6}$

Table 1.

The research of influence of frequency instability upon the error of the objects distance measuring

Instability of frequency, $\Delta f/f$	10^{-5}				10^{-6}			
True value	10	17	25	35	10	17	25	35
Expectation function, m	10.07	16.25	26.32	34.96	9.99	16.98	25.05	34.99
Expectation function of function deviation from average deviation, m	0.31	1.78	2.35	0.32	0.03	0.15	0.32	0.02
Mean square deviation, m	0.15	4.45	6.87	0.19	0.002	0.039	0.12	0.0009
Distance error, m	0.07	0.75	1.32	0.04	0.01	0.02	0.05	0.01
Instability of frequency, $\Delta f/f$	10^{-7}				10^{-8}			
True value	10	17	25	35	10	17	25	35
Expectation function, m	10.00	16.99	24.99	35.001	9.999	16.999	24.999	34.9999
Expectation function of function deviation from average deviation, m	0.003	0.015	0.029	0.002	$1 \cdot 10^{-4}$	$8 \cdot 10^{-4}$	0.001	0.0001
Mean square deviation, m	$1 \cdot 10^{-5}$	0.0003	0.0014	$8 \cdot 10^{-6}$	$4 \cdot 10^{-8}$	$8 \cdot 10^{-8}$	$3 \cdot 10^{-6}$	$1.7 \cdot 10^{-8}$
Distance error, m	$1 \cdot 10^{-4}$	0.01	0.01	0.001	$1 \cdot 10^{-5}$	0.001	0.001	0.0001

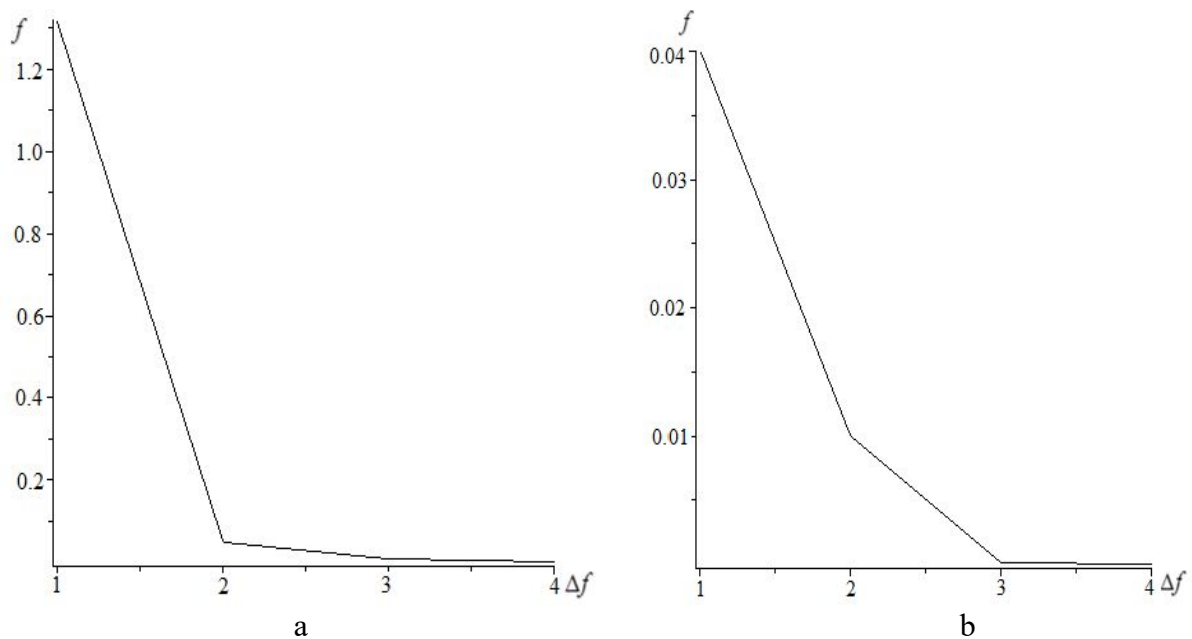


Fig. 3. Dependence of the distance measuring error on the frequency instability for:
a – $\Delta f/f = 10^{-7}$; b – $\Delta f/f = 10^{-8}$

The obtained dependencies show that the distance measurement error using multi-frequency phase method decreases by the exponential relationship.

Let us perform mathematical modelling in order to study the impact of measuring error of the monophonic signal amplitude and phase shift upon the distance measuring error using multi-frequency phase method. Let us make use of the common mathematical modelling algorithm. Its main stages are the following: setting the initial conditions; introducing measurement errors; carrying out calculations according to the method of measurement; repeated calculations in order to apply Monte Carlo method to receive a sample of the given size; statistical analysis of the obtained modelling results.

Let us introduce the restrictions of initial conditions in order to perform mathematical modelling. Let us assume that the values of distance are within the range of 50 m. Let us set four distances: 10 m, 15 m, 30 m and 35 m. If the maximum distance is 50m then according to the expression:

$$l_{max} \leq \frac{c}{2f_{min}}, \quad (7)$$

the minimum frequency should not exceed 3 MHz Let us set the frequency incremental step less than 3 MHz In order to introduce the signals measurement errors in the results of the calculations let us define the parameters of the probing signals to be measured. The values of the vectors of the probing signals are measured according to the analytical multi-frequency method. Each vector of the signal is set by the signal amplitude and initial phase. When the probing signals are used we carry out measurements of the phase shift between the reflected monophonic signal and the reference probing signal. Let us use the following expression to model the monophonic signal:

$$a_{\Sigma}(f) = \sum_{i=1}^n a_i e^{\frac{f_j}{f_{min}} \phi_i}, \quad (8)$$

where a_i – signal amplitude reflected from i object; ϕ_i – signal phase shift reflected from i object; f_j – current frequency; f_{min} – initial frequency.

Adding the error into the mathematical model is carried out by superposition of random values upon the monophonic signal amplitude and the phase shift. To do this we used the tools of MatLab R 2013 mathematical software. Accordingly the expression (8) will be the following:

$$a_{\Sigma}(f) = \sum_{i=1}^n a_i e^{\frac{f_j}{f_{min}} \phi_i} + \Delta a_j e^{\frac{f_j}{f_{min}} \Delta \phi_j}, \quad (9)$$

where Δa_j – amplitude error on j frequency; $\Delta \phi_j$ – phase error on j frequency.

The errors of amplitude and phase are set with uniform distribution since modern digital measuring instruments are characterised with the measurement error exactly with such function. The amplitude error dispersion is set within 0.1% and 0.001%, the phase shift is set within 1° to 0.01° which corresponds to methodical and instrumental measurement errors of modern measuring instruments.

Let us estimate the impact of each factor upon the result of the distance measurement. Firstly, let us determine the impact of the frequency incremental step change. The frequency incremental step change is set within 1.5 MHz to 2.5 MHz. Increase in value is 0.5 MHz. Wherein we set the minimum value of amplitude determination errors ($1/4096 a_{\Sigma}$) and phase shift (0.01°).

To illustrate the received sets of distance with random component the following histograms of frequency distribution of the values occurrence have been constructed (they are shown in Fig. 4 - 5).

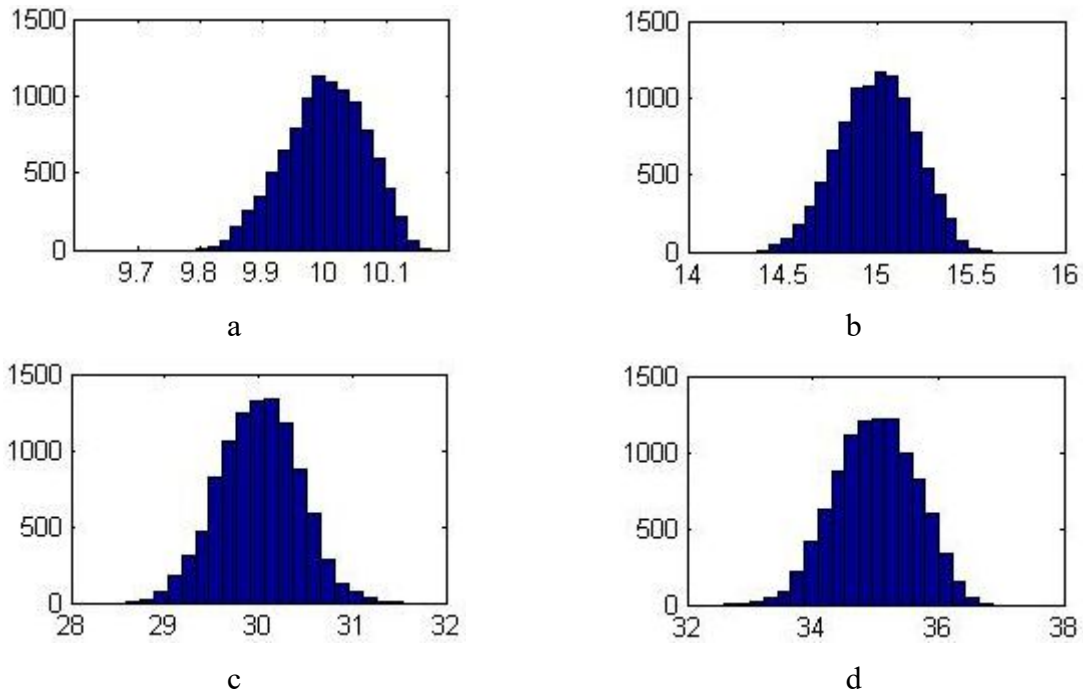


Fig. 4. Histograms of distance distribution in case of initial frequency is $f=2$ MHz and minimum values of the phase shift and amplitude errors where: a – $L=10$ м, $m=10.0005$, $\sigma=0.064134$; b – $L=15$ м, $m=15.0001$, $\sigma=0.20129$; c – $L=30$ м, $m=30.0024$, $\sigma=0.42011$; d – $L=35$ м, $m=35.0011$, $\sigma=0.6384$

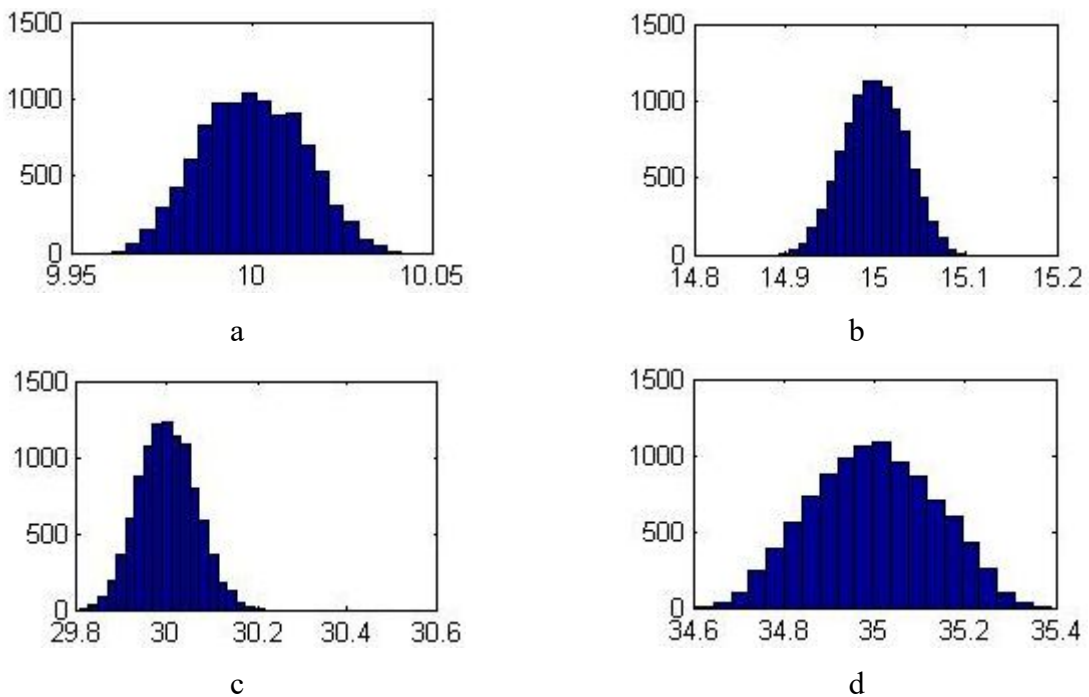


Fig. 5. Histograms of distance distribution in case of initial frequency is $f=2.5$ MHz and minimum values of the phase shift and amplitude errors where: a – $L=10$ м, $m=10.0002$, $\sigma=0.014017$; b – $L=15$ м, $m=14.9992$, $\sigma=0.0333$; c – $L=30$ м, $m=29.9992$, $\sigma=0.062326$; d – $L=35$ м, $m=34.998$, $\sigma=0.13516$

The analysis of the received histograms leads to the following conclusions. The laws of distance distribution at small values of the frequency incremental step are close to the Rayleigh law (Fig. 4). The law is normal for greater frequencies (Fig. 5). In this connection the deviation of the expectation function from the true value of distance is decreasing. This is also true for the mean square deviation.

Let us explore the impact of the monophonic signal amplitude determining error as the next stage. The amplitude error is set from the minimum value of $1/4096a_{\Sigma}$ to its maximum value of $1/256a_{\Sigma}$. Change of error is carried out in two times that corresponds to one discharge of the analog-to-digital converter. The phase shift measurement error is set to the lowest (0°). The incremental step of frequency change is 2.5 MHz. The analysis of the received data shows that the distribution laws for small errors are similar to the normal law. The distribution law is similar to Rayleigh law in case of the great values of the amplitude error. Deviation of the expectation function from the true value and mean square deviation increases in case of error increase.

Let us explore the impact of the phase shift measurement error upon the distance measuring error as the next stage. In the process of modelling we will change the phase shift within 0.01° to 0.5° with the error change by 5 times. The amplitude measurement error is set for $1/4096a_{\Sigma}$. The incremental step of frequency change is 4 MHz. The analysis of the received data shows that the error of the phase shift identification affects the value of the expectation function deviation from the true value and mean square deviation. When the phase shift error increases the distance error and mean square deviation also increase. However, the greatest distance error observed does not exceed two thousandths of a meter. That is why, the phase shift measurement methods and devices with an accuracy of 0.5° or greater are enough for measuring purposes. This conclusion is particularly important taking into consideration the fact that the presence of noise can significantly impact the values of the phase shift measurement error.

The peculiarity of the multi-frequency phase method is solving the system of linear equations as one of the stages of the distance finding. In this case, the accuracy of the distance measurement is affected by the conditioning number of the system matrix of linear equations of the multi-frequency phase method. It has been shown that the value of the monophonic reflected signal vector is different at different frequencies. Thus, changing the frequency values of the probing signals results in changing of the conditioning number and therefore the objects distance measuring error.

The results of mathematical modelling. The general trend is that the conditioning number decreases to a certain minimum value with the increase of the initial probing frequency. Then it increases to its maximum value with the following decreasing. This dependency is periodically repeated with the frequency increasing. With the increase of the probing frequency change incremental step the periodicity of the dependency is preserved, however, the minimum value is changed. The performed modelling shows that the change incremental step value of 4 MHz of the probing frequency preserves the minimum value of the conditioning number 13.5 for the initial frequency of 35 MHz. But the conditioning number is 16 for zero initial frequency. The lowest value of the conditioning number is observed when the frequency change incremental step value is 3.9 MHz. Dependency graph for this frequency incremental step is shown in Figure 6.

On the other hand, when a smaller probing frequency change incremental step was set within 2.5 to 3.5 MHz the conditioning number was 3-5 times bigger comparatively to its minimum value. Thus, the following conclusion can be drawn. Probing with less frequency incremental step does not significantly increase the matrix conditioning number so there is a transfer of the amplitude and phase shift measurement errors with their slight increase into the distance measuring error. Thus we can narrow the frequency range of probing signals. To

reduce the distance measuring error we should use more accurate methods of amplitude measuring and it will allow simplifying measurement instrumentation.

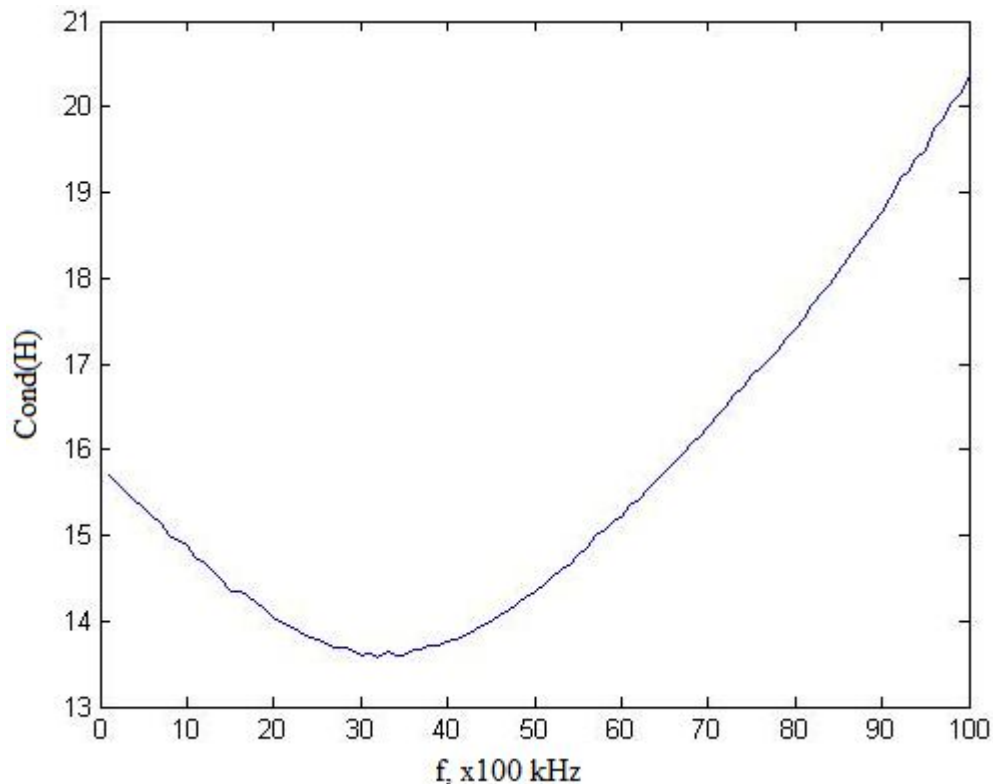


Fig. 6. Dependence of the conditioning number of the system matrix of linear equations on the initial probing frequency for the frequency incremental step of 3.9 MHz

The other values of distance result in a change of dependence. When the distance of one object is changed, the value of the conditioning number and the frequency it is observed at is changed.

As well as the accuracy of the distance measuring depends on the frequency range of the probing signals, the discrimination power of the distance measuring multi-frequency phase method depends on the frequency of harmonic signals the scanning of the objects is accomplished by. It is necessary to establish the relationship between the minimum distance between the objects which can be identified and the initial frequency.

Based on theoretical provisions laid down in the previous works of the authors, if the objects are located in close proximity, the vectors of the signals reflected from two objects at the beginning of the frequency range are close to each other. In this connection the increase of the probing frequency results in the increase of the monophonic signals vectors. To separate the two vectors it is necessary that the angle between the vectors is not less than the minimum value that can be separated. This condition may be met by different ways. Firstly, it is possible to measure the phase shift and amplitude of the monophonic signal with a given accuracy according to which the signals reflected from each object are separated by the results of solving the system of linear equations. Secondly, it is possible to increase the frequency change incremental step of the probing signal. It results in the increase of the angle between the vectors and thus the phase difference between them, which allows you to separate the signal reflected from each object. In this case, it is possible to measure the phase shifts and amplitudes of the signals reflected from each object with greater error. Thirdly, the discrimination power depends on the conditioning number of the matrix.

The practice of radar distance measurement says that identification capability is determined by the distance measuring error. And it is determined by its doubled value Δl . Therefore, in order to determine the distinguished capability we can use the expression (2).

Let us perform mathematical modelling in case of near location of the objects and establish relationships with a precision measurement of the phase shift and amplitude of the monophonic signals and the conditioning number of the system matrix of linear equations.

Let us take the initial conditions for the modelling as follows. We set four objects like in the previous modelling. The distance between two objects is from 2 to 1 m. The distance of 10 m is used as a reference one. We also will change the incremental step of the frequency from 2.5 MHz to 4 MHz, the original frequency from 0 to 1 MHz and the phase shift measuring errors from 1° to 0.1° and amplitude from $1/256 a_{\Sigma \max}$ to $1/2048 a_{\Sigma \max}$ of the monophonic signal. The result of the mathematical modelling is to establish the basic laws of various factors influence upon the probability characteristics of the objects distance.

The obtained data show that identification is improved with frequency increasing. With regard to the above mentioned the smaller is the distance between the objects, the greater frequency incremental step is to be set. Moreover, there is some critical frequency which provides the possibility of the objects identification. The change of the initial frequency does not result in any significant changes in the objects distance distribution histogram. In the same way the change of accuracy in determining the amplitude of the monophonic signal within a number of discharges also does not result in the improvement of the objects identification.

The change of the phase shift measuring accuracy results in the change of identification indicators. It has been determined above that the identification capability depends on the phase shift measurement error of the monophonic signal. Similarly, the discrimination power depends on the value of the error.

Conclusions

1. The algorithm of mathematical modelling of the formation process of the reflected monophonic signal in the presence of several reflection objects has been worked out. The algorithm consists of the following phases: setting the initial values, calculating the vectors values of the monophonic signals as a sum of signals reflected from each object, the vectors change by taking into account the amplitude error, the phase shift and the frequency of the probing signal.

2. The mathematical modelling of the process of the objects distance measuring using multi-frequency phase method has been performed. In the process of modeling we have changed the basic parameters of the probing signal and the monophonic reflected signal, namely: initial frequency, frequency incremental step, frequency instability, amplitude designation error and monophonic signal phase shift error. Monte Carlo method has been applied in the process of modelling. Frequency instability was set according to normal distribution, and the amplitude and phase error were set with uniform distribution.

3. The mathematical modelling of distance measuring using multi-frequency phase method has shown that distance measuring error is decreased if the probing signal frequency instability and the monophonic signal vectors measurement error are reduced. With regard to the abovementioned the mean square deviation of the distance is decreased. Calculations of the distance error coincide with the data obtained by the mathematical modelling. It has been found that it is appropriate, in the process of the objects probing at the depth of 50 meters, to use the frequency incremental step of 4 MHz, where the signal generator frequency instability is at least $10^{-6} f$, the amplitude measurement error is $1/1024 a_{\Sigma \max}$, the phase shift measurement error does not exceed 0.1° . In this case, the distance measurement error does not exceed 0.6 m.

4. The research results of influence of the probing signal initial frequency and incremental step change in the distance measuring error has revealed that the changes in these two parameters result in the system matrix of linear equations with different values. The result is the matrixes with equal values of the conditioning number. The initial frequency increase

results in reducing the conditioning number from the values of tens of thousands to 15-20. The probing signal frequency change incremental step also results in the change of the conditioning number, but in a smaller range. Lower distance measuring errors are observed at small values of the conditioning number, due to the fact that the matrixes with such conditioning numbers less propagate the monophonic signal vector error onto the resulting error in distance.

5. The research of the identification capacity of the distance measuring multi-frequency phase method has been carried out. It has been shown that the identification of two objects located at a close distance depends on all the factors affecting the measurement accuracy and have the same dependencies.

Reference list

1. Senchyshyna, Y.V. Improved multi-frequency phase method of ranging / Y.V. Senchyshyna, V.R. Liubchyk, A.V. Klepikovsky. – XIIIth International Scientific and technical conference «Up-to-date Problems of Radio Electronics, Telecommunication and Computer Engineering» (TCSET–2016), February 23–26, Lviv – Slavsko, Ukraine, 2016. – Pp. 250-251.
2. Ultra-Wideband Radar with Arbitrary Sounding Features, MRRS'2005: International Workshop on Microwaves, Radar and Remote Sensing, September 19–21, Kiev, Ukraine, 2005. – Pp. 272 - 276.
3. Kalinin, V.I. Ultra Bandwidth Noise Radar-Location on the Bases of Aerial Arrays with Signals Recirculation / V.I.Kalinin, V.V. Chapursky // Radio Technics and Electronics, 2008. – Vol. 53. №10. – Pp. 1266 -1277.
4. Shynkaruk, O.M. Analytical Distance Measuring Multi-Frequency Phase Method / O.M. Shynkaruk, V.R. Liubchyk, M.O. Lantvoit // Materials of Intern. Scientific and Technical Conference. «Radio-Technical Fields, Signals, Devices and Systems», March 11–15, Kyiv, Ukraine, 2013.– Pp. 140 -141.

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ БАГАТОЧАСТОТНОГО ФАЗОВОГО МЕТОДУ ДАЛЬНОМЕТРІЇ

В.Р.Любчик¹, А.В. Клепиковський², Ю.О. Бабій³, Є.С. Ленков⁴, В.О. Ковальов⁵

¹ Хмельницький національний університет,
вул. Інститутська, 11, м. Хмельницький, 29000, Україна; e-mail: vitaly1612@gmail.com;

² Буковинський національний медичний університет,
Театральна пл., 2, м. Чернівці, 58002, Україна; e-mail: andrei.klepikovskiy@gmail.com,

³ Національна академія Державної прикордонної служби України імені Богдана Хмельницького,
вул. Шевченка, 46, м. Хмельницький, 29000, Україна; e-mail: julscorpio@gmail.com,

⁴ Військовий інститут телекомунікацій та інформатизації,
вул. Московська, 45/1, м. Київ, 01011, Україна;

⁵ Державне Підприємство "Одеський науково-дослідний інститут телевізійної техніки",
вул. Мечнікова, 132, м. Одеса, 65028, Україна

Задача високоточного вимірювання дальності та радіальної швидкості рухомих цілей, як наземних, повітряних так і морських, є неновою. Для її розв'язання застосовують різноманітні радіолокаційні засоби. В залежності від задачі, яку мають вирішувати радіолокаційні системи, розрізняють їх різні типи і види. Найбільш гостро постає завдання охорони кордонів держави. В такому разі розрізнення малорозмірних цілей на невеликих відстанях та на значних дальностях є безсумнівно актуальною задачею. Відомі методи вимірювання дальностей в радіолокації, в основному, використовують імпульсні сигнали та розділення сигналів, відбитих від кожного об'єкту, за часом приходу. При цьому зондуючі сигнали, що забезпечують достатню точність, займають значний частотний діапазон. Це створює проблеми при побудові блоків дальномірних радіолокаційних систем. Найбільш точними є фазові методи дальнометрії. Вони дозволяють забезпечити високоточне вимірювання дальності цілей за умови чіткого обмеження частотного діапазону зондуючих сигналів, адже використовуються гармонічні сигнали та багаточастотність. Аналіз останніх досліджень показав, що розроблені в останні роки багаточастотні фазові методи дальнометрії дозволяють розділяти сигнали, відбиті від багатьох об'єктів, використовуючи обмежений частотний діапазон зондуючих сигналів та вимірювання значень векторів відбитих сигналів. Теоретичні положення та методи радіолокаційних вимірювань можна використовувати для розробки принципово нових радіосистем дальнометрії, вимірювання радіальної швидкості цілей та радіолокаційного спостереження у військовій сфері. Особливо це актуально при розробці радіолокаційних систем, що повинні розрізняти цілі на невеликих відстанях одна від одної на одній лінії. В статті проведено математичне моделювання процесу формування сумарного відбитого сигналу за наявності декількох об'єктів відбиття. Процес моделювання складається з етапів: встановлення початкових значень; розрахунок значень векторів сумарних сигналів як суми сигналів, відбитих від кожного об'єкту, зміна векторів шляхом врахування похибки амплітуди, фазового зсуву та частоти зондуючого сигналу. Проведено математичне моделювання процесу вимірювання дальності об'єктів за багаточастотним фазовим методом. При проведенні моделювання змінювались основні параметри зондуючого сигналу та сумарного відбитого сигналу, а саме: початкова частота, крок частоти, нестабільність частоти, похибка визначення амплітуди та фазового зсуву сумарного сигналу. При проведенні моделювання застосовано метод Монте-Карло. Нестабільність частоти задавалась з нормальним розподілом, похибка з амплітудою і фазою із рівномірним розподілом. Отримані результати свідчать, що математичне моделювання вимірювання дальності за багаточастотним фазовим методом показало, що при зменшенні нестабільності частоти зондуючого сигналу та похибки вимірювання векторів сумарних сигналів похибка вимірювання дальності зменшується.

Ключові слова: рухома ціль, дальність, радіолокаційна система, зондуючий сигнал, дальнометрія, фазовий метод.

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ МНОГОЧАСТОТНОГО ФАЗОВОГО МЕТОДА ДАЛЬНОМЕТРИИ

В.Р.Любчик¹, А.В. Клепиковский², Ю.А. Бабий³, Е.С. Ленков⁴, В.А. Ковалев⁵¹ Хмельницкий национальный университет,
ул. Институтская, 11, г. Хмельницкий, 29000, Украина, e-mail: vitality1612@gmail.com² Буковинский государственный медицинский университет,
Театральная пл., 2, г. Черновцы, 58002, Украина, e-mail: andrei.klepikovskiy@gmail.com,³ Национальная академия Государственной пограничной службы Украины имени Богдана Хмельницкого,
ул. Шевченко, 46, г. Хмельницкий, 29000, Украина; e-mail: julsorpio@gmail.com,⁴ Военный институт телекоммуникаций и информатизации,
ул. Московская, 45/1, г. Киев, 01011, Украина;⁵ Государственное предприятие "Одесский научно-исследовательский институт телевизионной техники",
ул. Мечникова, 132, г. Одесса, 65028, Украина

Задача высокоточного измерения дальности и радиальной скорости движущихся целей, как наземных, воздушных так и морских, является неновой. Для ее решения применяют различные радиолокационные средства. В зависимости от задачи, которую должны решать радиолокационные системы, различают их различные типы и виды. Наиболее остро стоит задача охраны границ государства. В таком случае различие малоразмерных целей на небольших расстояниях друг от друга и на значительных дальностях является несомненно актуальной задачей. Известные методы измерения дальностей в радиолокации, в основном, используют импульсные сигналы и разделения сигналов, отраженных от каждого объекта, по времени прихода. При этом зондирующие сигналы, обеспечивающие достаточную точность, занимают значительный частотный диапазон. Это создает проблемы при построении блоков дальномерных радиолокационных систем. Наиболее точными являются фазовые методы дальнометрии. Они позволяют обеспечить высокоточное измерение дальности целей при условии четкого ограничения частотного диапазона зондирующих сигналов, поскольку используются гармоничные сигналы. Анализ последних исследований показал, что разработанные в последние годы многочастотные фазовые методы дальнометрии позволяют разделять сигналы, отраженные от многих объектов, используя ограниченный частотный диапазон зондирующих сигналов и измерения значений векторов отраженных сигналов. Теоретические положения и методы радиолокационных измерений можно использовать для разработки принципиально новых радиосистем дальнометрии, измерения радиальной скорости целей и радиолокационного наблюдения в военной сфере. Особенно это актуально при разработке радиолокационных систем, которые должны различать цели на небольших расстояниях друг от друга на одной линии. В статье проведено математическое моделирование процесса формирования суммарного отраженного сигнала при наличии нескольких объектов отражения. Процесс моделирования состоит из этапов: установление начальных значений; расчет значений векторов суммарных сигналов как суммы сигналов отраженных от каждого объекта, изменение векторов путем учета погрешности амплитуды, фазового сдвига и частоты зондирующего сигнала. Полученные результаты свидетельствуют, что математическое моделирование измерения дальности данным методом показало, что при уменьшении нестабильности частоты зондирующего сигнала и погрешности измерения векторов суммарных сигналов погрешность измерения дальности уменьшается.

Ключевые слова: подвижная цель, дальность, радиолокационная система, зондирующий сигнал, дальнометрия, фазовый метод.

ТЕОРЕТИЧЕСКОЕ РАЗВИТИЕ ОБЩЕГО ПОДХОДА К ПРОБЛЕМЕ ВЫЯВЛЕНИЯ НАРУШЕНИЙ ЦЕЛОСТНОСТИ ЦИФРОВЫХ КОНТЕНТОВ, ОСНОВАННОГО НА АНАЛИЗЕ ПОЛНОГО НАБОРА ИХ ФОРМАЛЬНЫХ ПАРАМЕТРОВ

И.И. Бобок

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: werter666@ukr.net

Целостность информации является одним из основных критериев ее безопасности. Сегодня информационные объекты все чаще имеют цифровое представление: изображения, аудио, цифровое видео. Использование таких объектов с целью, отличной от развлекательной (в медицине, прессе, науке, судебных расследованиях и т.д.), возможно лишь при отсутствии их несанкционированных изменений. Это делает проблему проверки их целостности, задачу разработки новых подходов и методов для такой проверки чрезвычайно актуальной. В работе получил дальнейшее теоретическое развитие новый общий подход к решению проблемы обнаружения несанкционированных изменений цифровых контентов, основанный на анализе сингулярных чисел и сингулярных векторов блоков их матриц, полученных путем стандартного разбиения, одним из разработчиков которого является автор. Предложенное усовершенствование обеспечит повышение чувствительности разрабатываемых на его основе для экспертизы цифровых изображений, видео методов и реализующих их алгоритмов к (малым) возмущающим воздействиям за счет повышения чувствительности формальных параметров, используемых для анализа целостности контента.

Ключевые слова: нарушение целостности, сингулярные числа, сингулярные векторы, цифровое изображение, цифровое видео, n -оптимальный вектор

Введение

Целостность информации является одним из основных критериев ее безопасности. Спецификой сегодняшнего дня является повсеместное использование цифровых контентов, в частности, цифровых изображений (ЦИ), видео (ЦВ), цифрового аудио. При использовании таких объектов в прессе, медицине, науке, судебных расследованиях и т.д. необходимо быть уверенным в отсутствии их несанкционированных изменений. Это делает проблему проверки их целостности чрезвычайно актуальной.

Современный уровень развития IT-технологий привел к тому, что разного рода фальсификации цифровых контентов, в частности ЦИ, средствами графических редакторов, таких как Adobe Photoshop, Corel Draw и другие, стали чрезвычайно распространенными, а существующие современные способы выявления таких нарушений целостности ЦИ по тем или иным причинам не являются удовлетворительными [1-3].

Основы принципиально нового общего подхода к организации проверки целостности ЦИ, ЦВ недавно были разработаны в [4,5], где были выявлены, теоретически обоснованы и практически проверены новые свойства полного набора формальных параметров, определяющих изображение, кадры ЦВ. Получены характеристики взаимного расположения левого и правого сингулярных векторов, отвечающих наибольшему сингулярному числу матрицы (блока матрицы) изображения, кадра ЦВ, и вектора, составленного из сингулярных чисел. Показано, что для большинства $l \times l$ -блоков оригинального изображения, полученных в результате стандартного разбиения его матрицы (независимо от формата хранения – с потерями, без потерь) угол между левым (правым) упомянутым сингулярным вектором и вектором, составленным из сингулярных чисел, определяется углом между n -оптимальным вектором $n^O = (1/\sqrt{l}, 1/\sqrt{l}, \dots, 1/\sqrt{l})^T \in R^l$ и вектором стандартного базиса пространства R^l соответствующей размерности, при этом установленная особенность нарушается для упомянутых формальных параметров в неоригинальном изображении, что является показателем нарушения его целостности, а значит может быть использовано как основа для разработки методов и алгоритмов выявления такого нарушения. Один из таких методов для выявления нарушения целостности ЦИ, являющегося следствием стеганопреобразования, который принципиально может быть адаптирован для экспертизы ЦВ и аудио, был предложен в [5]. Алгоритмическая реализация предложенного метода превосходит по эффективности современные стеганоаналитические алгоритмы, что говорит о перспективности нового подхода, однако остается недостаточно чувствительной к малым возмущающим воздействиям, отличным от стеганопреобразования, в частности, к наложению шума: возможны ошибки как первого (в случае мультипликативного шума с малой дисперсией), когда модифицированное ЦИ воспринимается как оригинальное, так и второго рода, когда оригинальное изображение трактуется как такое, для которого нарушена целостность.

Таким образом, новый подход к решению проблемы выявления нарушений целостности цифровых контентов, очевидно являясь перспективным, требует дальнейшего развития.

Цель статьи и постановка заданий

Целью работы является дальнейшее теоретическое развитие общего подхода к проблеме выявления нарушений целостности цифровых контентов, основанного на анализе СНЧ и СНВ (блоков) матрицы контентов, которое обеспечит повышение чувствительности используемых для экспертизы ЦИ и ЦВ их формальных параметров к возмущающим воздействиям.

Для достижения поставленной цели в работе решаются следующие *задачи*:

1. Определение такого преобразования матрицы блока ЦИ (кадра ЦВ), в результате которого составляющие полного набора параметров соответствующей матрицы будут более чувствительными к (малым) возмущающим воздействиям, которые претерпевает цифровой контент;

2. Используя результат решения задачи 1, уточнить базовые положения рассматриваемого общего подхода к проблеме выявления нарушений целостности цифровых контентов.

Основная часть

Пусть F – $n \times n$ – матрица ЦИ, разбитая стандартным образом [6] на непересекающиеся $l \times l$ – блоки. Анализируемыми при экспертизе ЦИ формальными

параметрами в [4,5] являлись сингулярные числа (СНЧ) и сингулярные векторы (СНВ) блоков матрицы F , образующие полный набор формальных параметров, определяющий контент, получаемые при помощи нормального сингулярного разложения, которое для блока B выглядит следующим образом:

$$B = U\Sigma V^T, \quad (1)$$

где U, V - ортогональные $l \times l$ -матрицы, столбцы которых $u_1, \dots, u_l$ и $v_1, \dots, v_l$ - соответственно левые и правые СНВ B , $\Sigma = \text{diag}(\sigma_1, \dots, \sigma_l)$, $\sigma_1 \geq \dots \geq \sigma_l \geq 0$ - СНЧ B .

СНВ u_1 и v_1 блока B оригинального ЦИ, а также вектор $\bar{\sigma} = \sigma / \|\sigma\|$, где $\sigma = (\sigma_1, \sigma_2, \dots, \sigma_l)^T \in R^l$, являются нечувствительными, sign-нечувствительными, неотрицательными, геометрически располагаются в первом координатном ортанте пространства R^l [4,5], что говорит о существовании связи между u_1 , v_1 , $\bar{\sigma}$ в блоках оригинального ЦИ.

Нечувствительность вектора $\bar{\sigma}$ очевидно вытекает из имеющего место для СНЧ матрицы B соотношения [7]:

$$\max_{1 \leq i \leq l} |\sigma_i(B) - \sigma_i(B + \Delta B)| \leq \|\Delta B\|_2, \quad (2)$$

где ΔB матрица возмущения блока B , $\|\bullet\|_2$ — спектральная матричная норма;

Основой подхода, предложенного в [4,5], являлось установленное для оригинального ЦИ соотношение

$$\angle(u_1, \bar{\sigma}) \approx \angle(v_1, \bar{\sigma}) \approx \angle(n^o, e_1), \quad (3)$$

показывающее, что угол между векторами u_1 и $\bar{\sigma}$ ($\angle(u_1, \bar{\sigma})$), v_1 и $\bar{\sigma}$ ($\angle(v_1, \bar{\sigma})$) для большинства $l \times l$ -блоков оригинального ЦИ близок к углу между n -оптимальным вектором $n^o = (1/\sqrt{l}, 1/\sqrt{l}, \dots, 1/\sqrt{l})^T \in R^l$ пространства R^l и вектором стандартного базиса $e_1 = (1, 0, \dots, 0) \in R^l$ ($\angle(n^o, e_1)$). Для достижения цели работы соотношение (3) нуждается в уточнении.

Для симметричной неотрицательной матрицы BB^T с учетом (1) имеет место соотношение: $BB^T = (U\Sigma V^T)(U\Sigma V^T)^T = U\Sigma^2 U^T$, которое представляет собой нормальное спектральное разложение BB^T , совпадающее в силу свойств матрицы BB^T с ее нормальным сингулярным разложением, определяемое однозначно. При этом собственные значения матрицы BB^T , равны ее сингулярным числам и определяются квадратами СНЧ B , а левые СНВ B - ортонормированные лексикографически положительные собственные векторы BB^T , совпадающие с ее левыми, правыми СНВ.

Рассмотрим подробно свойства СНЧ $\sigma_i(BB^T)$, $i = \overline{1, l}$, матрицы BB^T . Как и для любой матрицы, СНЧ BB^T являются нечувствительными к возмущающим воздействиям, т.е. для них выполняется соотношение (2):

$$\max_{1 \leq i \leq l} |\sigma_i(BB^T) - \sigma_i(BB^T + \Delta(BB^T))| \leq \|\Delta(BB^T)\|_2, \quad (4)$$

где $\Delta(BB^T)$ - возмущение матрицы BB^T в результате возмущающего воздействия на матрицу ЦИ, при котором возмущение самого блока B равно ΔB .

Заметим, что в (2), (4) спектральную матричную норму можно заменить на норму Фробениуса $\|\bullet\|_F$ в силу соотношения [7]: $\|A\|_2 \leq \|A\|_F$, имеющего место для любой квадратной матрицы A .

Если блок B получил возмущение ΔB , то возмущение для BB^T определим из соотношения:

$$(B + \Delta B)(B + \Delta B)^T = BB^T + B \cdot (\Delta B)^T + \Delta B \cdot B^T + \Delta B \cdot (\Delta B)^T = BB^T + \Delta(BB^T),$$

где

$$\Delta(BB^T) = B \cdot (\Delta B)^T + \Delta B \cdot B^T + \Delta B \cdot (\Delta B)^T.$$

Тогда

$$\|\Delta(BB^T)\|_F = \|B \cdot (\Delta B)^T + \Delta B \cdot B^T + \Delta B \cdot (\Delta B)^T\|_F.$$

В силу свойств матричной нормы Фробениуса [7], имеем:

$$\begin{aligned} & \|\Delta(BB^T)\|_F \leq \\ & \leq \|B \cdot (\Delta B)^T\|_F + \|\Delta B \cdot B^T\|_F + \|\Delta B \cdot (\Delta B)^T\|_F \leq \|B\|_F \|(\Delta B)^T\|_F + \|\Delta B\|_F \|B^T\|_F + \|\Delta B\|_F \|(\Delta B)^T\|_F. \end{aligned}$$

Из определения нормы Фробениуса очевидно, что:

$$\|B\|_F = \|B^T\|_F; \quad \|\Delta B\|_F = \|(\Delta B)^T\|_F.$$

Тогда последнее неравенство принимает вид:

$$\|\Delta(BB^T)\|_F \leq 2 \cdot \|B\|_F \|\Delta B\|_F + \|\Delta B\|_F^2. \quad (5)$$

Для ЦИ, как правило, $\|B\|_F > 1$, а $\|\Delta B\|_F > 0$, тогда правая часть (5) удовлетворяет соотношению:

$$2 \cdot \|B\|_F \|\Delta B\|_F + \|\Delta B\|_F^2 > 2\|\Delta B\|_F + \|\Delta B\|_F^2 > \|\Delta B\|_F. \quad (6)$$

Соотношение (6) означает, что верхняя граница для значений $\|\Delta(BB^T)\|_F$ больше, чем $\|\Delta B\|_F$, что, в свою очередь, приводит к тому, что возмущения СНЧ матрицы BB^T в общем случае могут оказаться больше, чем возмущения СНЧ B в результате возмущения блока B на ΔB , т.е. СНЧ BB^T , оставаясь нечувствительными к возмущающим воздействиям, значительно реагируют на (малое) возмущающее воздействие ΔB , чем СНЧ самого блока B , а значит для достижения цели работы вектор

$$\bar{\sigma} = \sigma_{BB^T} / \|\sigma_{BB^T}\|,$$

где

$$\sigma_{BB^T} = (\sigma_1(BB^T), \sigma_2(BB^T), \dots, \sigma_l(BB^T))^T = (\sigma_1^2, \sigma_2^2, \dots, \sigma_l^2)^T \in R^l,$$

является более предпочтительным, чем вектор $\bar{\sigma}$.

Аналогичные рассуждения будут иметь место и для симметричной неотрицательной матрицы $B^T B$, для которой с учетом (1) имеем:

$$B^T B = V \Sigma^2 V^T.$$

. Последнее равенство представляет нормальное спектральное разложение $B^T B$, совпадающее с ее нормальным сингулярным разложением. Собственные значения матрицы $B^T B$ равны ее сингулярным числам $\sigma_i(B^T B)$, $i = \overline{1, l}$ и, как и в случае матрицы BB^T , определяются квадратами СНЧ B , т.е. вектор

$$\sigma_{B^T B} = (\sigma_1(B^T B), \sigma_2(B^T B), \dots, \sigma_l(B^T B))^T = (\sigma_1^2, \sigma_2^2, \dots, \sigma_l^2)^T = \sigma_{BB^T},$$

а при его нормировании получим:

$$\bar{\bar{\sigma}} = \sigma_{B^T B} / \|\sigma_{B^T B}\| = \bar{\sigma}.$$

Правые СНВ B - ортонормированные лексикографически положительные собственные векторы $B^T B$, совпадающие с ее правыми и левыми сингулярными векторами.

Вектор $\bar{\bar{\sigma}}$ имеет еще одно значительное преимущество по сравнению с $\bar{\sigma}$. Одним из базисных положений рассматриваемого подхода является близость векторов $\bar{\sigma}$ и e_1 , которая определяется малым значением угла между ними: $\angle(e_1, \bar{\sigma}) \approx 0$. Сравним углы, образующие $\bar{\bar{\sigma}}$ и $\bar{\sigma}$ с вектором e_1 .

Скалярное произведение $(\bar{\sigma}, e_1)$ векторов $\bar{\sigma}$ и e_1 определяется в соответствии с формулой:

$$(\bar{\sigma}, e_1) = \frac{\sigma_1}{\sqrt{\sigma_1^2 + \sigma_2^2 + \dots + \sigma_l^2}},$$

откуда с учетом нормированности вектора $\bar{\sigma}$ получаем:

$$\cos \alpha = \frac{\sigma_1}{\sqrt{\sigma_1^2 + \sigma_2^2 + \dots + \sigma_l^2}}, \quad (7)$$

где $\alpha = \angle(e_1, \bar{\sigma})$.

В то же время,

$$(\bar{\bar{\sigma}}, e_1) = \frac{\sigma_1(BB^T)}{\sqrt{(\sigma_1(BB^T))^2 + (\sigma_2(BB^T))^2 + \dots + (\sigma_l(BB^T))^2}} = \frac{\sigma_1^2}{\sqrt{\sigma_1^4 + \sigma_2^4 + \dots + \sigma_l^4}},$$

откуда

$$\cos \beta = \frac{\sigma_1^2}{\sqrt{\sigma_1^4 + \sigma_2^4 + \dots + \sigma_l^4}}, \quad (8)$$

где $\beta = \angle(e_1, \overline{\sigma})$.

Возведем правые части (7) и (8) в квадрат и рассмотрим значения, обратные к полученным:

$$\frac{\sigma_1^2 + \sigma_2^2 + \dots + \sigma_l^2}{\sigma_1^2} = 1 + \left(\frac{\sigma_2}{\sigma_1}\right)^2 + \dots + \left(\frac{\sigma_l}{\sigma_1}\right)^2; \quad (9)$$

$$\frac{\sigma_1^4 + \sigma_2^4 + \dots + \sigma_l^4}{\sigma_1^4} = 1 + \left(\frac{\sigma_2}{\sigma_1}\right)^4 + \dots + \left(\frac{\sigma_l}{\sigma_1}\right)^4. \quad (10)$$

Учитывая, что σ_1 - это максимальное СНЧ блока B , сравнивая правые части (9) и (10), получим:

$$1 + \left(\frac{\sigma_2}{\sigma_1}\right)^4 + \dots + \left(\frac{\sigma_l}{\sigma_1}\right)^4 \leq 1 + \left(\frac{\sigma_2}{\sigma_1}\right)^2 + \dots + \left(\frac{\sigma_l}{\sigma_1}\right)^2,$$

т.е.

$$\frac{\sigma_1^4}{\sigma_1^4 + \sigma_2^4 + \dots + \sigma_l^4} \geq \frac{\sigma_1^2}{\sigma_1^2 + \sigma_2^2 + \dots + \sigma_l^2},$$

что означает:

$$\cos \beta \geq \cos \alpha,$$

и соответственно

$$\beta \leq \alpha.$$

Последнее неравенство с учетом всего вышесказанного позволяет уточнить соотношение (3). Таким образом, для оригинального ЦИ, кадра ЦВ имеет место соотношение:

$$\angle(u_1, \overline{\sigma}) \approx \angle(v_1, \overline{\sigma}) \approx \angle(n^o, e_1). \quad (11)$$

Очевидно, что приближенное равенство в (11) достигается с меньшей погрешностью, чем в (3), что необходимо приведет к повышению эффективности методов выявления нарушения целостности цифровых контентов, основанных на (11), по сравнению с методами, основанными на (3) [5].

Выводы

В работе предложено дальнейшее развитие общего подхода к решению проблемы выявления нарушений целостности ЦИ, ЦВ.

В ходе работы определены преобразования двух видов матрицы B блока ЦИ (кадра ЦВ): $B^T B$ и BB^T . Такие преобразования позволили выделить из полного набора формальных параметров $B^T B$ и BB^T такие параметры, которые являются предпочтительными по сравнению с аналогичными параметрами B для достижения поставленной цели. А именно: СНЧ матриц $B^T B$, BB^T , являясь квадратами СНЧ B , оставаясь нечувствительными к возмущающим воздействиям, сильнее реагируют на них, чем СНЧ B . Установлено, что нормированный вектор СНЧ матриц $B^T B$, BB^T менее отличается от вектора e_1 стандартного базиса, чем аналогичный вектор для B . Это позволило уточнить базовое соотношение связи параметров блока оригинального ЦИ, кадра ЦВ рассматриваемого общего подхода.

Полученные теоретические результаты дают принципиальную возможность для разработки основанных на них новых методов выявления нарушений целостности цифровых контентов, обладающих большей чувствительностью к (малым) возмущающим воздействиям, по сравнению с теми, которые основывались на первоначальных положениях рассматриваемого подхода.

Список литературы

1. Rey, C. A survey of watermarking algorithms for image authentication / C. Rey, J.-L. Dugelay // EURASIP J. Appl. Signal Process, 2002. – №1. – С.613–621.
2. Amerini, I. Copy-move forgery detection and localization by means of robust clustering with J-linkage / I. Amerini, L. Ballan, R. Caldelli, A. del Bimbo, L. del Tongo, G. Serra // Signal Processing, 2013. – Т.28, №6. – С.659–669.
3. Farid, H. Image Forgery Detection / H. Farid // IEEE Signal processing magazine, 2009. – С.16–25.
4. Кобозева, А.А. Основы общего подхода к разработке универсальных стеганоаналитических методов для цифровых изображений / А.А.Кобозева // Праці Одеського політехнічного університету, 2014. – Вип.2(44). – С.136–146.
5. Kobozeva, A.A. General Principles of Integrity Checking of Digital Images and Application for Steganalysis / A.A. Kobozeva, I.I. Bobok, A.I. Garbuz // Transport and Telecommunication. - 2016. – Vol. 17, Issue 2. – Рр. 128–137.
6. Гонсалес, Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс; пер. с англ. П.А. Чочиа. – М. : Техносфера, 2006. – 1070 с.
7. Деммель, Д. Вычислительная линейная алгебра [Текст]: теория и приложения / Д. Деммель; Пер. с англ. Х.Д. Икрамова. – М.: Мир, 2001. – 430 с.

ТЕОРЕТИЧНИЙ РОЗВИТОК ЗАГАЛЬНОГО ПІДХОДУ ДО ПРОБЛЕМИ ВИЯВЛЕННЯ ПОРУШЕНЬ ЦІЛІСНОСТІ ЦИФРОВИХ КОНТЕНТІВ, ЗАСНОВАНОГО НА АНАЛІЗІ ПОВНОГО НАБОРУ ЇХ ФОРМАЛЬНИХ ПАРАМЕТРІВ

І.І. Бобок

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: werter666@ukr.net

Цілісність інформації є одним з основних критеріїв її безпеки. Сьогодні інформаційні об'єкти все частіше мають цифрове представлення: зображення, аудіо, цифрове відео. Використання таких об'єктів з метою, що відрізняється від розважальної (в медицині, пресі, науці, судових розслідуваннях і т.і.), можливо лише за відсутності їх несанкціонованих змін. Це робить проблему перевірки їх цілісності, задачу розробки нових підходів і методів для такої перевірки надзвичайно актуальною.

В роботі отримав подальший теоретичний розвиток новий загальний підхід до вирішення проблеми виявлення несанкціонованих змін цифрових контентів, заснований на аналізі сингулярних чисел і сингулярних векторів блоків їх матриць, отриманих шляхом стандартного розбиття, одним з розробників якого є автор. Запропоноване удосконалення забезпечить підвищення чутливості до (малих) збурювальних дій методів і алгоритмів, що їх реалізують, які розробляються на його основі, для експертизи цифрових зображень, відео за рахунок підвищення чутливості формальних параметрів, використовуваних для аналізу цілісності контенту.

Ключові слова: порушення цілісності, сингулярні числа, сингулярні вектори, цифрове зображення, цифрове відео, n -оптимальний вектор

THEORETICAL DEVELOPMENT OF THE GENERAL APPROACH TO SOLVING THE PROBLEM OF DETECTING THE INTEGRITY VIOLATIONS OF DIGITAL CONTENT BASED ON THE ANALYSIS OF A COMPLETE SET OF FORMAL PARAMETERS

I.I. Bobok

Odessa National Polytechnic University,
1, Shevchenko Ave., Odesa, 65044, Ukraine; e-mail: werter666@ukr.net

Integrity of information is one of the main criteria for its safety. Today, information objects mainly have a digital representation: images, audio, digital video. The use of such objects for purposes other than entertainment (for example, in the medicine, press, science, judicial investigations, etc.) is possible only in the absence of their unauthorized changes. It makes the problem of integrity checking, and the task of developing new approaches and methods for such verification is extremely relevant.

In this article, a new general approach to solving the problem of detecting unauthorized changes in digital content was obtained. Proposed approach is based on the analysis of singular numbers and singular vectors of blocks of their matrices, that obtained by standard partitioning. The proposed improvement will increase the sensitivity of methods and algorithms (including the small disturbance) by increasing the sensitivity of the formal parameters used to analyze the integrity of the content.

Keywords: integrity violation, singular value, singular vector, digital image, digital video, optimal-vector

ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ПРОГРАМНОЇ РЕАЛІЗАЦІЇ МЕТОДІВ ПОШУКУ ОБЕРНЕНОГО ЕЛЕМЕНТА ЗА МОДУЛЕМ

М.М. Касянчук, І.З. Якименко, С.В. Івасєв, О.В. Момотюк

Тернопільський національний економічний університет,
вул. Львівська, 11, Тернопіль, 46020, Україна; e-mail: kasyanchuk@ukr.net, iyakymenko@ukr.net,
stepan.ivasiev@gmail.com, momotjuk98@gmail.com

Знаходження мультиплікативного оберненого елемента за модулем дуже часто є необхідною умовою для розв'язування багатьох задач сучасної теорії чисел, обчислювальної та прикладної математики, асиметричної криптографії, зокрема, криптосистем RSA та Ель-Гамала. У роботі проведено експериментальне дослідження часових характеристик програмної реалізації пошуку оберненого елемента за модулем на основі класичного методу розширеного алгоритму Евкліда та запропонованих методів додавання модуля та додавання залишку із застосуванням мови програмування високого рівня C++. Для дослідження використовувалися числа різної розрядності. Показано, що в переважній більшості розглянутих випадків метод додавання модуля характеризується більш високою швидкістю в порівнянні з двома іншими. Представлено графічні залежності середнього часу пошуку оберненого елемента різними методами від розрядності вибраних чисел. Для нівелювання випадкових впливів на час роботи усі обчислення повторювалися 100 разів. Запропоновані методи ефективно можна використовувати для пошуку оберненого елемента за модулем.

Ключові слова: алгоритм Евкліда, обернений елемент за модулем, асиметрична криптографія, додавання модуля, додавання залишку, середній час, часові характеристики.

Вступ

Операція пошуку мультиплікативного оберненого елемента за модулем на даний час є однією з найважливіших і одночасно найбільш обчислювально складних в сучасній теорії чисел [1-2]. Поширеність цієї операції зумовлена її застосуванням в сучасній асиметричній криптографії (криптосистеми RSA, Ель-Гамала [3], шифрування на основі математичного апарату еліптичних кривих [4], протоколи електронного цифрового підпису та обміну ключами [5] тощо), системі залишкових класів [6-7] та її різних модифікаціях [8-9], кодуванні даних на основі модулярної арифметики [10], інших застосуваннях прикладної та дискретної математики. Тому задача дослідження програмної реалізації різних методів пошуку мультиплікативно оберненого елемента за модулем є надзвичайно актуальною.

Мультиплікативно оберненим елементом до числа a за модулем n називається таке число b , для якого виконується рівність $a - b \bmod n = 1$, тобто $b = a^{-1} \bmod n$. Натуральні числа a та n при цьому повинні бути взаємно простими. В [11] детально описані методи пошуку оберненого елемента, з яких найбільш поширеними є такі:

1. Перебором всіх можливих варіантів;
2. За допомогою теореми Ейлера;
3. На основі розширеного алгоритму Евкліда.

Перший метод характеризується високою обчислювальною складністю, оскільки повний перебір вимагає значних часових затрат.

При використанні теореми Ейлера $a^{\varphi(n)} \bmod n = 1$ отримується $a^{\varphi(n)-1} \bmod n = a^{-1} \bmod n$ [12]. Це передбачає виконання операції модулярного експоненціювання [13-14], що може привести до переповнення розрядної сітки процесора і ускладнює пошук оберненого елемента для багаторозрядних чисел.

Найбільш поширеним є метод пошуку мультиплікативного оберненого елемента за модулем на основі розширеного алгоритму Евкліда [15]: спочатку потрібно записати прямий алгоритм Евкліда, згідно якого при $n > a = r_0$, де n і a – цілі числа, виконується така послідовність операцій:

$$\begin{aligned} n &= r_0 \cdot q_1 + r_1, \quad q_1 = a, \quad 0 \leq r_1 < r_0; \\ r_0 &= r_1 \cdot q_2 + r_2, \quad 0 \leq r_2 < r_1; \\ &\dots\dots\dots \\ r_{n-3} &= r_{n-2} \cdot q_{n-1} + r_{n-1}, \quad 0 \leq r_{n-1} < r_{n-2}; \\ r_{n-2} &= r_{n-1} \cdot q_n + r_n, \quad 0 \leq r_n < r_{n-1}; \\ r_{n-1} &= r_n \cdot q_{n+1} + 0. \end{aligned}$$

Оскільки a і n є взаємно простими, то $r_n=1$. Розширений алгоритм Евкліда передбачає зворотній порядок проходження прямого алгоритму:

$$1 = r_n = r_{n-2} - q_n r_{n-1} = r_{n-2} - q_n (r_{n-3} - q_{n-1} r_{n-2}) = r_{n-2} - q_n r_{n-3} + q_n q_{n-1} r_{n-2} = -q_n r_{n-3} + (1 + q_n q_{n-1}) r_{n-2} = -q_n r_{n-3} + (1 + q_n q_{n-1}) (r_{n-4} - q_{n-2} r_{n-3}) = \dots$$

Описана процедура продовжується до тих пір, поки не буде отриманий вираз $v \cdot n + t \cdot r_0 = 1$, де величина $b = t \bmod n = a^{-1} \bmod n$ і буде шуканим оберненим елементом. В таблиці 1 наведено приклад пошуку оберненого елемента на основі розширеного алгоритму Евкліда.

Таблиця 1.

Пошук оберненого елемента $41^{-1} \bmod 157$ на основі розширеного алгоритму Евкліда

Алгоритм Евкліда	Розширений алгоритм Евкліда
$157=41 \cdot 3+34$ $41=34 \cdot 1+7$ $34=7 \cdot 4+6$ $7=6 \cdot 1+1$	$1=7-1 \cdot 6=7-1 \cdot (34-4 \cdot 7)=-1 \cdot 34+5 \cdot 7=-1 \cdot 34+5 \cdot (41-1 \cdot 34)=5 \cdot 41-6 \cdot 34=$ $=5 \cdot 41-6 \cdot (157-3 \cdot 41)=-6 \cdot 157+23 \cdot 41;$ $41^{-1} \bmod 157=23$

Даний метод характеризується великою кількістю ділень з остачею, перемножень і підстановок, хоча він володіє найменшою часовою складністю в порівнянні з іншими двома, наведеними вище.

Метою даної роботи є розробка нових методів пошуку оберненого елемента за модулем без виконання обчислювально складних операцій множення та ділення з остачею, а також експериментальне порівняння програмної реалізації пошуку оберненого елемента за модулем на основі розширеного алгоритму Евкліда та запропонованими методами.

Основна частина

З теорії чисел відомо [16], що вираз $a \cdot b \bmod n = 1$ можна переписати таким чином: $a \cdot b = k \cdot n + 1$, де k – деяке ціле число. Звідси слідує, що для пошуку оберненого елемента необхідно до модуля додати 1 і перевірити, чи ділиться націло отримане число на a . Якщо не ділиться, то далі до отриманого числа потрібно послідовно додавати модуль до тих пір, поки результатом ділення не буде ціле число. Математично це записується так:

$$\begin{aligned} n_0 &= n + 1; \quad b_0 = (n + 1)/a; \\ n_1 &= 2 \cdot n + 1; \quad b_1 = (2 \cdot n + 1)/a; \\ &\dots \\ n_i &= (i + 1) \cdot n + 1; \quad b_i = ((i + 1) \cdot n + 1)/a; \quad b_i \in \mathbb{Z}. \end{aligned}$$

Блок-схема алгоритму пошуку оберненого елемента на основі додавання модуля представлена на рисунку 1, а в таблиці 2 – приклад його застосування.

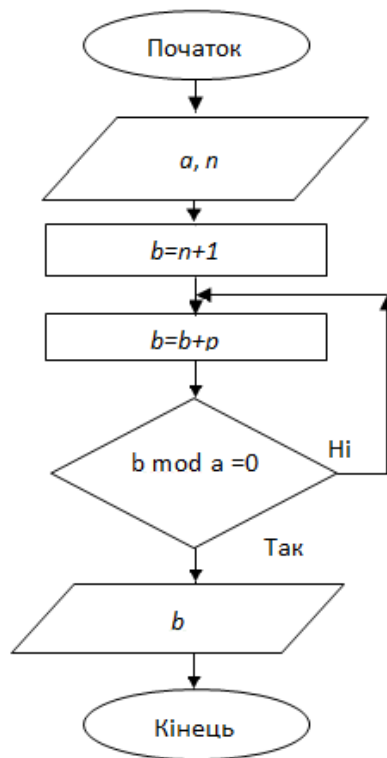


Рис. 1. Блок-схема пошуку оберненого елемента на основі додавання модуля

Таблиця 2.

Пошук оберненого елемента $41^{-1} \bmod 157$ на основі додавання модуля

i	0	1	2	3	4	5
n_i	158	315	472	629	786	943
b_i	3,85...	7,68...	11,51...	15,34...	19,17...	23

Отже, $41^{-1} \bmod 157 = 23$. Результат отриманий без використання громіздких операцій ділення з остачею та множення.

Для зменшення чисел, які використовуються в даній процедурі, можна додавати не модуль (дослідження часових характеристик апаратної реалізації цього методу

проведено, зокрема, в [17]), а залишок $n_{00} = n \bmod a$ до тих пір, поки остача від ділення отриманого результату на число a не буде дорівнювати 0. Математичний запис даного алгоритму матиме такий вигляд:

$$\begin{aligned} b_{01} &= (n_{00} + 1) \bmod a; \\ b_{11} &= (b_{01} + n_{00}) \bmod a; \\ b_{21} &= (b_{11} + n_{00}) \bmod a; \\ &\vdots \\ b_{i1} &= (b_{i-11} + n_{00}) \bmod a = 0. \end{aligned}$$

Обернений елемент шукається за формулою $b = a^{-1} \bmod n = (i+1)n/a$.

Блок-схема алгоритму пошуку оберненого елемента на основі додавання залишку представлена на рисунку 2, а в таблиці 3 – приклад його застосування з врахуванням, що $n_{00} = 157 \bmod 41 = 34$.

Отже, $41^{-1} \bmod 157 = (6 \cdot 157 + 1)/41 = 23$. Кількість ітерацій даного алгоритму така ж сама, як і в попередньому, однак переважна більшість операцій виконується над значно меншими числами.

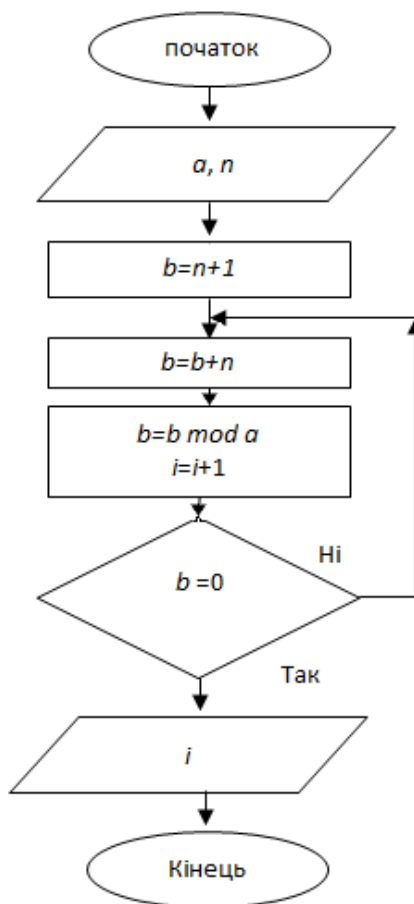


Рис. 2. Блок-схема пошуку оберненого елемента на основі додавання залишку

Таблиця 3.

Пошук оберненого елемента $41^{-1} \bmod 157$ на основі додавання залишку

i	0	1	2	3	4	5
b_{i1}	35	28	21	14	7	0

На відміну від розширеного алгоритму Евкліда, запропоновані методи дозволяють розпаралелити процес пошуку оберненого елемента на декілька потоків. Початок обчислень в кожному потоці для методів додавання модуля та залишку відповідно визначається з таких формул:

$$N_0 = \left(\left\lceil \frac{(j-1)a}{z} \right\rceil + 1 \right) n + 1; \quad (1)$$

$$N_1 = \left(\left(\left\lceil \frac{(j-1)a}{z} \right\rceil + 1 \right) n_{00} + 1 \right) \bmod a \quad (2)$$

де j - номер потоку, z - кількість потоків. Максимальна кількість ітерацій в кожному потоці становитиме $a/z+1$.

Для експериментальних досліджень було обрано портативний комп'ютер Lenovo B50-70 з процесором Intel Pentium 3558U (1.7 ГГц). Об'єм оперативної пам'яті в пристрої становив 4 GB. При проектуванні програмного комплексу, що забезпечував обчислення, було обрано мову програмування високого рівня C++, яка дозволяє трансформувати коди під різні архітектури та операційні системи.

Даний комп'ютер не дозволяє розпаралелювати обчислення на будь-яку кількість потоків, тому після визначення меж усі обчислення виконувалися послідовно, а час пошуку оберненого елемента за модулем вибирався в тому потоці, де знаходився шуканий результат.

На рисунку 3 показано графічну залежність середнього часу пошуку оберненого елемента на основі додавання модуля (штрихова лінія) та залишку (суцільна лінія) від кількості паралельних потоків z при $n=1021$ та $n=65521$ (рис. 3). Останні є найбільшими простими десяти- та шістнадцятирозрядними числами. Число a пробігає значення від 2 до $n-1$ з кроком 1.

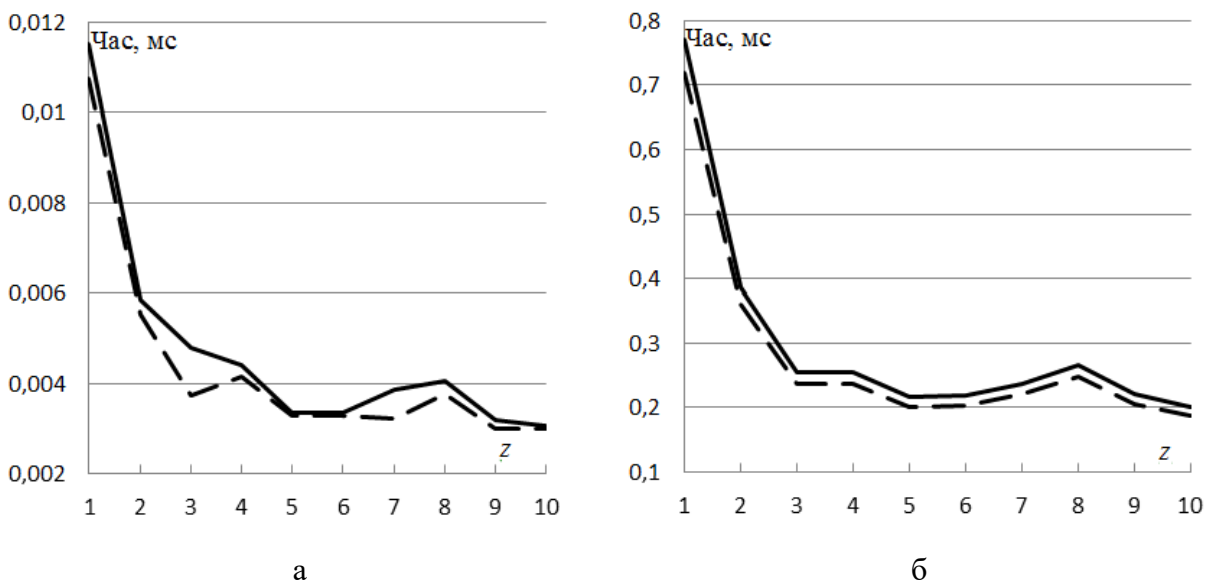


Рис. 3. Графічна залежність середнього часу пошуку оберненого елемента на основі додавання модуля (штрихова лінія) та залишку (суцільна лінія) від кількості паралельних потоків при: а – $n=1021$; б – $n=65521$

З рисунка 3 видно, що в обох випадках метод додавання модуля володіє більшою швидкістю, ніж додавання залишку. Графіки мають приблизно однаковий характер. При розпаралелюванні на два та три потоки час обчислень різко зменшується

порівняно з послідовним виконанням усіх операцій ($z=1$). При подальшому збільшенні z інтенсивність зменшення часу спадає. Незначне збільшення часу спостерігається, коли $z=7, 8$, і надалі графік повільно спадає. Тому для подальших досліджень було вибрано $z=6$.

На рисунку 4 показано графічну залежність часу пошуку оберненого елемента на основі додавання модуля (штрихова лінія) та залишку (суцільна лінія) при $z=6$ та $n=65521$, а в таблиці 4 представлений фрагмент з частиною отриманих результатів.

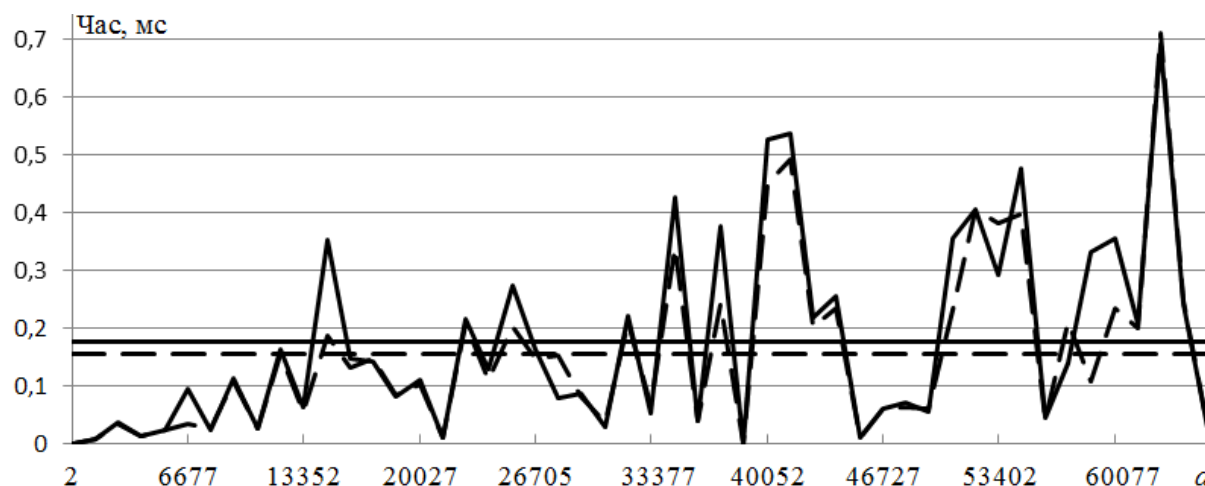


Рис. 4. Графічна залежність часу пошуку обернених елементів на основі додавання модуля (штрихова лінія) та залишку (суцільна лінія) при $z=6$ та $n=65521$ та середні часи обчислень (штрихова та суцільна прямі відповідно)

Таблиця 4.

Фрагмент з частиною отриманих результатів

a	b	Час пошуку, мс	
		Додавання модуля	Додавання залишку
17357	55744	0,146275	0,142446
18692	49968	0,08318	0,08077
20027	29906	0,10303	0,111585
21362	22510	0,009311	0,009736
22697	35106	0,207195	0,216458
24032	50643	0,109552	0,129591
25367	33547	0,202232	0,272227
26702	30557	0,146747	0,164092
28037	25648	0,152182	0,078502

Число a змінюється від 2 до 65417 з кроком 1335, який був вибраний з міркувань того, щоб розрахунки оберненого елемента здійснювалися для 50-ти значень. Крім того, наведено середній час обчислень обома методами (штрихова пряма – додавання модуля, суцільна пряма – додавання залишку). Графіки 1 і 2 носять осцилюючий характер, однак загальний тренд вказує на збільшення часу із ростом числа a . В переважній більшості випадків метод додавання модуля є швидший (усереднений час обчислень розглянутих прикладів становить 0,15499 мс), ніж метод додавання залишку (середній час – 0,176144 мс), в 1,136 рази.

На рисунку 5 показано графічну залежність середнього часу пошуку оберненого елемента на основі розширеного алгоритму Евкліда (крива 1) та запропонованих

методів додавання модуля (штрихові лінії 3, 5) та залишку (суцільні лінії 2, 4) при $z=1$ (криві 2, 3) і $z=6$ (криві 3,5) від розрядності модуля. Модуль n вибирався найбільшим простим, але меншим за 2^k , де k змінювалося від 10 до 19,5 з кроком 0,5. Число a набувало 1000 різних значень. Крок його зміни вибирався таким, щоб охопити весь діапазон від 1 до n .

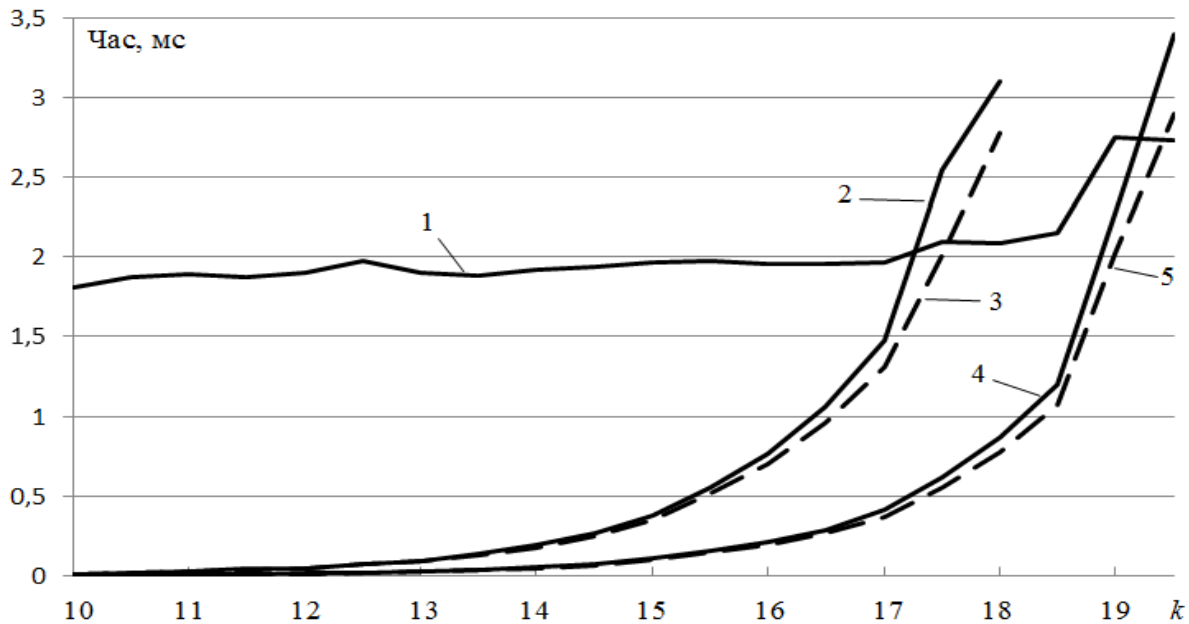


Рис. 5. Графічна залежність часу пошуку оберненого елемента від розрядності модуля на основі: 1 – розширеного алгоритму Евкліда; 2 – запропонованих методів додавання модуля при $z=1$; 3 – запропонованих методів додавання модуля при $z=6$; 4 – залишку при $z=1$; 5 – залишку при $z=6$;

Як видно з рисунка 5, при використанні алгоритму Евкліда із збільшенням розрядності чисел час збільшується дуже повільно. При $k=19$ час різко зростає і далі знову настає практично горизонтальна ділянка графіка. В обох запропонованих методах середній час збільшується приблизно параболічно, причому метод додавання модуля має більшу швидкодію. При $z=1$, тобто без розпаралелення, алгоритм Евкліда випереджає запропоновані алгоритми при $k=17,5$, а для $z=6$ – при $k=19,5$. Це вказує на необхідність розпаралелення процесу обчислень для зменшення часу пошуку оберненого елемента за модулем.

Для нівелювання випадкових впливів на час роботи усі експерименти повторювалися 100 разів.

Висновки

У роботі проведено експериментальне дослідження часових характеристик програмної реалізації пошуку оберненого елемента за модулем на основі класичного методу розширеного алгоритму Евкліда та запропонованих методів додавання модуля та додавання залишку із застосуванням мови програмування високого рівня C++. Показано, що в переважній більшості розглянутих випадків метод додавання модуля характеризується більш високою швидкодією в порівнянні з двома іншими. Представлено графічні залежності середнього часу пошуку оберненого елемента різними методами від розрядності вибраних чисел. Запропоновані методи ефективно можна використовувати для розпаралелення процесу обчислень та зменшення часу пошуку оберненого елемента за модулем.

Список літератури

1. Lorencz, R. New Algorithm for Classical Modular Inverse / R.Lorencz // Cryptographic Hardware and Embedded Systems. International Workshop, 2002. – Pp. 57-70.
2. Parthasarathy, S. Multiplicative inverse in mod(m) / S. Parthasarathy // Algologic Technical Report, 2012. – №1. – Pp. 1-3.
3. Kasyanchuk, M.M. Algorithms theory of RSA and El Gamal in differentiated notation of Rademacher-Krestenson basis / M.M. Kasyanchuk, I.Z. Yakymenko, O.I. Volynskiy, I.R. Pituh // Reports of Khmelnytsky National University. Technical sciences, 2011. – №3. – Pp. 265-273.
4. Hankerson, D. Guide to EllipticCurve Cryptography / D. Hankerson, A. Menezes, S. Vanstone.- New York, USA: Springer-Verlag, 2004. – 311 p.
5. Stallings, W. Cryptography and Network Security: Principles and Practice / W. Stallings. - New York, USA: Prentice Hall Press Upper Saddle River, 2010. – 719 p.
6. Omondi, A. Residue number systems: theory and implementation / A. Omondi, B. Premkumar. - London: Imperial College Press, 2007. – 296 p.
7. Kasyanchuk, M.M. Foundations for the Analytical Computation of Coefficients of Basic Numbers of Krestenson's Transformation / M.M. Kasyanchuk, Ya. M. Nykolaychuk, I. Z. Yakymenko // Cybernetics and Systems Analysis, 2014. – Vol 50, №5. – Pp. 649-654.
8. Nykolaychuk, Ya.M. Theoretical Foundations of the Modified Perfect Form of Residue Number System / Ya.M.Nykolaychuk, M.M.Kasyanchuk, I.Z.Yakymenko // Cybernetics and Systems Analysis, 2016. – Vol. 52, №2. – Pp. 219-223.
9. Kasianchuk, M. Conception of theoretical bases of the accomplished form of Krestenson's transformation and its practical application / M. Kasianchuk // Proceedings of the 4-th International Conference "Advanced Computer Systems and Networks: Design and Application" (ACSN-2009). – L'viv, Ukraine, 2009. – Pp. 299 - 301.
10. Яцків, В.В. Модифіковані коректуючі коди системи залишкових класів та їх застосування / В.В. Яцків // Інформаційні технології та комп'ютерна інженерія, 2013. – №2. – С. 39-45.
11. Zhengbing, Hu. The Analysis and Investigation of Multiplicative Inverse Searching Methods in the Ring of Integers Modulo M / Hu Zhengbing, I. A. Dychka, M. Onai, A. Bartkoviak // International Journal of Intelligent Systems and Applications (IJISA), 2016. – Vol. 8, №11. – Pp. 9-18.
12. Онай, М.В. Пошук мультиплікативно оберненого елементу у кільці лишків за довільним модулем методами, що ґрунтуються на модулярному піднесенні до степеня / М.В. Онай, А.Ю. Бартков'як // Матеріали шістнадцятої міжнародної наукової конференції імені академіка Михайла Кравчука. Т.2: Алгебра. Геометрія. Математичний аналіз. – Київ, 2015. – С. 139-141.
13. Kozaczko, D. Vector Module Exponential in the Remaining Classes System / D.Kozaczko, M.Kasianchuk, I.Yakymenko, S.Ivasiev // Proceedings of the 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS-2015),1, September, Warsaw, Poland, 2015. – Pp.161-163.
14. Касянчук, М.М. Експериментальне дослідження програмної реалізації методів модулярного експоненціювання / М.М.Касянчук, І.З.Якименко, Т.М.Долинюк, Н.А.Рендзеняк // Інформатика та математичні методи в моделюванні, 2015. – Т.5, №4. – С. 376 -382.
15. Дичка, І.А. Застосування k -арного методу Евкліда для пошуку мультиплікативно оберненого елемента у кільці лишків за модулем m / І.А. Дичка, М.В. Онай, А.Ю. Бартков'як // Матеріали статей П'ятої Міжнародної науково-практичної конференції «Інформаційні технології та комп'ютерна інженерія». - Івано-Франківськ, 2015. – С. 151-153.
16. Виноградов, И.М. Основы теории чисел / И.М.Виноградов. – Москва-Ижевск: НИЦ «Регулярная и хаотическая динамика», 2003. – 176 с.
17. Rajba, T. Research of Time Characteristics of Search Methods of Inverse Element by the Module / T. Rajba, A. Klos-Witkowska, S. Ivasiev, I. Yakymenko, M. Kasianchuk // Proceedings of the 2017 IEEE 9th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS-2017),1, September, Bucharest, Romania, 2017.– Pp.82 - 85.

ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ ПРОГРАММНОЙ РЕАЛИЗАЦИИ МЕТОДОВ ПОИСКА ОБРАТНОГО ЭЛЕМЕНТА ПО МОДУЛЮ

М.Н. Касянчук, И.З. Якименко, С.В. Ивасьев, О.В. Момотюк

Тернопольский национальный экономический университет,
ул. Львовская, 11, г. Тернополь, 46020, Украина; E-mail: kasyanchuk@ukr.net, jiz@tneu.edu.ua,
stepan.ivasiev@gmail.com, momotjuk98@gmail.com

Нахождение мультипликативного обратного элемента по модулю очень часто является необходимым условием для решения многих задач современной теории чисел, вычислительной и прикладной математики, асимметричной криптографии, в частности, криптосистем RSA и Эль-Гамала. В работе проведено экспериментальное исследование временных характеристик программной реализации поиска обратного элемента по модулю на основе классического метода расширенного алгоритма Евклида и предложенных методов добавления модуля и добавления остатка с использованием языка программирования высокого уровня C++. Для исследования использовались числа разной разрядности. Показано, что в подавляющем большинстве рассмотренных случаев метод добавления модуля характеризуется более высоким быстродействием в сравнении с двумя остальными. Представлены графические зависимости среднего времени поиска обратного элемента разными методами от разрядности выбранных чисел. Для нивелирования случайных влияний на время работы все вычисления повторялись 100 раз. Предложенные методы можно эффективно использовать для поиска обратного элемента по модулю.

Ключевые слова: алгоритм Евклида, обратный элемент по модулю, асимметричная криптография, добавление модуля, добавление остатка, среднее время, временные характеристики.

EXPERIMENTAL RESEARCH OF PROGRAM IMPLEMENTATION OF METHODS OF THE INVERSE ELEMENT SEARCH BY MODULE

M.M. Kasianchuk, I.Z. Yakymenko, S.V. Ivasiev, O.V. Momotjuk

Ternopil National Economic University,
11, Lvivska Str., Ternopil, 46020, Ukraine; e-mail: kasyanchuk@ukr.net, jiz@tneu.edu.ua,
stepan.ivasiev@gmail.com, momotjuk98@gmail.com

Finding a multiplicative inverse element by module is very often a necessary condition for solving many tasks of modern theory of numbers, computational and applied mathematics, asymmetric cryptography, in particular RSA and El Gamal cryptosystems. Experimental study of time characteristics of program implementation for finding the inverse element by module on the basis of the classical method of the extended Euclidean algorithm and the offered methods for adding a module and remainder addition with the use of high-level programming language C ++ was conducted in the work. The numbers of different bit capacity were used for the research. It was shown that in the majority of the considered cases the method of adding a module is characterized with higher performance compared to the other two. Graphic dependencies of average time of the inverse element search by different methods on bit capacity of the selected numbers were presented. All calculations were repeated 100 times for leveling random effects on the operating time. The proposed methods can be effectively used to find the inverse element by module.

Keywords: Euclid's algorithm, inverse element by module, asymmetric cryptography, addition module, remainder addition, average time, time characteristics.

УДОСКОНАЛЕННЯ СТЕГАНОАНАЛІТИЧНОГО МЕТОДУ ВИЯВЛЕННЯ ВКЛАДЕНЬ ДОДАТКОВОЇ ІНФОРМАЦІЇ В ЦИФРОВИХ ЗОБРАЖЕННЯХ, ЗАСНОВАНОГО НА АНАЛІЗІ ПОСЛІДОВНИХ ТРІАД КОЛІРНИХ ТРИПЛЕТІВ

Г.В. Ахматєєва, В.В. Мурова

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: a.v.akhmatieva@onu.ua

В роботі проводиться дослідження впливу модифікацій коефіцієнтів дискретного косінусного перетворення (ДКП) на просторову область цифрових зображень за допомогою аналізу послідовних тріад кольорних триплетів в матриці унікальних кольорів зображення з метою наступного стеганоаналізу стеганоповідомлень, сформованих шляхом модифікацій в області ДКП. На основі результатів обчислювальних експериментів проведено удосконалення розробленого раніше стеганоаналітичного методу виявлення наявності вкладень додаткової інформації в цифрових зображеннях, заснованого на аналізі послідовних тріад триплетів. Розроблено програмний інтерфейс в середовищі MATLAB для стеганоаналізу цифрових зображень.

Ключові слова: стеганоаналіз, цифрові зображення, дискретне косинусне перетворення, аналіз послідовних тріад триплетів, інтерфейс

Вступ

Широке розповсюдження інформаційних технологій та легкий доступ до мережі Internet надають величезні можливості для спілкування людей, які проживають в різних країнах світу, обміну між ними інформацією, яка може бути представлена у будь-якій формі: документи, зображення, аудіо, відео та інші. Доступність та зручність використання електронних засобів комунікації має також зворотну сторону – можна безконтрольно обмінюватися небезпечними для суспільства повідомленнями, схованими у будь-якій непримітний цифровий контент за допомогою стеганографічних методів, що дозволяє зберегти в таємниці сам факт існування такого спілкування. Для запобігання негативних наслідків прихованої комунікації актуальним є розвиток стеганоаналізу, основною задачею якого є виявлення факту наявності або відсутності вкладень додаткової інформації (ДІ) у будь-якому цифровому контенті [1-2].

В якості контейнерів для вбудови ДІ сьогодні, як правило, використовують цифрові зображення (ЦЗ), які завдяки наявності в них значної кількості надлишкової інформації забезпечують високу пропускну спроможність прихованого каналу зв'язку (ППС) при збереженні цілісності сприйняття зображення. Проте останні розробки в області стеганоаналізу [3-5] направлені на покращення ефективності детектування стеганоповідомлень (СП), сформованих вбудовою ДІ в цифровий контент саме при малих значеннях ППС. Зазначені методи здійснюють аналіз області перетворень цифрових контентів, що значно впливає на ефективність виявлення СП, сформованих при малих значеннях ППС. Найефективнішим стеганоаналітичним методом, інформація про який є доступною з відкритих джерел, спроможним ефективно

виявляти наявність ДІ, вбудованої в умовах малих значень ППС, є метод, що аналізує просторову область цифрових контентів і заснований на аналізі послідовних тріад кольірних триплетів у матриці унікальних кольорів ЦЗ, запропонований в [6].

Розроблений в [6] метод був апробований лише у випадку вбудови ДІ методом LSB в просторову область цифрових зображень [7]. В реальних умовах для вбудови ДІ, як правило, використовується область перетворень, зокрема область дискретного косинусного перетворення (ДКП). Модифікація коефіцієнтів ДКП лежить в основі поширених стеганографічних програм F5 [8] та останніх розробок [9-10]. Очевидно, що збурення коефіцієнтів ДКП призведуть до збурень в просторовій області ЦЗ, що може бути визначено за допомогою стеганоаналітичного методу, заснованого на аналізі послідовних тріад кольірних триплетів.

Мета і задачі роботи

Метою роботи є удосконалення стеганоаналітичного методу виявлення вкладень ДІ в ЦЗ, заснованого на аналізі послідовних тріад кольірних триплетів в матриці унікальних кольорів, що забезпечить його спроможність виявляти збурення в результаті модифікацій коефіцієнтів ДКП, що відбулися в результаті стеганоперетворення.

Для досягнення поставленої мети необхідно вирішити наступні *задачі*:

1. Проаналізувати вплив модифікацій коефіцієнтів ДКП 8×8-блоків ЦЗ, що відповідають низьким, середнім та високим частотам блоків, на значення яскравості кольірних складових в просторовій області при збереженні цілісності сприйняття ЦЗ;

2. На основі виявлених особливостей збурень значень яскравості кольірних складових ЦЗ удосконалити стеганоаналітичний метод, заснований на аналізі послідовних тріад кольірних триплетів в матриці унікальних кольорів цифрових контентів;

3. Розробити програмний інтерфейс в середовищі MATLAB для забезпечення зручного стеганоаналізу ЦЗ.

Оцінку візуальної цілісності модифікованого ЦЗ будемо визначати за допомогою PSNR – пікового відношення «сигнал-шум».

Основна частина

В якості контейнерів будемо розглядати кольорові ЦЗ в форматі з втратами, представлені у відповідності до кольірної схеми RGB. Кожний піксель ЦЗ представлений як триплет значень (r_{mn}, g_{mn}, b_{mn}) , r_{mn}, g_{mn}, b_{mn} - значення яскравості (m, n) -го пікселя червоної, зеленої і синьої кольірних складових відповідно. Усі унікальні триплети ЦЗ будемо називати унікальними кольорами, їх кількість дорівнює U .

В основі стеганоаналітичного методу [6] лежить аналіз кількості послідовних Red, Green- і Blue-тріад в матриці унікальних кольорів UCT розміром $U \times 3$, що містить U упорядкованих унікальних триплетів (r_k, g_k, b_k) , $k = \overline{1, U}$, де під послідовними Red-, Green- і Blue-тріадами розуміємо:

$$(r_k, g_k, b_k) \in UCT \text{ AND } (r_k - 1, g_k, b_k) \in UCT \text{ AND } (r_k + 1, g_k, b_k) \in UCT, k = \overline{1, U}; \quad (1)$$

$$(r_k, g_k, b_k) \in UCT \text{ AND } (r_k, g_k - 1, b_k) \in UCT \text{ AND } (r_k, g_k + 1, b_k) \in UCT, k = \overline{1, U}; \quad (2)$$

$$(r_k, g_k, b_k) \in UCT \text{ AND } (r_k, g_k, b_k - 1) \in UCT \text{ AND } (r_k, g_k, b_k + 1) \in UCT, k = \overline{1, U} \quad (3)$$

відповідно. При підрахуванні кількості послідовних тріад триплетів послідовна тріада асоціюється з середнім триплетом $(r_k, g_k, b_k) \in UCT$, для якого виконуються умови (1), (2) або (3) в залежності від виду тріади.

В роботах [6-7] було встановлено, що оригінальне ЦЗ містить не більше 2.5% середніх триплетів, які відповідають Red-, Green- і Blue-тріадам. В результаті модифікацій просторової області цифрових контентів кількість послідовних тріад значно зростає, що указує на проведенні перетворення в колірних складових ЦЗ. З метою виявлення збурень значень яскравості просторової області в результаті модифікацій коефіцієнтів ДКП за допомогою аналізу кількості послідовних тріад в матриці унікальних кольорів був проведений обчислювальний експеримент, в ході якого відбувалися модифікації коефіцієнтів ДКП однієї довільно обраної колірної складової ЦЗ, які відповідають низьким, середнім та високим частотам при збереженні цілісності сприйняття цифрового зображення за формулою

$$d_{ij}^* = k_{зміни} \cdot d_{ij}, i = \overline{1, 8}, j = \overline{1, 8}, \quad (4)$$

де d_{ij}, d_{ij}^* - значення коефіцієнтів 8×8 -блоків оригінального і модифікованого ЦЗ відповідно, $k_{зміни}$ - величина зміни коефіцієнту ДКП.

Обчислювальний експеримент проводився на основі 200 ЦЗ розміром 512×384 з бази ЦЗ UCID [11] в форматі TIF, які були Perezбережені в формат JPG з максимальною якістю стиску $Q=100$. Після модифікацій коефіцієнтів ДКП ЦЗ зберігається без втрат в форматі TIF.

В результаті обчислювального експерименту встановлено, що спостерігається не порушена цілісність сприйняття ЦЗ при:

- $k_{зміни} = \overline{0.75, 1.25}$ у випадку модифікації низькочастотних коефіцієнтів (середнє значення PSNR для 200 ЦЗ становить 45.7% для червоної, 46.14% – для зеленої, 42.55% - для синьої колірних складових);

- $k_{зміни} = \overline{0.5, 2}$ у випадку модифікації середньочастотних коефіцієнтів (середнє значення PSNR для 200 ЦЗ при $k_{зміни} = 2$ становить 43.9% для червоної, 43.59% – для зеленої, 41.95% - для синьої колірних складових);

- $k_{зміни} = \overline{0.4, 3.5}$ у випадку модифікації високочастотних коефіцієнтів (середнє значення PSNR для 200 ЦЗ при $k_{зміни} = 3.5$ становить 41.73% для червоної, 41.98% - для зеленої, 42.09% - для синьої колірних складових).

З урахуванням отриманих значень PSNR надалі значення змінної $k_{зміни}$ для коефіцієнтів ДКП в обчислювальному експерименті становлять: $k_{зміни}^{(low)} \in \{0.75, 1.25\}$ для низькочастотних коефіцієнтів, $k_{зміни}^{(middle)} \in \{0.5, 0.75, 1.5, 2\}$ для середньочастотних коефіцієнтів, $k_{зміни}^{(high)} \in \{0.85, 1.15, 1.25, 2, 2.5, 3, 3.5\}$ для високочастотних коефіцієнтів ДКП.

На наступному етапі обчислювального експерименту проводився стеганоаналіз отриманих в результаті модифікацій ЦЗ за допомогою аналізу вмісту послідовних тріад колірних триплетів та були отримані помилки першого роду – пропуск модифікацій ЦЗ, які наведені в табл. 1.

Як видно з табл. 1, стеганоаналітичний метод [6] ефективно визначає модифікації коефіцієнтів ДКП, які відповідають низьким та середнім частотам, та модифікації високочастотних коефіцієнтів ДКП при значеннях $k_{зміни} \geq 2$ незалежно від обраної колірної

складової. У випадку незначних модифікацій високочастотних коефіцієнтів ($k_{зміни} \in \{0.85, 1.15, 1.25\}$) спостерігаються до 7.5% помилок першого роду для червоної колірної складової, до 12.3% для синьої колірної складової, у випадку модифікацій високочастотних коефіцієнтів зеленої колірної складової майже всі зображення були визначені як оригінальні контейнери.

Таблиця 1.

Помилки першого роду в результаті виявлення модифікацій коефіцієнтів ДКП, %

	Низькі частоти			Середні частоти			
$k_{зміни}$	0.75	1.25		0.5	0.75	1.5	2
Red	0	0		0	0	0	0
Green	0	0		0	0	0	0
Blue	0	0		0	0	0	0
	Високі частоти						
$k_{зміни}$	0.85	1.15	1.25	2	2.5	3	3.5
Red	7.4627	7.4627	2.9851	0	0	0	0
Green	98.5294	98.5294	95.5882	0	0	0	0
Blue	12.3077	12.3077	6.1538	0	0	0	0

В результаті більш глибокого аналізу вмісту послідовних тріад триплетів в матриці унікальних кольорів ЦЗ, визнаних такими, що не містять вбудованої інформації, було встановлено, що причиною таких помилок можливі два варіанти:

1. Збурення коефіцієнтів ДКП незначні і значно не впливають на просторову область ЦЗ;

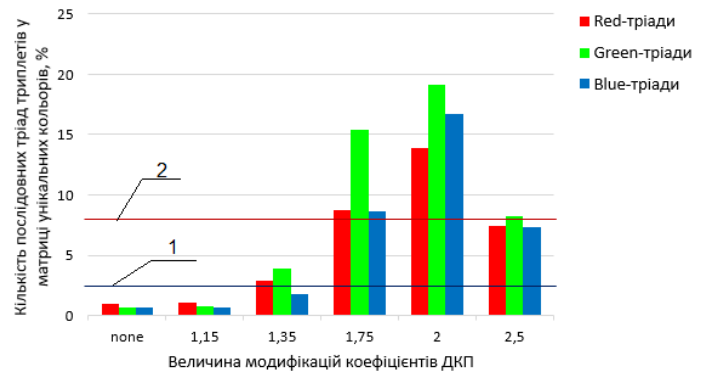
2. Збурення коефіцієнтів ДКП призводять до порівняно однакового вмісту послідовних тріад триплетів, які перевищують порогові значення стеганоаналітичного алгоритму $T_{low} = 2.5$ і $T_{up} = 8$.

Проілюструємо можливі збурення у кількості середніх триплетів на прикладі рис. 1. Два високочастотних коефіцієнти зеленої колірної складової ЦЗ, отриманого камерою мобільного пристрою, були модифіковані на величину $k_{зміни} \in \{1.15, 1.35, 1.75, 2, 2.5\}$ за формулою (4). Результуючі зображення зберігалися в форматі без втрат, для яких підраховано вміст послідовних Red-, Green-, Blue-тріад, де горизонтальні лінії 1 і 2 позначають рівень порогових значень T_{low} і T_{up} стеганоаналітичного методу [6] відповідно.

Згідно з кроками стеганоаналітичного методу, наведеними в [6], наявність додаткової інформації в розглянутому прикладі (рис. 1) буде виявлено лише у випадку $k_{зміни} \in \{1.75, 2, 2.5\}$, оскільки максимальне значення кількості послідовних тріад (Green-тріад) перевищує порогове значення T_{up} . При $k_{зміни} = 1.35$ кількість Red- і Green-тріад перевищує порогове значення T_{low} , однак не виконується умова $pG > 1.5 \cdot pR \ \& \ pG > 1.5 \cdot pB$, де pR, pG, pB - відсоток середніх триплетів, що відповідають Red-, Green-, Blue-тріадам відповідно, відносно до кількості унікальних кольорів, наслідком чого є помилка першого роду. При $k_{зміни} = 1.15$ зміни високочастотних коефіцієнтів значно не впливають на кількість послідовних тріад, які не перевищують порогове значення T_{low} . В деяких випадках модифікації коефіцієнтів ДКП призводять до збурень просторової області ЦЗ, але однозначно виявити колірну складову неможливо у зв'язку з близькими за значеннями pR, pG, pB , або у випадку, коли максимальний вміст послідовних тріад відповідає колірній складовій, яка не зазнала модифікацій.



а



б

Рис. 1. Зміни кількості послідовних тріад триплетів в результаті модифікації коефіцієнтів ДКП: а – оригінальне ЦЗ, б – кількість послідовних тріад триплетів в матриці унікальних кольорів в результаті модифікації значень коефіцієнтів ДКП на величину $k_{зміни}$; 1 – рівень порогового значення T_{low} , 2 – рівень порогового значення T_{up}

З метою більшої гнучкості при виявленні стеганоповідомлень та мінімізації помилок детектування було проведено удосконалення стеганоаналітичного методу, заснованого на аналізі послідовних тріад триплетів в матриці унікальних кольорів, основні кроки якого наступні:

Крок 1. Формування матриці UCT розміром $U \times 3$ унікальних триплетів кольорів (r_k, g_k, b_k) , $k = \overline{1, U}$ для ЦЗ I .

Крок 2. Підрахування кількості послідовних тріад триплетів для кожної колірної складової.

2.1. Якщо для поточного триплету (r_k, g_k, b_k) , $k = \overline{1, U}$ в UCT одночасно існують триплети $(r_k + 1, g_k, b_k)$ і $(r_k - 1, g_k, b_k)$, то $countR = countR + 1$, $countR$ – кількість Red-тріад в UCT ;

2.2. Якщо для поточного триплету (r_k, g_k, b_k) , $k = \overline{1, U}$ в UCT одночасно існують триплети $(r_k, g_k + 1, b_k)$ і $(r_k, g_k - 1, b_k)$, то $countG = countG + 1$, $countG$ – кількість Green-тріад в UCT ;

2.3. Якщо для поточного триплету (r_k, g_k, b_k) , $k = \overline{1, U}$ в UCT одночасно існують триплети $(r_k, g_k, b_k + 1)$ і $(r_k, g_k, b_k - 1)$, то $countB = countB + 1$, $countB$ – кількість Blue-тріад в UCT .

Крок 3. Обчислити кількість середніх триплетів послідовних тріад відносно загальної кількості унікальних кольорів (%):

$$pR = \frac{countR}{U} \cdot 100, \quad pG = \frac{countG}{U} \cdot 100, \quad pB = \frac{countB}{U} \cdot 100, \quad p_{\max} = \max(pR, pG, pB),$$

де $p_{\max}$ – максимальне значення серед pR, pG, pB .

Крок 4. Детектування наявності/відсутності ДІ.

4.1. Якщо

$$(pR = p_{\max}) \& (pR > T_{up} \& (pR > 1.5pG \parallel pR > 1.5pB) \parallel (pR > 1.75pG \parallel pR > 1.75pB)),$$

то I містить вбудовану ДІ у червоній колірній складовій;

інакше крок 4.2.

4.2. Якщо

$$(pG = p_{\max}) \& (pG > T_{up} \& (pG > 1.5pR \parallel pG > 1.5pB) \parallel (pG > 1.75pR \parallel pG > 1.75pB)),$$

то I містить вбудовану ДІ у зеленій колірній складовій,
інакше крок 4.3.

4.3. Якщо

$$(pB = p_{\max}) \& (pB > T_{up} \& (pB > 1.5pG \parallel pB > 1.5pR) \parallel (pB > 1.75pG \parallel pB > 1.75pR)),$$

то I містить вбудовану ДІ у синій колірній складовій,
інакше крок 4.4.

4.4. Якщо $pR < T_{low}$ & $pG < T_{low}$ & $pB < T_{low}$,

то наявність вбудованої ДІ в I не виявлено,
інакше наявність вбудованої ДІ в I виявлено,
де $T_{low} = 2.5$ і $T_{up} = 8$ – порогові значення.

Обчислювальна складність запропонованого алгоритму для обробки ЦЗ розміром $M \times M$ визначається як $O(M^4)$.

Для виконання стеганоаналізу ЦЗ та дослідження впливу змін коефіцієнтів ДКП на просторову область ЦЗ в середовищі в MATLAB було реалізовано програмний інтерфейс, представлений на рис. 2.



Рис. 2. Інтерфейс програмної реалізації стеганоаналітичного алгоритму

Форма інтерфейсу складається з наступних елементів:

1. Області «Вхідне зображення» і «Вихідне зображення», які відображають оригінальне ЦЗ та ЦЗ, отримане в результаті перетворення, відповідно.

2. Кнопка «Завантажити зображення», з якої починається робота в програмі, дозволяє завантажити ЦЗ для аналізу (може бути обрано ЦЗ як в форматі з втратами, так і в форматі без втрат). Результат: на формі в області «Вхідне зображення» з'являється обране ЦЗ.

3. Кнопка «Перевірити зображення» виконує стеганоаналіз обраного ЦЗ – це може бути як оригінальний контейнер, так і СП. Результат виводиться в текстовому полі «Додаткова інформація».

4. Блок «Перетворення» дозволяє обрати колірну складову, яка буде використовуватися для перетворення, задати індекси двох коефіцієнтів ДКП та

величину зміни заданих коефіцієнтів. Після введення необхідних параметрів натискається кнопка «Виконати». Результат: в області «Вихідне зображення» з'являється результуюче зображення, а також вікно для вибору місця збереження зображення в форматі TIF.

5. Блок «Аналіз» дозволяє виконати стеганоаналіз сформованого зображення. Результат: в полі «PSNR» виводиться значення PSNR порівняння оригінального і результуючого зображень, в полі «Додаткова інформація» виводиться результат стеганоаналізу.

Висновки

В роботі проаналізовано вплив модифікацій коефіцієнтів ДКП на просторову область ЦЗ за допомогою аналізу послідовних тріад кольірних триплетів в матриці унікальних кольорів ЦЗ. Встановлено, що модифікації як низькочастотних, так і середньочастотних і високочастотних коефіцієнтів ДКП призводить до збурень у кількості послідовних Red-, Green-, Blue-тріад, які можна виявити відповідним стеганоаналітичним методом.

Визначено, в яких випадках спостерігаються помилки детектування СП, аналіз яких дозволив удосконалити стеганоаналітичний метод виявлення наявності вкладень ДД, заснований на аналізі послідовних тріад триплетів.

Було спроектовано та реалізовано програмний інтерфейс в середовищі MATLAB для забезпечення зручного управління перетворенням в результаті модифікацій коефіцієнтів ДКП та стеганоаналізу цифрових зображень.

Список літератури

1. Стеганография, цифровые водяные знаки и стеганоанализ: [монография] / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин, С.А. Сапожников. — М.: Вузовская книга, 2009. — 220 с.
2. Bohme, R. Advanced statistical steganalysis / R. Bohme. — Springer, 2010. — 302 p.
3. Jinyang Su. Steganalysis using regional correlation and second-order Markov features / Su Jinyang, Zeng Xianting, Wang Lei // International Journal of Security and Its Applications, 2015. — Vol. 9, № 1. — Pp. 69-76.
4. Fengyong Li. JPEG Steganalysis With High-Dimensional Features and Bayesian Ensemble Classifier / Fengyong Li, Xinpeng Zhang, Bin Chen, and Guorui Feng // IEEE signal processing letters, 2013. — Vol. 20, № 3. — Pp. 233-236.
5. Manisha Saini. DWT feature based blind image steganalysis using neural network classifier / Manisha Saini, Rita Chhikara // International Journal of Engineering Research & Technology (IJERT), 2015. — Vol. 4, Issue 04. — Pp. 776-782.
6. Ахматметьева, А.В. Стеганоанализ цифровых изображений, хранящихся в формате с потерями / А.В. Ахматметьева // Захист інформації, 2016. — Вип.23. — С.135-145.
7. Ахматметьева, А.В. Выявление области применения стеганоаналитического подхода, основанного на анализе пространственной области цифровых контентов / А.В. Ахматметьева // Problemele energeticii regionale [Проблемы региональной энергетики]. Электронный журнал Академии наук Республики Молдова, 2016. — № 2 (31). — С. 104-111.
8. Fridrich, J. Statistically undetectable JPEG steganography: Dead ends, challenges, and opportunities / J. Fridrich, T. Pevný, J. Kodovský // In J. Dittmann and J. Fridrich, editors, Proceedings of the 9th ACM Multimedia & Security Workshop. — 20-21 September, 2007. — Pp. 3-14.
9. Anupam Mondal. A Novel Approach of Image Based Steganography Using Pseudorandom Sequence Generator Function and DCT Coefficients / Anupam Mondal, Shiladitya Pujari // I. J. Computer Network and Information Security, 2015. — №3. — Pp. 42-49.
10. Arshiya Sajid Ansari. JPEG Image Steganography based on Coefficients Selection and Partition / Arshiya Sajid Ansari, Mohammad Sajid Mohammadi, Mohammad Tanvir Parvez // I.J. Image, Graphics and Signal Processing, 2017. — №6. — Pp. 14-22.

11. Uncompressed Color Image Database (UCID) [Электронный ресурс]: Multimedia Phylogeny Datasets. Режим доступа: <http://www.recod.ic.unicamp.br/~oikawa/datasets.html> (дата звернения: 08.10.2017).

**УСОВЕРШЕНСТВОВАНИЕ СТЕГАНОАНАЛИТИЧЕСКОГО МЕТОДА ВЫЯВЛЕНИЯ
ВЛОЖЕНИЙ ДОПОЛНИТЕЛЬНОЙ ИНФОРМАЦИИ В ЦИФРОВЫХ ИЗОБРАЖЕНИЯХ,
ОСНОВАННОГО НА АНАЛИЗЕ ПОСЛЕДОВАТЕЛЬНЫХ ТРИАД ЦВЕТОВЫХ ТРИПЛЕТОВ**

А.В. Ахматетьева, В.В. Мурова

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: a.v.akhmametieva@opu.ua

В работе проводится исследование влияния модификаций коэффициентов ДКП на пространственную область цифровых изображений, используя анализ последовательных триад цветных триплетов в матрице уникальных цветов изображения, с целью дальнейшего стеганоанализа стеганообобщений, сформированных путем модификации области ДКП. На основе проведенных вычислительных экспериментов проведено усовершенствование разработанного ранее стеганоаналитического метода выявления наличия вложений дополнительной информации в цифровых изображениях, основанного на анализе последовательных триад триплетов. Разработан программный интерфейс в среде MATLAB для стеганоанализа цифровых изображений.

Ключевые слова: стеганоанализ, цифровые изображения, дискретное косинусное преобразование, ДКП, анализ последовательных триад триплетов, интерфейс

**IMPROVEMENT OF THE STEGANALYTIC METHOD FOR DETECTING THE ADDITIONAL
INFORMATION ATTACHMENTS IN DIGITAL IMAGES, BASED ON THE ANALYSIS OF
SEQUENTIAL TRIADS OF COLOR TRIPLETS**

A.V. Akhmametieva, V.V. Murova

Odesa National Polytechnic University,
1 Shevchenko Ave., Odesa, 65044, Ukraine; e-mail: a.v.akhmametieva@opu.ua

In the paper we study the effect of modification of DCT coefficients on the spatial domain of digital images using analysis of sequential triads of color triplets in a matrix of unique colors of the image, for further steganalysis of stego formed by modifying the DCT domain. On the basis of the computational experiments the improvement of the previously developed steganalytic method for detecting the presence of additional information attachments in digital images was carried out. A software interface for steganalysis of digital images was developed in MATLAB environment.

Keywords: steganalysis, digital image, discrete cosine transform, DCT, analysis of sequential triplets of triplets, interface

ПРОГНОЗУВАННЯ НАДІЙНОСТІ ПРОЦЕСУ ФУНКЦІОНУВАННЯ СКЛАДНИХ СИСТЕМ ТА РИЗИК ЇХ ВІДМОВИ

В.О. Хорошко, Ю.Є. Хохлячова

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

В роботі розглядаються базові фундаментальні чинники змісту математичної моделі, яку прагнемо побудувати, а саме, прогнозування надійності процесу функціонування складних систем та ризик їх відмови в найголовнішому базовому вигляді цих показників. Це є ймовірність безвідмовного процесу функціонування системи (надійність та живучість) в певних просторових і технологічних умовах протягом певного проміжку часу та за цих же умов – ймовірність відмови (ризик) систем.

Ключові слова: надійність складних систем, прогнозування надійності, ризик відмови складних систем, живучість систем.

Вступ

Однією з головних проблем науки та техніки є створення складних систем різного призначення, від ефективності й надійності функціонування яких залежать всі області діяльності суспільства. Прикладом таких систем є інформаційно-обчислювальні системи та мережі, автоматизовані системи керування складними процесами та інші. Зростаюча складність цих систем не дозволяє забезпечити необхідний рівень надійності та живучості функціонування їх тільки за рахунок підвищення якості складових елементів. Теоретичні дослідження та практика експлуатації показали, що необхідно врахувати ризик їх відмови та його вартість.

Дослідження взаємозв'язаної та емпіричної залежності ризику та його вартості, де під ризиком розуміється його базове тлумачення як ймовірності негативної події або ризик розуміється в абсолютному вигляді. В результаті аналізу формуються підходи до побудови математичної моделі функції вартості ризику у вигляді аналітичного виразу з метою використання її в можливому процесі оптимізації складних систем [1].

Якщо досліджувати сучасний рівень системного підходу до вивчення об'єктивних процесів, які відбуваються в суспільстві взагалі і в його компонентах – управлінні, технології, економіці, то неважко встановити, що вік ґрунтується на двох складових. Перша складова, а точніше, первинна, що визначається об'єктивною реальністю, – це аналогії, які характеризують усі процеси, де б вони не протікали, чи у суспільстві, чи в його окремії галузі, зокрема в складній техніко-технологічній системі. Друга складова є більш суб'єктивною. Це формальне виділення, ідентифікація та формалізація цих аналогій, інформаційне втиснення їх змісту в межі рівнянь, нерівностей чи інших математичних об'єктів, розбіг яких допустимий за потреби використання. Тому альфа та омега системного підходу до вивчення всього цілого та компонент є дослідження процесу функціонування складних систем, а вірніше, процесу якісного функціонування, де критерій якості будується відповідно до потреб способів або засобів використання системи. Побудова критерію якості є одним з найскладніших наукових завдань, розв'язання якого теоретично зумовлює реальні можливості

досягнення показника його певного рівня. Тому від аналітичного його вигляду (чи іншої структури математичної моделі) залежить можливість його оптимізації чи іншої раціоналізації, адже поки що може бути не розроблений (або в принципі не існувати) математичний апарат, що забезпечує реалізацію цієї процедури. Звідси випливає, що вирішально важливо будувати критерій, враховуючи та зважаючи на його реальну форму й зміст, бо перше допускає математичну можливість вирішення задачі, а друге – досягнення саме тих цілей (чи близьких до них первісних або похідних), що задовольняють дослідника-розробника. Саме цим пояснюється надзвичайно поширена форма критерію якості у вигляді лінійної моделі, бо лінійне програмування є найбільш розроблена й вивчена галузь математичних моделей, хоча рівень застосовності розв’язання лінійних завдань досить низький в силу дуже наближеного, в основному, модельного відображення реальному процесу лінійними залежностями, тобто в силу низької адекватності математичної моделі.

Основна частина

В багатьох реальних вирішених практичних задачах лінійні моделі приносили й приносять надзвичайну користь, і класичні приклади цього твердження широко відомі в теоретичній та застосованій літературі [1-4]. В зв’язку з цим виникають питання: лінійність - це є форма чи це є зміст моделі? Де знаходиться границя між формою та змістом в моделі? Чи існує така границя? Це надзвичайно цікаві аспекти проблеми математичного моделювання, і відповідь на них можна знайти, починаючи з кінця, тобто з цільової функції, що формулюється потребами споживача. Хоча можна виділити фундаментальні базові чинники, які, по-перше, необхідні для складання форми моделі (клас математичного об’єкту, наприклад, клас неперервних функцій та ін.) і так само необхідні для складання змісту моделі (прогноз надійності та живучості систем, прогноз ризику). Між тим крайніми фундаментальними чинниками модель може містити показники, що еволюціонують від форми до змісту і навпаки, в залежності від кінцево сформованої цільової функції завдання та накладених на неї обмежень. Для прикладу можна навести елемент моделі – експоненціальна функція. Цілком ясно, що вона є об’єктом форми при визначенні певних числових розв’язків з її застосуванням, але не менш зрозуміло, що вона є змістом моделі при дослідженні й оцінюванні її адекватності.

З цього випливає, що математична модель є надзвичайно глибоким і об’ємним сховищем інформації, що визначається певними показниками, грані істини яких повертаються до нас чи формою моделі, чи її змістом. І така діалектична сутність (діалектика полягає в тому, що один чинник є в другому, для другого і через другий чинник і навпаки) її надзвичайно цікава, але з’ясування сутності зв’язку відкладемо, бо це є змістом іншого дослідження. В даній роботі нас цікавлять базові фундаментальні чинники змісту математичної моделі, яку прагнемо побудувати, а саме, прогнозування надійності процесу функціонування складних систем та ризик їх відмови в найголовнішому базовому вигляді цих показників. Це є ймовірність безвідмовного процесу функціонування системи (надійність та живучість) в певних просторових і технологічних умовах протягом певного проміжку часу та за цих же умов – ймовірність відмови (ризик) систем. Позначимо ці ймовірності відповідно через p та x , тоді, згідно з визначенням:

$$p + x = 1, \quad (1)$$

бо нічого не може відбуватися інакше, ніж те, що якимось відбувається – це філософське тлумачення, а імовірна сутність – альтернативність подій, кожна з яких протилежна іншій і в сумі складають увесь простір подій.

Опоненти можуть заперечувати такому погляду, бо на їх погляд є примітивізм в трактуванні ризику. Адже введена величина x настільки є проста, хоча математично прозора і змістовно ємна, настільки й змістовно бідна, що не відрізняє ймовірність x -ризiku не зустрітись з «приятелем» від цієї ж таки ймовірності x (те ж саме числове значення). Навіть більше, в x не видно ні розсіювання значень випадкової величини, ні математичного очікування її чи функції від неї, ні поганих, або й катастрофічних наслідків її низького рівня, ні транжирного вираження коштів на забезпечення цього рівня x -ризiku втрати зустрічі з подією. Хочемо заспокоїти опонентів, Ви маєте рацію, Ви праві. Особливо, якщо зважити на термін «ризик в абсолютному виразі» [2,4], що майже повністю змістовно співпадає з (1), або «системні показники ризику» [2,4], що перегукуються з системою показників ризику, з їх можливими межами значень. Але не менше від опонентів і ми претендуємо на істину. Річ в тому, що визначення й твердження опонентів лежать в одній півплощині, наші – в іншій. І вони поки що не перетинаються. На нашу користь можна віднести те, що в пропонованому тлумаченні x є базовим для моделі, а тому плідним для побудови інших показників, що конструктивно можуть і мають бути певними функціями від ризику x чи його вибіркового значень оцінки, або бути функціоналами різного споживчого типу на траєкторіях статистичного процесу надійності (живучості) і ризику функціонування складної системи. Але в основі лежить той самий x . Підкреслимо, що в запропонованій схемі ризик – категорія якісна, категорія якісного стану об'єкта, тому виміряти його можливо лише ввівши вимір (міру) якості. Це ж можна зробити, якщо побудувати показники якості (ризiku), причому не просто показники, а, наголошуємо, вимірні показники. Вважаємо, що крок на цьому шляху зроблено: це показник в абсолютному вигляді [4], або x в формулі (1).

Якщо (1) є моделлю, то, що чітко окреслюється образом, а що прообразом, і які взаємозалежні можуть трактуватись цим співвідношенням, має певний інтерес до трактувань відносно причинно-наслідкового зв'язку, що пов'язується з ризиком, точніше з рівнем його показника x . Але це не є в цій роботі науковою теорією, тобто теорією, що нами досліджується. Це є щось інше. Воно знаходиться в прикладній, тобто застосовній галузі, а там є свої цінності, свої форми й зміст і принаймні лише для них критерії. Ми створюємо теоретичний інструмент, вдосконалюємо, поліпшуємо його застосовні властивості. Але саме застосування – предмет окремої дослідної роботи. Особливо важливим є те, що при цьому показник ризику x – інформаційно невичерпний, і кожен з нього може почерпнути стільки, скільки може. Для тих, хто не хоче напружувати мислення, наведемо приклад, що зачіпає лише застосовану складову його інформаційної місткості.

1. Ризик (ймовірність) не зустріти приятеля $x=0,01$. Це практично є достеменною подією зустрічі, фактично ризику не має. Число 0,01 є надзвичайно малим, цим можна знехтувати.

2. Ризик (ймовірність) відказа складної системи (наприклад, поломка літака в польоті) $x = 0,01$. Адже це явна загроза катастрофи. Число 0,01 є дуже великим.

Одне й те саме число (як рівень показника ризику) в залежності від погляду споживача може бути надзвичайно малим, яким можна знехтувати, і катастрофічно великим. Маємо надію, що наведені аргументи в деякій мірі можуть задовольнити опонентів.

Далі продовжимо досліджувати величини p і x з метою використання їх в математичній моделі функції вартості ризику, сутність якої буде висвітлено далі. Тут ми вважаємо доречним стверджувати, що категорії надійності (живучості) і ризику є вічними. Тобто, скільки існує цивілізація, людина завжди оцінювала ризик і надійність

існування, наступного свого кроку. Нехай інтуїтивно, наївно, але оцінювала. Лише зі зростанням культури мислення вона відокремила ці поняття і тепер стала нерозлучна з ними все життя. Тому наука Ризику, наука Надійності (живучості) є вічною, скільки і як не розвиватиметься суспільство. Ця наука збагачуватиметься новими моделями, застосовними процедурами, щоб задовольнити неперервно зростаючі потреби людини в суспільстві її з іншими методами та засобами продуктів розвитку цивілізації. І завжди ці моделі будуть містити показники p і x , або їх похідні модифікації, що гарантуватиме зростання їх адекватності. Тому зрозумілим вважається, що висока якість об'єкту має базуватись на високому рівні його живучості (надійності), на допустимо низькому рівні ризику.

Далі спрямуємо міркування на з'ясування вартості ризику. Щоб зменшити ризик, потрібні певні затрати, тому логічним є поняття «вартості ризику», а точніше «вартість рівня x ризику», що визначається витратами на його досягнення.

Якщо дивитися на речі зі сьогодення, то в сучасних умовах ускладнювались системи, тому оцінка ризику є необхідною вже на стадії їх розробки та проектування [3,4]. Роботи з досягнення оптимального ризику обов'язково повинні починатися на ранніх стадіях розробки складних систем та продовжуватися на стадії її виробництва. Це набуває особливої ваги у випадку, коли розробка підсистем складної системи проводиться різними інститутами, а виробництво її здійснюється теж на різних підприємствах. Якщо за цих умов не наведені певні критерії ризику та не накладені певні обмеження на характеристики ризику окремих частин системи та підсистем, то може бути сформоване певне судження щодо можливості систем, тобто її тактико-технічні характеристики, і загалом можливості застосування й споживчі чинники якості. Тому виникає задача встановлення вимог до складних по ризику для окремих елементів та вузлів системи, що базується на вимогах до ризику по всій системі. Якщо розподіл вимог реалізувати довільно, то ця задача має, взагалі кажучи, безліч розв'язків. Як з цієї необмеженої множини визначити раціональне рішення, тобто в деякому сенсі оптимальне, – питання, що є сутністю поставленої тут задачі. Один з можливих способів відповіді на дане питання і розглядається далі.

Розрахунок оптимальних характеристик складової ризику кожного елемента системи, який би впливав з вимог до системи в цілому, є важливою проблемою початкового стану розробки та конструювання складної системи. Не зовсім коректно вжити термін «елемент» в роботі. Він вживається лише в смислі відносно простоти у порівнянні зі всією складною системою. Сам по собі елемент може бути також складною системою, і, можливо, доцільніше говорити про складну систему, створену своїми підсистемами.

Переходячи від загальних міркувань до конкретних, бачимо, що задача визначення допустимого рівня ризику в роботі того чи іншого елемента на основі встановлених вимог до ризику системи очевидно розв'язується неоднозначно. Кількість всіх можливих рішень, взагалі кажучи, складає теоретично $(n-1)$ -параметричну множину, де n – число, що дорівнює кількості елементів системи.

Очевидність цього твердження розглянемо на прикладі. Припустимо, що система, яка складається з десяти елементів, повинна мати ризик 5%, тобто з імовірністю 0,05 вийти з ладу, не пропрацювавши певний проміжок часу. Але характеристика ризику системи визначається параметрами ризику елементів. Якщо через x позначити функцію ризику системи, то в розглянутому прикладі

$$x(x_1, x_2, \dots, x_{10}) = 0.05, \quad (2)$$

де x_i – характеристика ризику i -го елемента ($i = 1, 2, \dots, 10$).

Таким чином, рівняння (2) є загальним математичним записом тих вимог та обмежень, які накладаються на елементи системи, а точніше на їх характеристики ризику. Але оскільки рівняння (2) має десять змінних $x_1, x_2, \dots, x_{10}$, то значення дев'яти з

них можна вибрати довільно, і лише ризик одного елемента доведеться розрахувати, виходячи з ризику системи та ризику вибраних дев'яти елементів. Користуючись рівнянням (2), це можна записати так:

$$x_j = x^{-1}(x_1, x_1, \dots, x_i, \dots, x_{j-1}, x_{j+1}, \dots, x_{10}), j = 1, 2, \dots, 10; i = 1, 2, \dots, j-1, j+1, \dots, 10, \quad (3)$$

де x^{-1} – обернена функція до функції (2), x_i – характеристика i -го елемента з тієї дев'ятки, для кожного елемента якої довільно вибиралися вимоги по ризику, x_j – розрахунковий ризик j -го елемента. Довільність вибору значення ризику елементів тут розуміється не в формально математичному, а в фізичному сенсі. Це означає, що значення x_i вибирається з можливих допустимих значень i -го елемента. Отже, знайдений зі співвідношення (3) x_j , є коренем рівняння (2), в якому всі x_i при $i \neq j$ фіксовані й фігурують в рівнянні як параметри. Оскільки кількість цих параметрів дорівнює дев'яти, то кількість значень x_i являє собою нескінченну дев'яти-параметричну множину.

З прикладу випливає, що задача визначення вимог до ризику кожного елемента системи, які ґрунтуються на вимогах до ризику всієї системи, має нескінченну множину рішень. Кожне з таких рішень має свої індивідуальні особливості та в певному сенсі свої недоліки та недосконалості й свої позитивні якості. Тому й постає проблема: як з безмежної кількості рішень визначити оптимальне за повним критерієм, чи хоча б раціональне? На практиці в більшості випадків цю проблему поки що розв'язують наступним чином. Знаходять декілька рішень даної проблеми, а потім їх евристично оцінюють. В залежності від досвіду розробника знайдені рішення будуть різними, кожен з них матиме свої позитивні та негативні сторони. У подальшому з побудованих рішень вибирають найкраще за евристичними міркуваннями та уявленнями розробника системи і згідно до нього проєктують систему. Але найкраще рішення з даної сукупності емпірично побудованих рішень ще не є найкращим з можливих, тобто оптимальним. Разом з тим під час розв'язання практичних задач розробники за відсутності математично-аналітичних даних досить часто мають задовольнятися лише цим наближенням, далеким від оптимального рішення.

Буває, що заради того, щоб хоч якось знайти рішення задачі, всі зв'язки та функціональні залежності, які мають місце в даній проблемі, лінеаризують, а потім з таким досить вільним припущенням розв'язують задачу лінійного програмування. Але це не є виходом із проблеми, оскільки лінійні моделі не можуть чітко та адекватно описати ймовірність процесу ризику.

В сучасних умовах, коли з'являються все складніші системи, проблема оптимального розподілу вимог до елементів системи стає надзвичайно актуальною. За оптимальним рішенням цієї задачі доводиться враховувати багато факторів, що впливають і на ризик у системі, і на саму структуру рішення. Так, рівень ризику у системі залежить певною мірою від обсягу проведених під час конструювання дослідницьких робіт, розмірів системи, маси системи тощо.

На рівень ризику системи також впливають інтервали допусків параметрів її елементів, контроль якості деталей під час виготовлення, типи й методи випробування та багато інших факторів. Все це має прямий зв'язок з витратами коштів. При більших витратах коштів на деякий елемент для його розробки може бути залучена більша кількість людей, кращі фахівці, досконаліше обладнання, використання сировини вищої якості, досягнутий кращий контроль якості продукції, та можуть бути проведені більш якісні випробування системи, в тому числі на ризик. Таким чином, чим більше коштів було вкладено в розробку та виробництво, тим вищу якість виключаючи ризик, матиме розроблювана система.

Таким чином, за аналогією з [5], можна стверджувати, що існує жорсткий зв'язок, детермінований чи стохастичний, між кількістю витрат на якість системи і рівнем

ризик x . Тобто має сенс говорити про вартість рівня ризику x , або про функцію вартості ризику, яку позначимо через $B(x)$, тобто:

$$B = B(x). \quad (4)$$

Необхідно дослідити властивості (4), які диктуються як фізичним змістом трактування змінних і констант, так і математичною структурою.

Ризик – це прорив крізь невизначеність у невідомість з недостатньо проінформованим (поінформованим) майбутнім, де можливо підстерігають нас негативні наслідки. Там, де зростає інформованість, зменшується невизначеність і зникає ризик. Якщо через A позначимо випадкову подію, яка відображає (моделює) невизначеність небажаного наслідку її випробування, то можливі наслідки його визначатимуть наслідки цього ризику – випробування. Тоді випробування - ризик? Не зовсім так, це щось ширше інформативно.

Визначення. Ризиком називається стан передвипробування або випробування випадкової події, невизначеність настання наслідку якого усвідомлено з небезпекою, але з надією на її оминучість. Ризик – це те, що передує відповіді на проблему, яка поставлена особою, що приймає рішення; ризик-фактор – це фактор (випадок, складний елемент A), що сприяє негативному наслідку випробування.

Визначення. Ймовірність (P) того, що при випробуванні події A настане небажаний результат, називається індексом ризику: $P = P(A)$. Дана імовірність є базовою характеристикою ризику. Всякий ризик формує так звану зону, в якій напруженість ризикового середовища визначається у відсотках за формулою $H = P * 100\%$.

Ризик і безпека. Нехай в стахостичному (ризиковому) середовищі розглядається деякий об'єкт, який ми позначимо подією A^0 . Взагалі кажучи, можна говорити про інформаційний об'єкт, який описується задовільно визначеним станом його перебування. Будемо розглядати подію A , як таку, що моделює (відображає образ, реальний об'єкт – оригінал або прообраз) визначений стан його перебування. А це значить, що з погляду стохастики можливий інший стан його, який не є визначеним в попередньому сенсі. Оскільки в даний момент t_1 часу A^0 знаходиться (а це і є випробування) у визначеному стані, то в результаті випробування в момент, де $t_2 > t_1$ подія A може перейти в інший стан, що не є визначений, а також може зберегти цей стан. Ризик зміни стану (такого переходу) позначимо через α (індекс ризику), а імовірність (надійність) збереження його – через β . Нехай в даний момент часу t_1 об'єкт A знаходиться в задовільному стані. Нас цікавить здатність його знаходження в цьому стані ще $t_2 - t_1$ часу, тобто до моменту t_2 . Ймовірність цієї події є суттєвою характеристикою безпеки і визначає її поріг. Надійність, з якою зберігається визначений стан події A , називається порогом безпеки об'єкту A . Звідси безпека об'єкту A^0 має визначатись (вимірюватись) своїм порогом β . Як правило, для практики має сенс розгляд об'єктів з відносно невисоким індексом ризику втрати (зміни) стану об'єкта, приміром $\alpha = 0,01$. Звідси поріг безпеки має бути $\beta = 1 - 0,01 = 0,99$, і тоді будемо говорити (дефініція), що об'єкт A^0 убезпечений з порогом безпеки порядку дві дев'ятки (0,99). Такий підхід дає можливість варіювання формалізованого визначення поняття безпеки з різним рівнем інформативного наповнення.

Визначення 1. Безпекою порогу β об'єкта A^0 називається визначений стан моделі його перебування – випробування події A з можливими наслідками втрати даної визначеності з індексом ризику α або її збереження надійністю $\beta = 1 - \alpha$.

Визначення 2. Безпекою об'єкта A^0 рівня (порогу) β визначається стахостичний стан його перебування (випробування події A) з можливим наслідком його збереження, або порушення з ймовірністю (ризиком) α або її збереження з надійністю $\beta = 1 - \alpha$.

Визначення 3. Рівень безпеки β , що визначається протилежним рівнем (індексом) ризику $\beta = 1 - \alpha$ – називається порогом безпеки.

Визначення 4. Безпекою об'єкта A називається його здатність зберігати поточний стан протягом певного проміжку часу в певних часових, просторових і технологічних умовах. За цим визначенням маємо, що безпека – це стан випадкової події, точніше процес випробування.

Визначення 5. Порогом безпеки об'єкту A називається ймовірність цієї події. Для деякого класу систем (об'єктів) на практиці може бути встановлене директивне значення порогу безпеки $\beta = \beta^*$, після якого система (об'єкт) з $\beta \geq \beta^*$ визначається (вважається) убезпеченою. Ця величина β^* впливає із класу відповідальності ПФС-об'єкту і не може бути встановлена теоретично абсолютним значенням.

Коли говорять про безпечну систему, то мають на увазі збереження нею наявного стану в наявних умовах і протягом певного часу. Оскільки сам стохастичний стан перебування залежить від різних обставин, то ризик втрати такого стану (навмисно зумовлений чи ні) є ризиком порушення безпеки системи. Індекс (рівень) цього ризику і визначає рівень небезпеки системи.

Невизначеність - ризик - безодня. Незнання, а точніше безодня незнання визначає невизначеність. Подолання невизначеності – це оволодіння окремими частинами безодні. Невизначеність є генератором ризику. Як же сприймається на відчуття ризик? Відомо, що випадкові події, а ще краще, випадкові величини сприймаються (характеризуються) ймовірносним розподілом, характеристиками-функціоналами (очікуване значення, варіація).

Для аналітичного сприйняття ризику вводимо показники (ідентифікатори ризику) і характеристики ризику. Що до ідентифікації ризику як явища та поняття, можна навести такі: індекс ризику, а також ризик-невизначеність або точніше ризик-неоднозначність. Ці показники ризику ідентифікують його (являють собою кожен окремо) нормовано-імовірнісно (рівень імовірності) та кількісно-інформативно (величина ентропії невизначеності-неоднозначності). Ризик ідентифікується через його показники та через характеристики, в основному, через числові, оскільки ми говоримо про математичний аналіз ризику, вірніше про його теорію як точну науку.

Щодо функції ризику, то можуть бути різні підходи її розуміння. Оперуючи в рамках (межах) теорії точної (імовірнісної) науки, ідентифікатори (показники) ризику і його характеристики (в основному, числові для їх математичного аналізу, оскільки бажаємо залишатися в межах цієї теорії) функції ризику мають поєднувати (стохастично зв'язувати, оскільки мова про детерміновано непередбачувані явища – сутності) величини (характеристики-показники) як два фактори одного й того ж явища (сутності) ризику (ризик-фактора). Нехай $\omega \in B$, де B – ризик-подія, і числова функція $\xi = \xi(\omega)$ побудована таким чином, що нерівність $\{\xi < x\}$ є подією для будь-якого дійсного x ; тоді раціонально будувати ризик-подію саме такими подіями типу $\{\xi < x\}$. Якщо індекс ризику – ймовірність явища $\{\xi < x\}$, то в якості функції ризику розумно розглядати величину, то зміну за зміною величини дійсного числа x – як аргумента цієї функції, розглядаючи (інтерпретуючи) саме величину x числовими показниками ризику. Таким чином залежність $F(x) = P\{\xi < x\}$ можна трактувати моделлю (точніше, однією з можливих) функцій ризику, $R(x) = \{\xi < x\}$. Відразу ж нагадуємо аналогії з теорії надійності, де функція надійності, точніше, її модель, має вигляд $N(x) = \{\xi \geq x\}$. Тоді формально-аналітично маємо прозоре підтвердження, що

$$R(x) + N(x) = P\{\xi < x\} = P\{(\xi < x) \cup ((\xi \geq x))\} = P\{\xi \in (-\infty, \infty)\} = P\{\Omega\} = I,$$

тобто, що ризик і надійність (живучість) – повна альтернатива категорій.

А тепер опустимось до можливої реальної ситуації (інженерно-економічної інтерпретації) сказаного. Нехай маємо B – певну економічну структуру, наприклад, деякий фонд, для якого час існування заплановано (детермінується) і становить рівно x , а ξ – реальний час (випадковий) його життя. Всі наші економічні прибуткові-збиткові операції, а також організаційно-технічні ми плануємо реалізувати в межах відведеного чи сплановано-розрахованого часу x (зауважимо, що не тільки ми розраховували-спланували величину x , то це вже є детермінована величина). Майбутнє допускає реалізацію одного з двох альтернативних наслідків: або $\{\xi < x\}$, або $\{\xi \geq x\}$. Другий наслідок говорить про надійність (живучість) існування нашої компанії, адже реальний час її життя є не менше запланованого часу x . Тому його зручно інтерпретувати як фактор надійності або живучості (ФН) компанії. І тоді для ФН $N(x) = \{\xi \geq x\}$ буде $P\{\xi \geq x\}$ її індексом надійності (живучості), тобто $I_{NX}P\{\xi \geq x\}$.

Перший наслідок $\{\xi < x\}$ є не що інше, як ризик-фактор і тоді $I_{RX}P\{\xi < x\}$. При зміні запланованого часу x буде змінюватись і I_{RX} , (наприклад, коли x збільшується, то I_{RX} також збільшується і навпаки). Будемо мати (розуміти) функцію ризику $F_R(x) = P\{\xi < x\}$ і відповідно функцію надійності (живучості) $F_N(x) = P\{\xi \geq x\}$. В межах експоненційно-геометричного (марківського, тобто без післядії) представлення моделювання нашого буття, отримані функції набувають більш ясного експоненційного вигляду $F_R(x) = 1 - e^{-hx}$, $F_N(x) = e^{-hx}$, де згідно відомих результатів теорії ймовірності, параметр законів λ^{-1} є математичним очікуванням (ймовірнісно середнім) часу ξ , тобто $\lambda = 1/M\xi$. В межах марківської теорії зручно ввести величину "стандартного" рівня індексу ризику, який відповідає ймовірності

$$I_R = P\{\xi < x / x = M\xi\} = P\{\xi < M\xi\} = 1 - e^{-1} = 1 - 1/e.$$

Доцільно розглядати послідовність "стандартних" рівнів ризику для практичного застосування в експертному наближеному оцінюванні, що відповідає значенням запланованого часу x у формі безмежної (в обидва кінці) послідовності, а саме:

$$x \in \{\dots 1/nM\xi, \dots, 1/3 M\xi, 1/2 M\xi, M\xi, 2M\xi, 3M\xi, \dots, nM\xi, \dots\}.$$

В межах прийнятих моделей легко проілюструвати алгебру ризиків на прикладі числових характеристик ризику, зокрема операцію додавання ризиків.

Захист від ризиків. Людині доводиться захищатись від ризику, уникаючи його, зменшуючи його можливу негативність наслідків, переносити його на інший об'єкт, поступившись, виплатою, диверсифікувати його, розділивши з іншими. Природний захист: від дощу можна захиститись парасолькою чи в домі та ін. Інтелектуальний захист розраховує на прогноз погоди: не йдемо без парасольки та інш. Інтелектуально-природний враховує виробництво плащів, парасольок, щоб захиститись від дощу, будівництва наметів та ін. Інтелектуально-інформаційний захист дозволяє враховувати прогноз погоди, наукові дослідження та передбачення та ін.

Деякі думки. Яку б задачу ми не розв'язували – ми розв'язуємо задачу прогнозу. Дійсно ми маємо комплекс вихідних умов x , ми володіємо вмінням розв'язувати задачі (методами і засобами), тобто маємо оператор розв'язку завдання, а потім розраховуємо, а фактично передбачаємо (прогнозуємо) результат Y , тобто будуємо з погляду формалізації співвідношення прогнозу

$$PX = Y. \quad (5)$$

Якщо ми володіємо результатом Y , а нас цікавить ресурс x , який був вчора витрачений на його здобуття, застосовуємо обернений оператор p^{-1} (якщо p^{-1} існує і про нього можна говорити) до співвідношення (5) і отримаємо

$$p^{-1}y = p^{-1}PX = IX = X, \quad (6)$$

де I – одиничний оператор. Тому співвідношення X і тим більше невизначеність завтра Y в сенсі прогнозу (5), або ж невизначеність сьогодення Y з невизначеністю вчора (ресурси, що продукували сьогодні), X – інтерполяція (6). Отож, невизначеність – це все, або майже все, що породжує проблеми та що є змістом будь-якої наукової діяльності та науки взагалі. Визначеність і невизначеність – альтернатива категорій. Вважають, що визначеним повністю є лише минуле, частково сьогодення; невизначеним є майбутнє, і ми будемо науки, щоб прогнозувати його (майбутнє), прогнозувати – розраховувати окремі його проблеми, програмувати – пророкувати окремі цікаві результати.

А тепер поміркуємо про минуле, чи так вже й достеменно воно визначено? Адже достовірність включає і безпомилковість, і достатність, і все охоплення інформації, і систему поглядів (світогляд), яким освітлюється ця інформація. Адже зрозуміло, що науковий світогляд з часом змінюється, і тому події далекого минулого фактологічно відображенні в той час пануючим світоглядом, який у поняттях (що змінюються) не завжди можливо адекватно відобразити сучасною мовою. Тому складно говорити про чітку границю, а тим більше межу між буттям визначеності і буттям невизначеності. Хоча альтернатива їх для кожної конкретної точки буття є абсолютною. Альтернатива категорій "визначеність"- "невизначеність" є абсолютною. Хоча границя між ними, а точніше межа є відносною і для кожної людини своєю (в силу рівня пізнання та поінформованості), відносною вона також є для певного часу, певного рівня культури.

Увесь світ і наше буття охоплені невизначеністю. Невизначеність потрохи завойовується визначеністю; там, де дивитись однозначно детерміновано не вдається, оглядають поглядом нову (але все ж таки завойовану у невизначеності) ланку. З цієї ланки не можна одержати достовірно інформації про її варіації, але ж зате можна приписати їм (цим варіаціям) певні імовірності. А це вже суттєвий крок до оволодіння новими продуктивними знаннями про неї, зокрема, приміром, будувати оцінки ентропії. Тож можна ще на ньому просунутись межею праворуч, долаючи невизначеність і прибавляючи визначеності.

Висновки

Щоб говорити про встановлення моделі функції ризику, необхідно дослідити її властивості, які диктуються як фізичним змістом трактування змінних і констант, так і математичною структурою, включаючи рівень її адекватності та аналітичної плідності в застосовуваних можливостях сучасного рівня розвитку математичного аналізу типів моделей, що розглядаються. Також розглянуто низку задач типу задач-визначень, задач-тверджень, задач оцінювання і аналізу. На перший погляд, вони розрізнені, з різних розділів науки, різні сюжетні лінії. Але в нас на це є інший погляд: вважаємо їх цілісно-об'єднаними, об'єднувчий стержень – формалізація, хоча не завжди вдається досягати належного рівня. Але це крок до побудови формалізації досліджуваних теорій, оскільки емпірично-вербальні структури їх дефіциту не складають.

Список літератури

1. Корнійчук, М.Т. Складні системи з випадковою зв'язаністю: ймовірне моделювання та оптимізація / М.Т. Корнійчук, І.К. Совтус. — К.: КНЕУ, 2003. — 374 с.

2. Єрмошик, В.В. Аналіз і оцінка ризиків інформаційної безпеки / В.В. Єрмошик, Я.В. Невоїт — К.: ПВП “Задруга”, 2015. – 123 с.
3. Креденцер, Б.П. Оцінка надійності резервованих систем при обмеженій вихідній інформації / Б.П. Креденцер, В.В. Вишнівський, М.К. Жердев, Д.І. Могилович, Л.С. Стойкова. — К.: Фенікс, 2013. – 336 с.
4. Хенди, Е.Д. Надежность технических систем и оценка риска / Е.Д. Хенди, Х. Кумамото. — М.: Машиностроение, 1984. – 528 с.
5. Корнійчук, М.Т. Ризик і безпека: кореляція категорій / М.Т. Корнійчук, В.О. Хорошко, Д.В. Чирков // Захист інформації, 2008. – Спец. вип. – С. 15-21.

ПРОГНОЗИРОВАНИЕ НАДЕЖНОСТИ ПРОЦЕССА ФУНКЦИОНИРОВАНИЯ СЛОЖНЫХ СИСТЕМ И РИСК ИХ ОТКАЗА

В.А.Хорошко., Ю.Е. Хохлачева.

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

В данной работе рассматриваются базовые фундаментальные факторы содержания математической модели, которую хотим построить, а именно, прогнозирования надежности процесса функционирования сложных систем и риск их отказа. Причем в главном базовом виде этих показателей. Это вероятность безотказного процесса функционирования системы (надежность и живучесть) в определенных пространственных и технологических условиях в течение определенного времени и при этих же условиях - вероятность отказа (риск) систем.

Ключевые слова: надежность сложных систем, прогнозирование надежности, риск отказа сложных систем, живучесть систем.

FORECASTING THE RELIABILITY OF THE PROCESS OF FUNCTIONING OF COMPLEX SYSTEMS AND RISK OF THEIR DISCLAIMER

V.O. Khoroshko., Yu.E. Hohlachova.

National Aviation University, Cosmonaut
1, Komarova Str., Kyiv, 03058, Ukraine; e-mail: professor_va@ukr.net

In this paper we consider the basic fundamental factors of the content of the mathematical model, which we seek to construct, namely, predicting the reliability of the process of functioning of complex systems and the risk of their failure. Moreover, in the most basic form of these indicators. This is the probability of a fail-safe process of functioning of the system (reliability and survivability) in certain spatial and technological conditions over a period of time and under the same conditions - the probability of failure (risk) of systems.

Keywords: reliability of complex systems, prediction of reliability, risk of failure of complex systems, system survivability.

ДИНАМІЧНІ ВЛАСТИВОСТІ ПРОЦЕСІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ НА ПРИКЛАДІ АУДИТУ КІБЕРБЕЗПЕКИ

О.Ю. Козлова¹, В.Г. Кононович¹, І.В. Кононович², М.Г. Романюков¹,
Л.М. Тимошенко¹

¹ Одеський національний політехнічний університет,
просп. Шевченко, 1, Одеса, 65044, Україна; e-mail: vl_kononovich@ukr.net

² Одеська національна академія харчових технологій
вул. Канатна, 112, м. Одеса, 65039, Україна; e-mail: kononovich@mail.ru

У роботі розглянуто процес розвитку від інформаційної безпеки до кібернетичної безпеки об'єктів інфраструктури, і зокрема процесів аудиту кіберзахищеності. Встановлено, що аспекти динаміки процесів інформаційної та кібербезпеки досліджені недостатньо, і не розкривають повний формальний та системний підхід до вирішення задач кібербезпеки. У зв'язку з цим, розроблена логіко-лінгвістична модель ризико-орієнтованого підходу до планування заходів кібербезпеки та найпростіша математична модель двох етапного циклічного управління процесами аудиту. Використання математичної моделі буде сприяти більш точному розумінню динамічних властивостей та розробці необхідних системних і позасистемних заходів забезпечення кібербезпеки.

Ключові слова: кібернетична безпека, модель динамічної системи, циклічне управління аудитом.

Вступ

Інформаційний та кібернетичний простори відіграють важливу роль в економічному та соціальному розвитку кожної країни світу. В Україні існує ціла низка проблем вразливості інформаційної сфери відносно стороннього кібернетичного впливу. Протистояти фізичному руйнуванню технічних засобів, порушенню функціонування об'єктів нападу та протиправній діяльності соціальних інженерів з дня на день стає все важче через недостатнє кадрове забезпечення відповідними фахівцями у сфері інформаційної та кібербезпеки. Необхідним є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави [1].

Небезпека кіберзлочинності була усвідомлена ще в часи приєднання України до міжнародної «Конвенції про кіберзлочинність». А термін «кібербезпека кіберпростору» з'явився у лексиконі українських спеціалістів зовсім недавно. І, перш за все, спалахнула термінологічна суперечка. Визначення понять «інформаційна безпека» та «кібербезпека» дуже схожі у багатьох авторів [1–3] і формально відрізняються додаванням понять «кіберпростір», як об'єкту захисту, «кіберзагроз» тощо. Кібербезпека розглядається як безпека специфічного виду інформації – управлінської інформації [2]. Приставка «кібер-» виділяє «клас кіберсистем, які використовуються для вирішення задач управлінського характеру». «В кіберсистемах на перше місце виділяється вимоги неперервності й стійкості управління. А ці вимоги можуть бути виконані лише при умові забезпечення доступності, цілісності та конфіденційності вхідної інформації [3]». Для остаточного розуміння цих термінів ще потрібні додаткові дослідження.

Міжнародна спільнота накопичила немало кількість стандартів та передових практик захисту найважливіших об'єктів інфраструктури [4]. Важливе місце в системі як інформаційної безпеки, так і кібербезпеки займає аудит [5, 6]. Основним призначенням *аудиту* інформаційної безпеки об'єкта інформаційної діяльності є формування, як правило, незалежної оцінки інформаційної безпеки.

За метою проведення аудит поділяється на аудит для підтвердження відповідності вимогам національної системи нормативно-правових документів інформаційної безпеки та на аудит підтвердження відповідності міжнародним стандартам ISO/IEC 15408 [7]».

Як і в багатьох сферах при системному підході системи інформаційної безпеки розглядаються як динамічні системи, які складаються із множини механізмів і функцій, які теоретично пов'язують із феноменом самоорганізації. Ряд спеціалістів застосовують методи нелінійної динаміки для вивчення властивостей процесів захисту інформації [8,9]. Процеси аудиту, зокрема внутрішнього, є принципово циклічним і нелінійними. Ці питання потребують своєї розробки.

Метою роботи є удосконалення термінології у частині понять «кібербезпеки» та розроблення найпростішої дискретної математичної моделі динаміки циклічного процесу обробки даних аудиту.

Визначення кібербезпеки та інформаційної безпеки

Закон України про основні засади забезпечення кібербезпеки України від 5 жовтня 2017 року визначає «кібербезпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечується сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенціальних загроз національній безпеці України у кіберпросторі», де «кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та або інших глобальних мереж передачі даних». «Кіберзахист – це сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем [10]». В чинному документі Закону України про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки від 9 січня 2007 року визначається «Інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [11]».

Взаємовідношення понять у сферах безпеки в кіберпросторі у контексті ISO 27032 представлені на рис. 1. Кібербезпека забезпечується у наступних сферах: безпека застосувань і операційних систем, безпека інформаційно-комунікаційних мереж, безпека роботи в Інтернет, захист інформації у ключових системах інформаційної інфраструктури і, зокрема, в об'єктах критичної інфраструктури, а також у сферах боротьби з кіберзлочинністю та забезпечення безпеки роботи у кіберпросторі. Даний рисунок справляє те уявлення, що кібербезпека є складовою частиною інформаційної безпеки. Формально це так. Кібернетичні системи, як системи управління, у своєму

сучасному вигляді, являються підмножиною інформаційних систем. Поняття кібербезпеки прийшло із військової сфери, де офіційно було застосоване в управлінні.

Але, судячи з визначень, які наведено вище, поняття «кібербезпека» більш ширше у відношенні об'єктів, яких воно стосується. На рис. 1 показані об'єкти/суб'єкти які охоплюються, відповідно, інформаційною (ІБ) та кібернетичною безпекою (КБ).

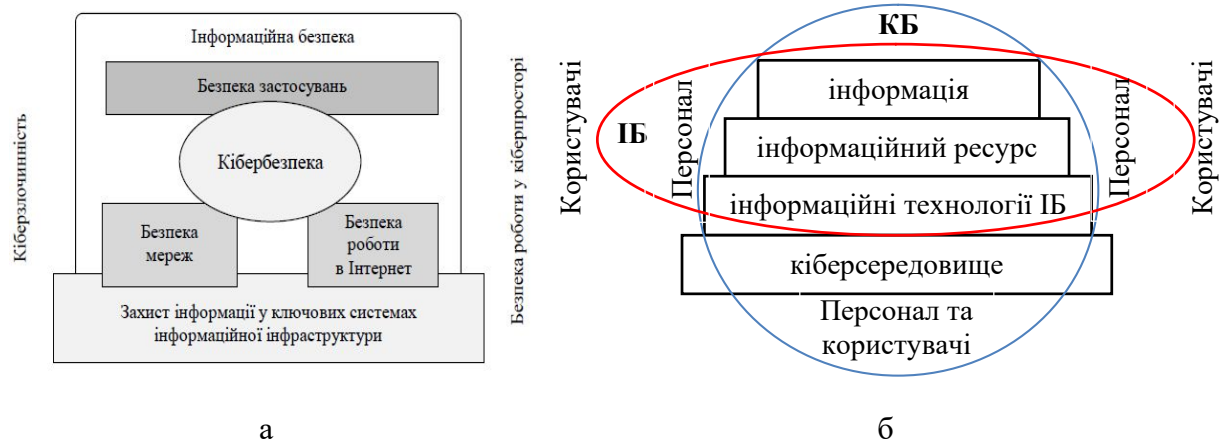


Рис. 1. Взаємовідношення понять у сферах безпеки в кіберпросторі: а – місце кібербезпеки серед інших сфер безпеки (Джерело – ISO 27032:2012); б – охоплення об'єктів інформаційної та кібербезпеки

Ретроспективно системи захисту інформації розвивалось наступними етапами:

- захист інформації системами технічного та криптографічного захисту, за допомогою криптографічних, технічних, організаційних, а тепер і програмних засобів;
- забезпечення інформаційної безпеки інформаційних ресурсів в автоматизованих системах. До інформаційних ресурсів відноситься інформація, засоби обробки інформації та (звернемо увагу) обслуговуючий персонал (НД ТЗІ 1.1-003-99);
- забезпечення інформаційної безпеки інформаційних технологій, зокрема в інформаційно-комунікаційних системах. На цьому етапі об'єктом захисту стає також відкрита інформація, важлива для особи, суспільства та держави;
- забезпечення кібернетичної безпеки кіберпростору. Кіберпростір охоплює інформацію, інформаційні технології, персонал, користувачів і все те, що виникає при комунікаціях суб'єктів і об'єктів та взаємодії їх між собою.

Сформулюємо головні відмінності інформаційної та кібербезпеки, користуючись переліком «Базові заходи кібербезпеки», які наведені у [12]:

- Об'єктом забезпечення кібербезпеки стає кіберпростір. Його важлива складова – інформаційно-комунікаційна та телекомунікаційна системи.
- Ще більше приділяється уваги готовності мереж, що важливо з точки зору відбиття DDOS-атак.
- Суб'єктом забезпечення кібербезпеки стають, крім персоналу, кінцеві користувачі. Для безпеки кінцевих користувачів передбачаються низка заходів, включаючи застосування персональних між мережевих екранів та систем виявлення вторгнень.
- Методи соціальної інженерії є не лише засобом нападу, а й захистом від атак.
- Актуалізуються як обов'язкові процеси менеджменту, моніторингу і аудиту, динаміка яких є предметом даного дослідження.

Управління процесами аудиту інформаційної безпеки

Управлінський цикл – це сукупність послідовно здійснюваних управлінських

операцій, у ході яких суб'єкт управління досягає бажаних результатів. У кожному циклі спостерігається певна послідовність управлінських дій. Додержання певного порядку їх виконання має важливе значення для забезпечення високої якості управління.

Прогнозування – це метод, в якому використовується як накопичений в минулому досвід, так і поточні припущення стосовно майбутнього з ціллю його визначення. Якщо прогнозування виконано якісно, результатом стане картина майбутнього, яку можна використовувати як основу для планування.

Циклічність і прогнозування за допомогою попередніх циклів майбутніх станів складають суть сучасного підходу до процесно-орієнтованого управління, тобто ідентифікації процесів та управління ними

Для зниження відхилень в управлінні можна застосувати концепцію PDCA (рис. 2). Основними елементами циклу являються:

Р – визначення цілей та прийняття рішення щодо необхідних змін, тобто розробка плану;

D – здійснення змін або втілення плану;

С – контроль виконання плану;

А – проведення необхідних дій, якщо результати не відповідають запланованим, або стандартизація в іншому випадку.



Рис. 2. Цикл постійного поліпшення системи менеджменту якості

При управлінні інформаційною безпекою використовують процеси оцінки ризиків інформаційної безпеки, організації і експлуатації захисних заходів, навчання персоналу інформаційній безпеці та інші. Серед них визначальними є процеси контролю та перевірки інформаційної безпеки. Аудит займає особливе місце в системі забезпечення інформаційної безпеки об'єкта інформаційної діяльності, який формує незалежну оцінку інформаційної безпеки. Своєчасність, точність і повнота оцінок інформаційної безпеки, отриманих у результаті аудиту, дають змогу виявити вразливості системи, скоригувати їх, щоб удосконалити процеси забезпечення інформаційної безпеки.

Результативність, надійність та об'єктивність висновків за результатами аудиту забезпечуються чітким дотриманням принципів проведення аудиту, таких як: відповідальність, обачність, неупередженість, непідкупність та уміння зберігати таємницю та інших.

Використання ризико-орієнтованого підходу до планування заходів аудиту є одним з можливих варіантів збільшення ефективності аудиту (рис. 3).

Аудит може бути зовнішнім та внутрішнім за методами проведення.

Зовнішній аудит – разовий захід та проводиться за ініціативою керівництва сторонньою організацією відповідної кваліфікації. Висновки за результатами цього

аудиту використовуються для покращення якості процесів організації. Проводити його слід регулярно.

Для самооцінки стану інформаційної безпеки силами самої організації проводиться внутрішній аудит, тобто проводиться пошук слабких місць, покращення якості процесів організації, оцінка ступеня відповідності системи забезпечення безпеки вимогам діючих нормативно-правових документів. Ця діяльність є безперервною і затверджується керівництвом організації.

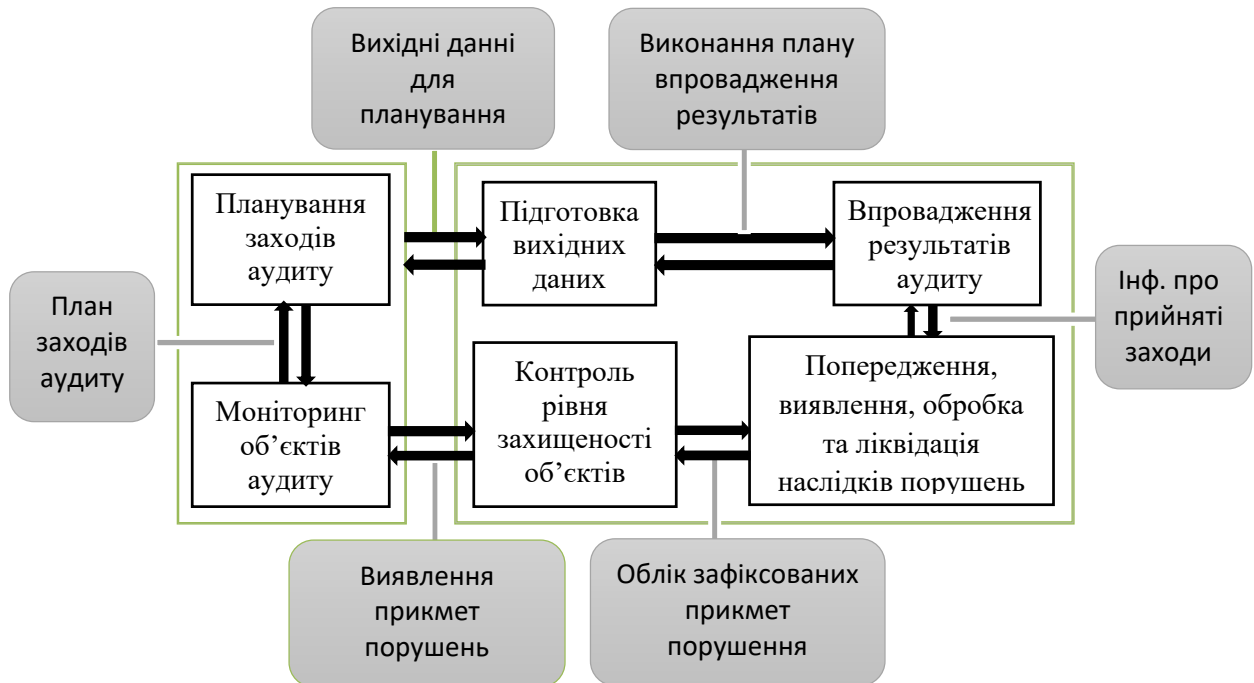


Рис. 3. Схема реалізації ризико-орієнтованого підходу до планування заходів аудиту

Аудит починається з процедури ініціації. На цьому етапі повинні бути визначені межі проведення обстеження, до яких відносяться переліки: фізичних осіб, ресурсів, приміщення, основні види загроз, організаційні, фізичні та програмно-технічні аспекти забезпечення інформаційної безпеки.

Найскладніший та найтриваліший етап збирання інформації аудиту, тому що саме на цьому етапі проводиться вивчення документації та тісна взаємодія аудитора з посадовими особами організації.

Далі аудитор повинні виконати аналіз даних, при цьому можна використовувати один із трьох методів.

Перший підхід, який базується на аналізі ризиків – найскладніший, трудомісткий та вимагає найвищої кваліфікації аудитора, тому що необхідно визначити індивідуальний набір вимог інформаційної безпеки, що враховує особливості середовища її функціонування та існуючі загрози інформаційної безпеки.

Другий підхід – практичний та опирається на використання стандартів інформаційної безпеки, які визначають базовий набір вимог інформаційної безпеки. Стандарти можуть визначити різні набори вимог залежно від рівня захищеності, приналежності та призначення.

Третій підхід припускає комбінування перших двох. Він є найефективніший. Базовий набір вимог інформаційної безпеки визначається стандартом, додаткові вимоги формуються а основі аналізу ризиків.

Четвертий підхід складний і найбільш відповідальний. Аналіз ризиків – це те, з чого повинна починатися побудова будь-якої інформаційної безпеки. Він полягає у виявленні існуючих ризиків та їх оцінки якісної або кількісної.

Далі проводиться оцінка відповідності вимогам стандартів. Виявляться вимоги інформаційної безпеки, які не реалізовані в системі. Виходячи з цього, робляться висновки про відповідність.

Вироблення рекомендацій за наслідками аналізу, які повинні бути конкретними, економічно обґрунтованими, аргументованими (підкріпленими результатами аналізу) і відсортованими за ступенем важливості.

Підготовка звітних документів, які повинні містити опис цілей проведення аудиту, характеристику обстеження, вказівку границь проведення аудиту та методів. Звіт є основним результатом проведення аудиту, якість якого характеризує якісь роботи аудитора.

Математична модель циклічного управління процесами аудиту

Подібна задача вирішувалась авторами, стосовно циклічного управління кібербезпекою в [8] і стосовно управління колективною та індивідуальною свідомістю громадян у [9]. «Ефективність людської дії здебільшого залежить від правильного управлінського рішення, що, у свою чергу, залежить від інформаційного моделювання ситуації, від пошуку потрібної інформації та її переробки. Лавиноподібне зростання інформаційних потоків, у яких змішувались потрібна і непотрібна інформація («інформаційні шуми»), у значній мірі утруднив поведінку людини та висунув на передній план вибірковий пошук потрібної інформації з наступною її редукцією для прийняття тих чи інших рішень [13]».

Розглянемо найпростішу модель циклового інформаційного процесу управління, який складається з двох етапів:

- аналізу інформаційного потоку даних аудиту (відбір потрібної інформації, редукція, консолідація, переробка) – x_{in} ;
- прийняття рішень та обробки вихідного інформаційного потоку для корекції заходів захисту (формування та видача управлінського рішення) – x_{out} .

Математична модель динамічної системи $\Phi(x, y)$ буде мати такий вигляд:

$$\Phi(x, y) = \begin{cases} x_{n+1} = x_n - k_{xy} p x_n^2 + k_{yx} q y_n^2 + x_{in} \\ y_{n+1} = y_n + k_{xy} p x_n^2 - (k_{yx} + k_{out}) q y_n^2 \end{cases} \quad (1)$$

де x, y – динамічні змінні, які визначають інтенсивність інформаційних елементів потоку на етапах обробки інформації; k_{ij} – перехідні коефіцієнти, що характеризують динамічну взаємодію етапів обробки інформації; p, q – розподільчі коефіцієнти, x_{in} – інтенсивність інформаційних елементів потоку, що поступають на перший етап обробки; причому, $\{k_{ij}\}$ і $\{p, q\} \in (0,1)$, $\{x, y\} \in R$, $x_{in} = const \in R^+$.

Наявність у системі двох груп коефіцієнтів (k_{ij} та p, q) має конкретну фізичну інтерпретацію: коефіцієнти k_{ij} описують відносну величину редукції і консолідації інформації за синтаксичними ознаками, наприклад, форматами відомостей і повідомлень, та задають долю інформаційного потоку, який переходить з одного етапу на сусідній. Частина інформаційного потоку переходить на попередній етап обробки для виправлення неточностей, врахування зауважень тощо. Коефіцієнти p, q описують розподіл елементів інформаційного потоку за їх видами по семантичним ознакам, наприклад, по змісту. Перехід між етапами обробки визначається добутком коефіцієнтів обох груп.

Висновки

Уточнення понять, пов'язаних з поняттям «кібербезпека» здійснено відносно розширення об'єктів забезпечення кібербезпеки у порівнянні з інформаційною безпекою, та визначення нових суб'єктів та механізмів кібербезпеки. Розроблена найпростіша дискретна математична модель динаміки циклічного процесу обробки даних аудиту, яка описує два етапи: етап аналізу інформаційного потоку даних аудиту (відбір потрібної інформації, редукція, консолідація, переробка); та етап прийняття рішень й обробки вихідного інформаційного потоку для корекції заходів захисту (формування та видача управлінського рішення). Напрямом подальшої роботи буде детальний аналіз моделі динаміки процесів аудиту кібербезпеки.

Список літератури

1. Бурячок, В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В. Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015. – 288 с.
2. Соколов, М.С. Кибернетическая безопасность – понятие, значение и эволюция от военных основ к самостоятельному виду безопасности // Военное право, 2012. – № 1. – 24 с.
3. Архипов, А. Приставка кибер-: все ли очевидно? / Александр Архипов // Захист інформації, 2016. – Том 18, №3. – С. 203-209.
4. Руководство по передовой практике защиты важнейших объектов неядерной энергетической инфраструктуры от террористических актов в связи с угрозами, исходящими от киберпространства / Антитеррористическое подразделение Департамента по противодействию транснациональным угрозам Секретариата ОБСЕ. – ОБСЕ: Vienna, Austria, 2013. – 96 с.
5. Курило, А.П. Аудит информационной безопасности / Курило А.П., Зефилов С.Л., Голованов В.Б. / М.: Издательская группа «БДЦ-пресс», 2006. – 304 с.
6. Аудит та управління інцидентами інформаційної безпеки : навч. посіб. / Корченко О.Г., Гнатюк С.О., Казмірчук С.В.– К.: Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. 190 с. .
7. Тардаскіна, Т.М., Кононович В.Г. Менеджмент інформаційної безпеки в галузі зв'язку: навч. посібник. Затверджено Міністерством освіти та науки України як навчальний посібник для студентів вищих навчальних закладів [Лист № 1/11-7791 від 13 серпня 2010 року] / – Одеса: ОНАЗ, 2010. – 268 с.
8. Кононович, В.Г. Нелінійні моделі циклічного управління кібербезпекою / В.Г. Кононович, І.В. Кононович, А.І. Міхова // «Інформаційні управляючі системи та технології» (ІУСТ – ОДЕСА – 2015). Матеріали Міжнародної науково-практичної конференції, 22 – 24 вересня 2015., Одеса / відп. ред. В.В. Вичужанін, 2015.– С.171 – 173.
9. Кононович, В.Г. Модель системы информационной безопасности консолидированной информации при информационном противоборстве (Раздел 16) / В.Г. Кононович, И.В. Кононович // Информационные технологии и защита информации в информационно-коммуникационных системах : монография / под редакцией В.С. Пономаренко – Х. : Вид-во ТОВ «Щедра садиба плюс», 2015.– С. 220 – 233.
10. Законодавство України: Наказ від 05.10.2017 № 2163-19 [Електронний ресурс] // Про Основні засади забезпечення кібербезпеки України. Режим доступу: <http://zakon3.rada.gov.ua/laws/show/2163-19> (дата звернення: 10.10.2017).
11. Законодавство України: Наказ від 09.01.2007 № 537-16 [Електронний ресурс] // Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки. Режим доступу: <http://zakon0.rada.gov.ua/laws/show/537-16> (дата звернення: 10.10.2017).
12. Марков, А.С. Руководящие указания по кибербезопасности в контексте ISO 27032 / А.С. Марков, В.Л. Цирлов // Вопросы Кибербезопасности, 2014. – № 1(2). – С. 28-25.
13. Информационная безопасность системы организационного управления. Теоретические основы : в 2 т. / Н.А. Кузнецов, В.В. Кульба, Е.А. Микрин и др.; Ин-т проблем передачи информ. РАН. – М.: Наука, 2006. – Т.1 – 495 с.

ДИНАМИЧЕСКИЕ СВОЙСТВА ПРОЦЕССОВ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ НА ПРИМЕРЕ АУДИТА КИБЕРБЕЗОПАСНОСТИ

О.Ю. Козлова¹, В.Г. Кононович¹, І.В. Кононович², М.Г. Романюков¹, Л.М. Тимошенко¹

¹Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: vl_kononovich@ukr.net

²Одесская национальная академия пищевых технологий
ул. Канатная, 112, м. Одесса, 65039, Украина; e-mail: kononovich@mail.ru

В работе рассмотрено процесс развития от информационной безопасности до кибернетической безопасности объектов инфраструктуры, и в частности, процессов аудита кибернетической защищенности. Установлено, что аспекты динамики процессов информационной и кибербезопасности исследованы недостаточно, и не раскрывают полный формальный и системный подход к решению задач кибербезопасности. В связи с этим, разработана логико-лингвистическая модель риск-ориентированного подхода к планированию мероприятий кибербезопасности и наипростейшая математическая модель двухэтапного циклического управления процессами аудита. Использование математической модели будет способствовать более точному пониманию динамических свойств и разработке необходимых системных и внесистемных мероприятий обеспечения кибербезопасности.

Ключевые слова: кибернетическая безопасность, модель динамической системы, циклическое управление аудитом.

DYNAMIC PROPERTIES OF PROVIDING OF CYBERSECURITY ON THE EXAMPLE OF CYBERSECURITY AUDIT

O.Yu. Kozlova¹, V.G. Kononovich¹, I.V. Kononovich², M.G. Romanukov¹, L.M. Timoshenko¹

¹Odessa National Polytechnic University,
1, Shevchenko Ave, Odessa, 65044, Ukraine; e-mail: vl_kononovich@ukr.net

²Odessa National Academy of Food Technologies
112, Kanatna Str, Odessa, 65039, Ukraine; e-mail: kononovich@mail.ru

The paper considers the process of development from information security to cybernetic security of infrastructure objects, in particular, the processes of cyber security audit. It has been established that the aspects of the dynamics of information and cyber security processes have not been adequately studied, and do not disclose the full formal and systematic approach to solving cyber security problems. In this regard, developed a logical-linguistic model of a risk-oriented approach to planning cyber security activities and the simplest mathematical model of two-stage cyclical management of audit processes. The use of the mathematical model will contribute to a more accurate understanding of the dynamic properties and the development of the necessary system and non-systemic measures to ensure cybersecurity.

Keywords: cybernetic security, model of dynamic system, cybersecurity audit.

ПРИМЕНЕНИЕ КЛАСТЕРНОГО АНАЛИЗА ДАННЫХ ДЛЯ ВЫДЕЛЕНИЯ МЕРЫ СХОЖЕСТИ ФАКТОРОВ ВЛИЯНИЯ НА РАБОТОСПОСОБНОСТЬ СЛОЖНЫХ ТЕХНИЧЕСКИХ СИСТЕМ

В.В. Вычужанин, Д.С. Шибает, Н.Д. Рудниченко

Одесский национальный морской университет,
ул. Мечникова, 34, Одесса, 65029, Украина; e-mail: nickolay.rud@gmail.com

В статье приведены результаты применения кластерного анализа данных для выделения меры схожести факторов влияния на работоспособность сложных технических систем. В качестве примера системы рассмотрена судовая энергетическая установка. Предложена концептуальная модель взаимодействия модулей системы поддержки принятия решений по управлению работоспособностью сложных технических систем с модулем кластеризации. Созданы карты домена понятий и ER-модель базы данных модуля кластерного анализа данных, построены дендрограммы выделения иерархической взаимосвязанности кластеров на базе применения методов Nearest neighbor и Furthest neighbor

Ключевые слова: кластерный анализ данных, сложные технические системы, работоспособность технических систем, меры схожести факторов

Введение

В настоящее время наблюдается устойчивая тенденция усложнения состава технических систем. Заметным является стремительное развитие и совершенствование сложных технических систем (СТС) в различных сферах человеческой жизни. К наиболее распространенным причинам подобного тренда можно отнести необходимость в: агрегации новых функциональных возможностей, расширении первоначального назначения, повышении требований к надежности работы [1,2].

Во многих отраслях применения СТС разрабатываются и используются дополнительные компоненты, расширяющие возможности систем, что приводит к появлению новых типов взаимосвязей между их отдельными элементами. Это оказывает существенное влияние на объем вычислительных действий по обработке данных, выполнение которых необходимо для эффективного функционирования системы и выполнения поставленных перед ней задач [3].

Во избежание возникновения аварийных сценариев эксплуатации СТС и различных программно-аппаратных сбоев, приводящих к понижению их работоспособности, необходимо применение методов превентивного мониторинга и диагностики состояния отдельных компонентов технических систем.

Учет характера воздействия на систему внешних и внутренних факторов различной природы, оказывающих серьезное влияние на функционирование таких систем, представляется в данных условиях наиболее приоритетной задачей. Ее решение возможно посредством применения систем поддержки принятия решений (СППР), использующих модели и имплементирующих современные методы, технологии и средства искусственного интеллекта [4].

Однако, анализ ряда источников позволяет установить, что в настоящее время существуют две сопутствующие проблемы проведения однозначной оценки влияния разнородных факторов на работу СТС.

Первая из них заключается в том, что факторы не всегда могут быть явным образом выделены, полноценно формализованы и четко определены, вследствие их стохастической вероятностной природы [5].

Второй проблемой является необходимость обеспечения средств оперативной обработки больших объемов данных, которые генерируются в процессе отслеживания состояния компонентов системы [6-9]. Для этого необходимо проектирование масштабируемых распределенных хранилищ данных, организующих оптимальную реляционную структуру хранения информации и осуществляющих поддержку возможностей многомерного интеллектуального анализа данных [10].

Решение подобных задач возможно путем разработки модуля кластерного анализа данных (КАД) с целью выявления скрытых закономерностей в больших объемах данных по факторам, оказывающим влияние на работоспособность СТС [11,12]. Современные технологии кластеризация осуществляют разбиение входных данных на отдельные группы, каждая из которых имеет определенные признаки [13]. Их использование наиболее эффективно в случаях необходимости выделения определенных правил, корреляции и тенденции в больших наборах данных, что является актуальным в рамках рассматриваемой нами задачи [14,15].

Цель статьи и постановка задачи исследований

Целью данной работы является применение КАД для выделения мер схожести факторов, оказывающих влияние на степень работоспособности СТС.

Задачами настоящего исследования являются:

1. Разработка концептуальной модели взаимодействия модулей СППР управления работоспособностью СТС с модулем КАД.
2. Разработка карты домена понятий проектируемого модуля КАД.
3. Разработка ER-модели базы данных для проведения КАД.
4. Применение иерархического метода КАД для выделения взаимосвязанности кластеров.

Основная часть

Для объединения функций получения и предобработки входных данных, идентификации неисправностей в системе, оценки сценариев снижения степени работоспособности СТС и формирования управляющих решений для предотвращения возникновения аварийных ситуаций необходимым является формирование централизованной и масштабируемой СППР. В предлагаемой концепции построения такой СППР (рис.1.), наряду с блоками, реализующими приведенные выше функции, целесообразно размещение отдельного блока интеллектуального анализа данных (ИАД). Данный блок включает в свой состав следующие функциональные модули: КАД, многомерного анализа данных (OLAP) и обработки результатов в форме графической реализации с интерфейсом пользователя (EDV). Использование этих модулей позволяет обеспечить комплексный подход к формированию перечня альтернатив для лица принимающего решения по предотвращению аварийных ситуаций СТС. Во-первых, это достигается благодаря асинхронному созданию необходимых SQL-запросов в БД на выборку, вставку, обновление и удаление (SUID) данных КАД и OLAP-модулями. Во-вторых, полученные, посредством функционирования этих модулей, результаты ИАД формализуются и сохраняются в

базу знаний в виде отдельных продукционных правил и векторов кластеров. Это может быть использовано в дальнейшем для расширения возможностей СППР или создания модуля экспертной системы или искусственной нейронной сети с целью автоматизации процесса кластеризации и формирования итоговых альтернатив.

Каждый из модулей КАД, OLAP и EDV целесообразно реализовать в виде отдельного программного приложения, функционирующего в отдельном потоке для ускорения процесса обработки данных, посредством применения порождающего шаблона проектирования Factory. К факторам, оказывающим влияние на работоспособность СТС, согласно ряду источников [5,16], можно отнести следующие: структурный и функциональный ущербы, вероятность выхода компонента из строя, степень ремонтпригодности, количество проведенных ремонтов, структурный и функциональный риск отказов, длительность эксплуатации, режим эксплуатации, степень износа, температура окружающей среды и воздействие внешних сил (неблагоприятное влияние климатических, природных или техногенных сил).

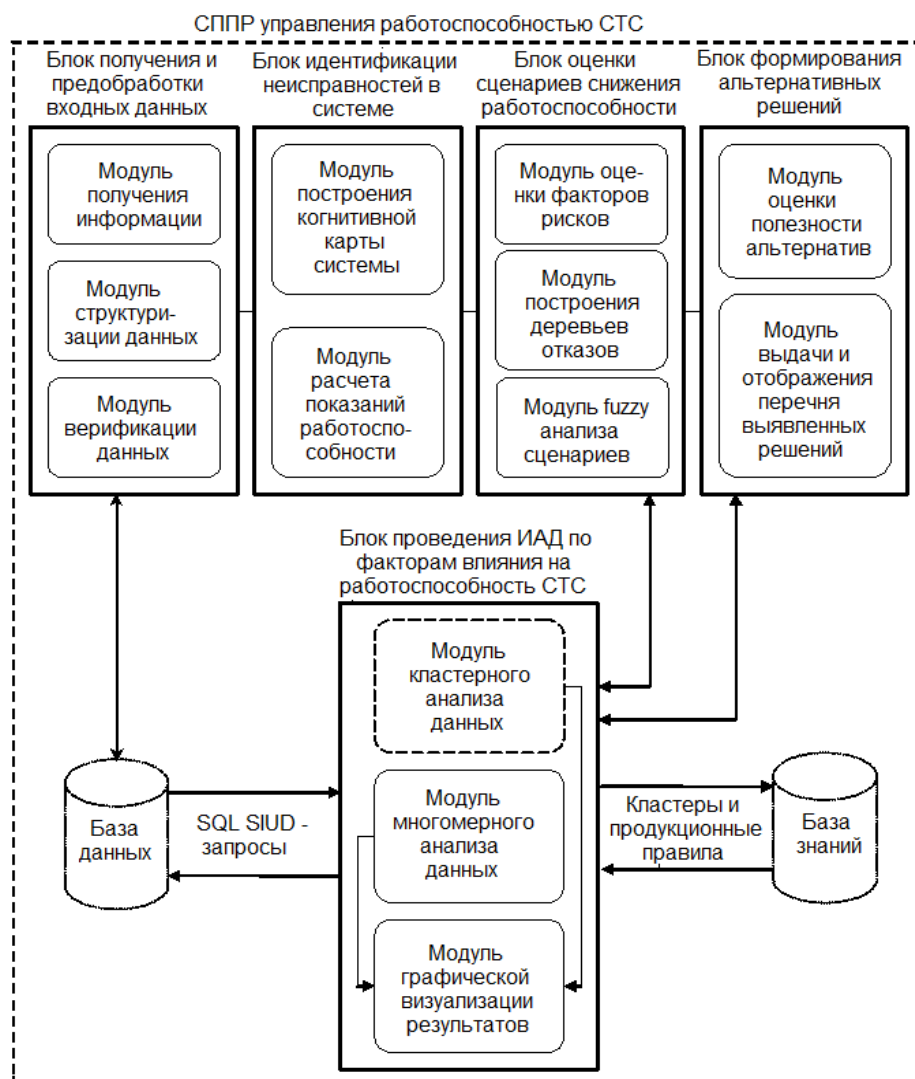


Рис. 1. Схема взаимодействия блока подсистемы КАД в рамках СППР

В качестве объекта исследования СТС в данной статье рассмотрена судовая энергетическая установка и ее статистика отказов из оффшорных и открытых источников данных (OREDA, EMSA, SRIC). Для расширяемой структуры, а также с целью обеспечения целостности и унификации процесса хранения данных разработана ER-модель БД средствами свободной СУБД MySQL WorkBench (рис.2).

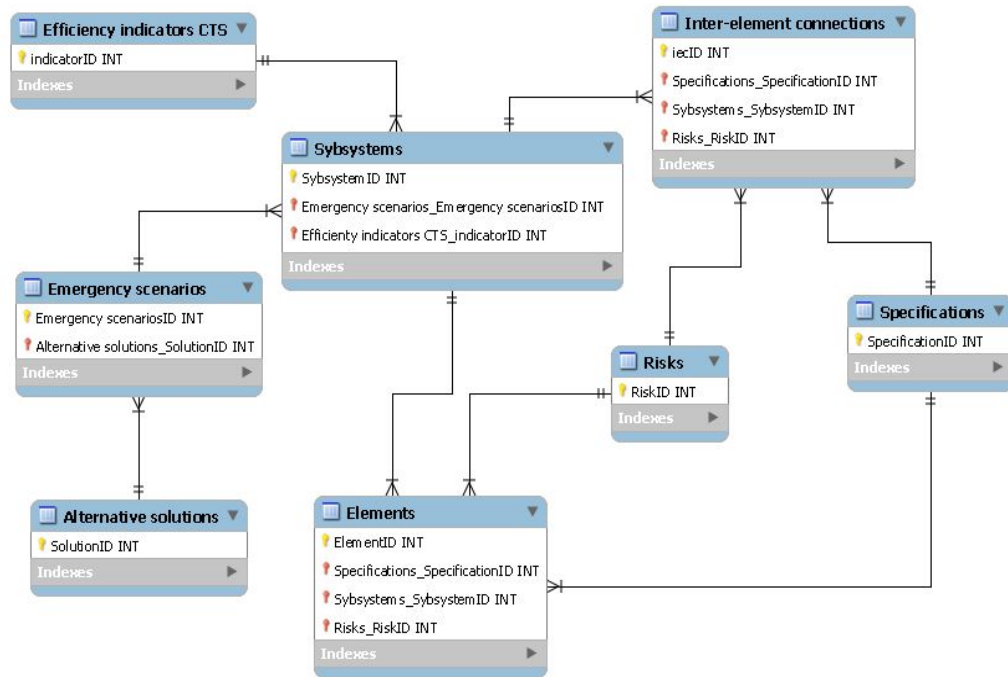


Рис. 2. ER-диаграмма связей между сущностями разработанной БД

Предусмотрено наличие связей типа «один ко многим», посредством создания внешних ключей между таблицами хранения данных, по: факторам работоспособности CTC (Efficiency Indicators CTS); элементам (Elements); межэлементным связям (Inter-element connections); подсистемам CTC (Sybsystems); техническим характеристикам компонентов (Specifications); альтернативным вариантам решений (Alternative solutions); аварийным сценариям развития (Emergency scenarios) и рискам (Risks). Для формализации процесса применения КАД для выделения мер схожести факторов, оказывающих влияние на степень работоспособности CTC, с помощью открытого облачного SaaS-сервиса mindmap.com разработана карта домена понятий, отображающая последовательность этапов кластеризации (рис.3).



Рис. 3. Карта домена понятий по этапам реализации процессов функционирования модуля КАД

Сбор входных данных из статистических БД осуществляется отдельным программным приложением (парсером), формирующим процесс переноса данных в разработанную БД. Отбор и обработка данных с последующей формализацией выполняется средствами используемой СУБД. Далее проводится нормализация, осуществляемая на базе определения среднего значения (СЗ) и стандартного отклонения (СО) по всем признакам в отдельности. Обозначим средние значения признаков как $\overline{P}_i$, а стандартные отклонения – как $S_i, i = 1, \dots, M$ (где M – количество признаков) для N - объектов по X - признакам. Таким образом, определение СЗ и СО производится по формулам (1) и (2):

$$\overline{P}_i = \frac{1}{N} \sum_{j=1}^N X_{ij}, \quad (1)$$

$$S_i = \sqrt{\frac{1}{N-1} \sum_{j=1}^N (X_{ij} - \overline{P}_i)^2}. \quad (2)$$

В качестве меры различия между анализируемыми объектами применяется евклидово расстояние. Его значение между некоторыми объектами X_j, X_k

$$D(X_j, X_k) = \sqrt{\sum_{i=1}^M (X_{ij} - X_{ik})^2}. \quad (3)$$

Для осуществления КАД использованы методы Nearest neighbor и Furthest neighbor, в которых дистанция между парой выделенных кластеров вычисляется на базе определения расстояний между наиболее близкими и наиболее далекими объектами выборки соответственно. Полученные, в результате проведения КАД дендрограммы выделения взаимосвязанности кластеров приведены на рис.4.

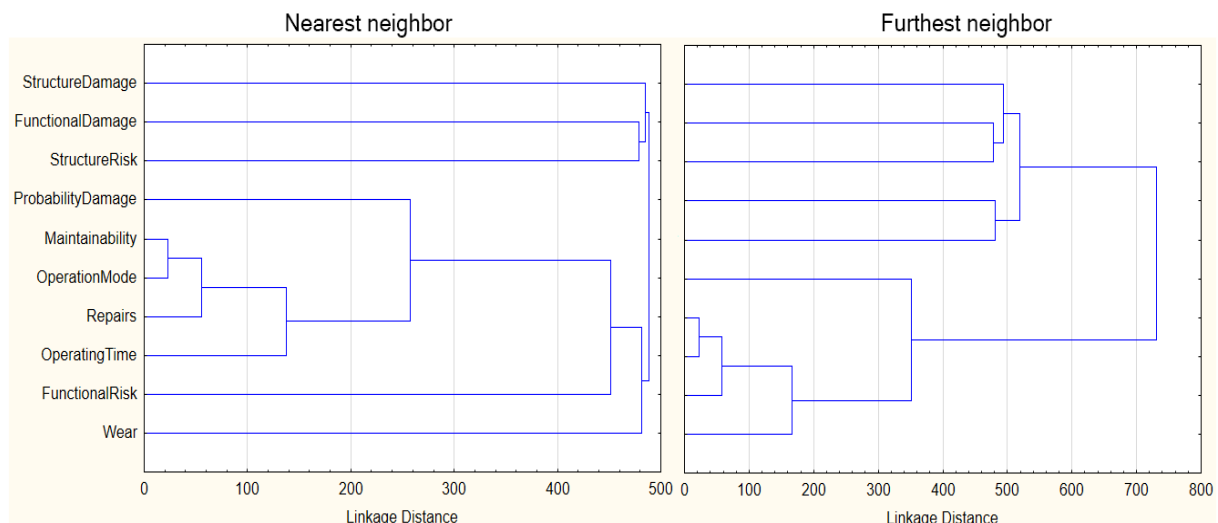


Рис. 4. Созданные дендрограммы выделения взаимосвязанности кластеров

Оценка адекватности результатов осуществлена путем определения внешних, внутренних и относительных метрик оценки качества кластеризации. Используются методы Rand statistic, Hubert statistics и Индекс Дана.

Выводы

Полученные результаты оценки адекватности позволяют утверждать, что ошибка кластеризации находится в допустимых пределах, однако лучшие значения метрик получено для метода Furthest neighbor. Анализируя процесс КАД можно отметить, что метод Nearest neighbor ориентируется на минимизацию числа больших по размеру кластеров, а метод Furthest neighbor направлен на увеличение числа компактных (меньших по размеру) кластеров.

Экспериментально установлено, что факторы функционального ущерба, структурного риска, вероятности выхода из строя, степени работоспособности и структурного ущерба обладают высокой степенью схожести и объединяются в один кластер через 4 итерации. Ко второму кластеру относятся факторы режима эксплуатации, количества ремонтов, времени эксплуатации, износа и функционального риска, которые также формируются в один кластер через 4 итерации. Дальнейшим развитием предложенной концепции КАД может быть уточнение принадлежности ряда объектов к нескольким кластерам путем использования нейро-нечеткой кластеризации.

Список литературы

1. Рудниченко, Н.Д. Информационная когнитивная модель технологической взаимозависимости сложных технических систем / Н.Д. Рудниченко, В.В. Вычужанин // Информатика и математические методы в моделировании. – 2013. – №3. – С. 240–247.
2. Вычужанин, В.В. Повышение эффективности эксплуатации судовой системы комфортного кондиционирования воздуха при переменных нагрузках. Монография/ В.В. Вычужанин, Одесса: ОНМУ, 2009.–206 с
3. Рудниченко, Н.Д. Оценка структурного и функционального рисков сложных технических систем / Н.Д. Рудниченко, В.В. Вычужанин // Восточно-европейский журнал передовых технологий. – 2014. – №1(67). – С. 18-22.
4. Rudnichenko, N. Concept implementation of decision support software for the risk management of complex technical system / N. Rudnichenko, V. Boyko, S. Kramskoy, Y. Hrechukha, N. Shibaeva // Advances in Intelligent Systems and Computing of the series Advances in Intelligent Systems and Computing. – 2016. – № 512. – P. 255-269.
5. Рудниченко, Н.Д. Разработка модели нейросети для прогнозирования риска отказов компонентов сложных технических систем / Н.Д. Рудниченко, В.В. Вычужанин // Информатика и математические методы в моделировании. – 2016. – №4. – С. 333-338.
6. Vychuzhanin, V.V. Big data mapping in the geopositioning systems for fishing industry / V.V. Vychuzhanin, D.S. Shibaev, V.D. Boyko, N.O. Shibaeva, N.D. Rudnichenko // Матеріали XII Міжнародної науково-технічної конференції CSIT 2017. – Т.1. – Львів: Вежа і Ко. – 2017. – С. 28-31.
7. Казиев, Г.З. Модели и методы кластеризации больших данных для их анализа и обработки / Г.З. Казиев, В.В. Курдюков // Сборник научных статей по итогам международной научно-практической конференции. НОУ ДПО "Санкт-Петербургский институт проектного менеджмента. – 2016. – С. 197-199.
8. Ахметханов, Р.С. Метод кластеризации диагностических данных при вибродиагностике технических систем / Р.С. Ахметханов, Е.Ф. Дубинин, В.И. Куксова // Вестник научно-технического развития. – 2017. – № 5(117). – С.3-16.
9. Вычужанин, В.В. Гибридные экспертные системы для противоаварийного управления сложными техническими системами/ В.В. Вычужанин, С.Н. Коновалов// Вісник Одеського національного морського університету, збірник наукових праць. – 2017. – № 2 (51). – С.165-179.
10. Vychuzhanin, V. Devising a method for the estimation and prediction of technical condition of ship complex systems / V. Vychuzhanin, N. Rudnichenko, V. Boyko, N. Shibaeva, S. Konovalov // Eastern-European Journal of Enterprise Technologies. – 2016. – №6/9 (84). – P. 4-11.
11. Григоренко, Д.В. Кластеризация систем обработки специальных данных / Д.В. Григоренко, В.Н. Ручкин // Методы и средства обработки и хранения информации. –Рязань: РГРТУ. – 2012. – С. 98 - 103.

12. Надев, А.И. Диагностика технического состояния судовых дизелей на основе интеллектуального анализа данных / А.И. Надеев, Б.Х. Нгок, Ф.В. Свирипов // Вестник АГТУ. – Сер.: Морская техника и технология. – 2011. – № 2. – С.105-110.
13. Егоров, А.В. Особенности методов кластеризации данных / А.В. Егоров, Н.И. Куприянова // Известия ЮФУ. Технические науки. – 2011. – №11. – С.174-178.
14. Сулов, С.А. Кластерный анализ: сущность, преимущества и недостатки / С.А. Сулов // Вестник НГИЭИ. – 2010. – №1. – С.51-57.
15. Kohonen, M.M. Self Organizing Map with Modified K-means clustering For High Dimensional Data Set / M.M. Kohonen // International Journal of Applied Information Systems (IJ AIS). Foundation of Computer Science FCS, New York, USA.– 2012. –P. 34–39.
16. Nobuo, K. Statistical Study on Reliability of Ship Equipment and Safety Management–Reliability Estimation for Failures on Main Engine System by Ship Reliability Database System / K. Nobuo // Bulletin of the JIME. – 2011. – Vol. 29. – №2. – P.64-70.

ЗАСТОСУВАННЯ КЛАСТЕРНОГО АНАЛІЗУ ДАНИХ ДЛЯ ВИДІЛЕННЯ МІРИ СХОЖОСТІ ФАКТОРІВ ВПЛИВУ НА ПРАЦЕЗДАТНІСТЬ СКЛАДНИХ ТЕХНІЧНИХ СИСТЕМ

В.В. Вичужанін, Д.С. Шибасєв, М.Д. Рудніченко

Одеський національний морський університет,
вул. Мечнікова, 34, Одеса, 65029, Україна; e-mail: nickolay.rud@gmail.com

У статті наведені результати застосування кластерного аналізу даних для виділення заходів схожості факторів впливу на працездатність складних технічних систем. Як приклад системи розглянута суднова енергетична установка. Запропоновано концептуальну модель взаємодії модулів системи підтримки прийняття рішень з управлінням працездатністю складних технічних систем з модулем кластеризації. Створено карти домену понять і ER-модель бази даних модуля кластерного аналізу даних, побудовані дендрограми виділення ієрархічної взаємозв'язку кластерів на базі застосування методів Nearest neighbor і Furthest neighbor

Ключові слова: кластерний аналіз даних, складні технічні системи, працездатність технічних систем, заходи схожості факторів

Ключові слова: кластерний аналіз даних, складні технічні системи, працездатність технічних систем, заходи схожості факторів

CLUSTER DATA ANALYSIS FOR THE SIMILARITY MEASURE IDENTIFY OF THE COMPLEX TECHNICAL SYSTEMS OPERABILITY FACTORS

V.V. Vichuzhanin, D.S. Shibaev, N.D. Rudnichenko

Odessa National Maritime University
34, Mechnikova Str., Odessa, 65029, Ukraine; e-mail: nickolay.rud@gmail.com

The article presents the results of the application of cluster data analysis to identify the measure of the similarity of the factors affecting the performance of complex technical systems. As an example of the system, a ship power plant is considered. A conceptual model of the interaction of the modules of the decision support system for managing the operability of complex technical systems with a clustering module is proposed. The concept domain maps and the ER model of the database of the cluster data analysis module have been created, dendrograms have been constructed for highlighting the hierarchical interconnection of clusters based on the Nearest neighbor and Furthest neighbor methods..

Keywords: cluster analysis of data, complex technical systems, the efficiency of technical systems, measures of similarities of factors.

СИНТЕЗ И МОДЕЛИРОВАНИЕ ЦИФРОВОГО УПРАВЛЯЮЩЕГО УСТРОЙСТВА ДЛЯ НЕСТАЦИОНАРНОГО ОБЪЕКТА

С.А. Бобриков, Е.Д. Пичугин, Н.Н. Дикий

Одесский национальный политехнический университет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: bobrikov1932@gmail.com

Проведен синтез цифрового управляющего устройства для объекта, параметры которого – коэффициент усиления и постоянная времени – могут изменяться в широких пределах. Заданная часть системы включает в себя исполнительное устройство (звено первого порядка) с неизменяющимися параметрами и двигатель – звено второго порядка с изменяющимися параметрами. Управляющее устройство обеспечивает постоянство показателей качества системы при любых значениях переменных параметров объекта в заданном диапазоне их значений. В качестве показателей процесса приняты максимальное перерегулирование в переходной характеристике и время переходного процесса. Разработана структурная схема цифрового регулятора и метод расчета его параметров. Работа выполнена путём моделирования системы в пакете MATLAB-Simulink.

Ключевые слова: регулятор, система управления, передаточные функции, переходная характеристика, показатели качества управления, объект управления, исполнительный механизм, усилитель, обратная связь, адаптивная система

Введение

Разрабатываемое управляющее устройство предназначено для работы в системе автоматического управления объектом, в котором некоторые параметры в процессе нормальной работы системы могут изменяться в широких пределах. Примерами подобных объектов могут служить: управляемая ракета, морское судно с грузом и без груза и др. В системах управления нестационарными объектами обычно используются методы адаптивного управления, что приводит к существенному усложнению как самой системы, так и методов её расчета и проектирования [1-6]. В работе [7] приведен метод расчёта регулятора, отличающийся сравнительной простотой и обеспечивающий работу системы управления с заданными показателями качества при изменении основных параметров объекта в широких пределах. Описанный в [7] регулятор представлен в аналоговой форме. В данной работе проведено исследование путём моделирования системы, разработанной в [7], при условии выполнения управляющего устройства в цифровой форме.

Цель работы

Целью работы является синтез и моделирование системы управления нестационарным объектом с цифровым регулятором. За основу построения системы принята схема, представленная в работе [7]. Результатом данной работы является дискретная передаточная функция регулятора и рекуррентное уравнение, позволяющее запрограммировать цифровое управляющее устройство.

Основная часть

Обобщенная структурная схема разрабатываемой системы показана на рис.1, где приняты следующие обозначения: $K_{yy}(p)$ – передаточная функция управляющего устройства, $K_{ум}(p)$ – передаточная функция усилителя мощности (исполнительного устройства), $K_{оу}(p)$ – передаточная функция объекта управления. Полагаем, что заданная часть системы (исполнительное устройство и объект управления) описываются следующими передаточными функциями:

$$K_{ум}(p) = \frac{K_1}{T_1 p + 1}, \quad K_{оу}(p) = \frac{K_2}{(T_2 p + 1)p}.$$

Принимаем условие, что параметры усилителя мощности K_1 и T_1 заданы и в процессе работы системы не меняются, а параметры объекта K_2 и T_2 могут изменяться в заданных пределах:

$$K_{2\min} \leq K_2 \leq K_{2\max}; \quad T_{2\min} \leq T_2 \leq T_{2\max}.$$

Разрабатываемое управляющее устройство должно обеспечить работу системы с заданными показателями качества при любых возможных значениях параметров объекта. В качестве показателей принимаем максимальное перерегулирование в переходной характеристике при условии, что время переходного процесса не превысит заданного значения.

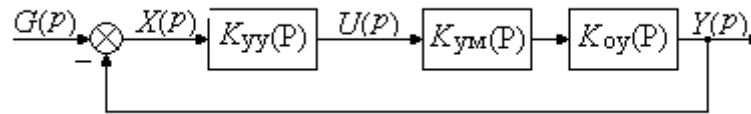


Рис. 1. Обобщенная структурная схема системы управления

Как показано в [7] управляющее устройство непрерывного действия (аналоговое) в такой системе может быть выполнено по следующей схеме, представленной на (рис.2).

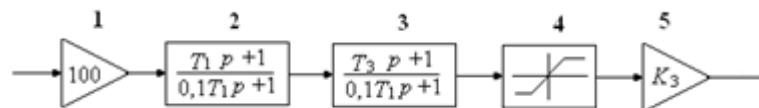


Рис. 2. Структурная схема аналогового управляющего устройства: 1,5 – усилители; 2,3 – линейные дифференцирующие звенья; 4 – нелинейность типа «насыщение»

В структурной схеме регулятора (рис.2) принимаем, что постоянная времени T_1 равна постоянной времени усилителя мощности в заданной части системы. Полагаем, что этот параметр в процессе работы системы не меняется. Постоянная времени T_3 определяется по заданным параметрам объекта управления (см. далее). В нелинейном звене 4 (насыщение) линейная часть имеет коэффициент 1, а насыщение наступает при входной величине, равной ± 2 . Структурная схема системы с аналоговым регулятором приведена на рис.3.

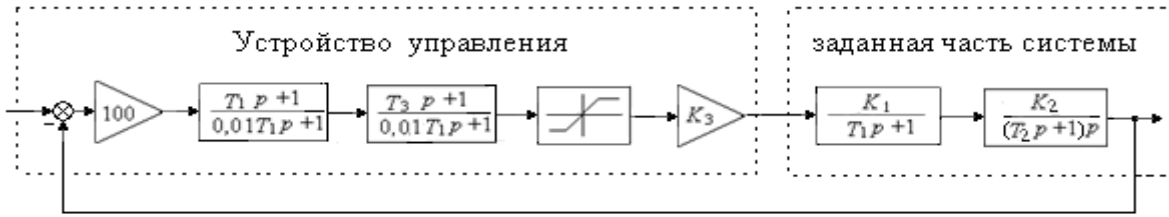


Рис. 3. Структурная схема системы с аналоговым регулятором

Передаточная функция разомкнутой системы управления без учета нелинейного звена равна (рис.3):

$$K_{\text{раз}}(p) = \frac{100(T_1p+1)(T_3p+1)K_3K_1K_2}{(0,01T_1p+1)^2(T_1p+1)(T_2p+1)p} = \frac{(T_3p+1)K_c}{(0,01T_1p+1)^2(T_2p+1)p}, \quad (1)$$

где $K_c = 100K_1K_2K_3$.

Данная система является существенно нелинейной. Устойчивые автоколебания в такой системе возникают, если линейная часть (с учетом коэффициента в линейной части характеристики нелинейного звена) неустойчива. Условие устойчивости линейной части системы (а, значит, и условие отсутствия автоколебаний в нелинейной системе) определим, используя алгебраический критерий устойчивости линейных систем (критерий Гурвица). Для этого определим передаточную функцию замкнутой системы (без учёта насыщения), а затем характеристическое уравнение замкнутой системы.

Передаточная функция замкнутой системы равна:

$$K_{\text{зам}}(p) = \frac{K_{\text{раз}}(p)}{1 + K_{\text{раз}}(p)} = \frac{(T_3p+1)K_c}{(0,01T_1p+1)^2(T_2p+1)p + (T_3p+1)K_c}.$$

Характеристическое уравнение замкнутой системы имеет вид:

$$(0,01T_1p+1)^2(T_2p+1)p + (T_3p+1)K_c = 0.$$

Сделав соответствующие преобразования приведём характеристическое уравнение замкнутой системы к виду:

$$a_0p^4 + a_1p^3 + a_2p^2 + a_3p + a_4 = 0,$$

где $a_0 = 0,01T_1^2T_2$; $a_1 = 0,02T_1T_2 + 0,01T_1^2$; $a_2 = T_2 + 0,02T_1$; $a_3 = 1 + T_3K_c$; $a_4 = K_c$.

В соответствии с критерием Гурвица условие устойчивости определяется следующими неравенствами:

$$\Delta_3 = \begin{vmatrix} a_1 & a_3 & 0 \\ a_0 & a_2 & a_4 \\ 0 & a_1 & a_3 \end{vmatrix} > 0; \quad \Delta_2 = \begin{vmatrix} a_1 & a_3 \\ a_0 & a_2 \end{vmatrix} > 0. \quad (2)$$

Подставив значения коэффициентов характеристического уравнения в неравенства (2) и сделав ряд преобразований и упрощений, находим условие устойчивости для коэффициента усиления системы K_c :

$$K_c < \frac{20T_{2\min}}{T_1T_3} + \frac{4}{T_3} + \frac{0,2T_1}{T_2T_3} \approx \frac{20T_{2\min}}{T_1T_3} = K_{\text{кр}}. \quad (3)$$

В управляющем устройстве неизвестными параметрами являются постоянная времени T_3 и коэффициент усиления K_3 . Величины этих параметров определяются из условия, что регулятор должен обеспечить заданные динамические свойства системы при изменении параметров объекта в процессе нормальной работы системы в заданных интервалах:

$$K_{2\min} \leq K_2 \leq K_{2\max}, \quad T_{2\min} \leq T_2 \leq T_{2\max}.$$

В качестве заданных динамических свойств принимаем минимальное перерегулирование в переходной характеристике ($\sigma_{\max} \leq 5\%$), и время регулирования $t_p \leq T_{2\max}$. Время регулирования определим, как интервал времени от начала подачи на вход системы единичного ступенчатого сигнала до момента, после которого ошибка управления не превышает 1%.

Величина постоянной времени T_3 определяется по заданной величине $T_{2\min}$ [7] с использованием графиков, приведенных на рис.4. Графики рис.4 построены при условии, что $K_c=100$. При этом максимальное перерегулирование не превышает 5%, а время регулирования $t_p \leq T_{2\max}$. Экспериментально установлено, что увеличение коэффициента усиления и постоянной времени объекта в 10 раз практически не влияет на показатели качества системы.

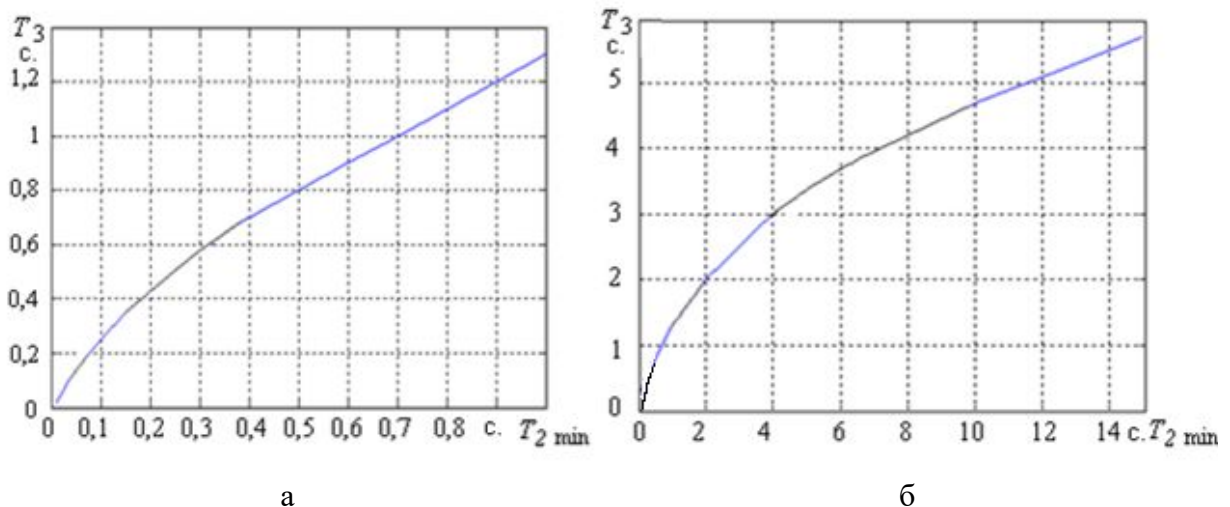


Рис. 4. Зависимость T_3 от минимального значения постоянной времени объекта управления $T_{2\min}$: а – $0 < T_{2\min} < 1$; б – $0 < T_{2\min} < 15$

Расчёт управляющего устройства проводим в следующей последовательности.

1. Расчет аналогового управляющего устройства.

Считаем заданными следующие параметры (рис.3): K_1 , T_1 , $K_{2\min}$, $K_{2\max}$, $T_{2\min}$, $T_{2\max}$. Принимаем условие: максимальное перерегулирование в переходной характеристике $\sigma_{\max} \leq 5\%$, время регулирования $t_p \leq T_{2\max}$, $T_{2\max} \leq 10T_{2\min}$, $K_{2\max} \leq 10K_{2\min}$. По кривым рис.4 для заданной величины $T_{2\min}$ находим соответствующее значение T_3 .

Принимая, что коэффициент усиления системы K_c равен (1):

$$K_c = 100K_1K_{2_{\text{вн}}K_3 = 100,$$

определяем величину коэффициента K_3 :

$$K_3 = \frac{100}{100K_1K_{2_{\text{вн}}}} = \frac{1}{K_1K_{2_{\text{вн}}}}$$

По формуле (3) проверяем критическое значение коэффициента усиления системы $K_{\text{скр}}$. Так как графики рис.4 построены для значения $K_c=100$, очевидно, что для обеспечения отсутствия в системе автоколебаний должно выполняться условие: $K_{\text{скр}} > 100$.

Непрерывная передаточная функция части управляющего устройства (без нелинейного звена и коэффициента K_3) имеет вид:

$$K_{yy}(p) = \frac{100(T_1p + 1)(T_3p + 1)}{(0,1T_1p + 1)^2} \quad (4)$$

2. Определение дискретной передаточной функции и рекуррентного уравнения цифрового управляющего устройства.

Определение дискретной передаточной функции управляющего устройства выполняем путем подстановки в непрерывную передаточную функцию (4) выражения [8]:

$$p = \frac{2(z - 1)}{T_0(z + 1)} \quad (5)$$

где T_0 – шаг квантования непрерывного сигнала по времени.

Для того, чтобы цифровая система управления максимально соответствовала исходной непрерывной системе, шаг квантования следует принять исходя из условия $T_0 \leq 0,5T_{\text{мин}}$, где $T_{\text{мин}}$ – наименьшая постоянная времени в непрерывной передаточной функции [9].

Дискретная передаточная функция вычислителя управляющего устройства имеет вид:

$$K_{yy}(z) = \frac{r_2z^2 + r_1z + r_0}{g_2z^2 + g_1z + g_0} = \frac{U(z)}{X(z)}, \quad (6)$$

где $X(z)$ и $U(z)$ соответственно z -изображения ошибки управления и сигнала на выходе вычислителя.

Представим уравнение (6) в следующем виде:

$$U(z)(g_2z^2 + g_1z + g_0) = X(z)(r_2z^2 + r_1z + r_0). \quad (7)$$

Заменяя z -изображения на оригиналы (решетчатые функции) и выделив выходную величину – $u[n]$ получим рекуррентное уравнение вычислителя:

$$u[n] = \frac{r_2}{g_2} x[n] + \frac{r_1}{g_2} x[n-1] + \frac{r_0}{g_2} x[n-2] - \frac{g_1}{g_2} u[n-1] - \frac{g_0}{g_2} u[n-2].$$

Пример.

Пусть параметры заданной части системы следующие: усилитель мощности - $K_1=0,5$; $T_1=0,01$ с; объект управления - $0,2 \leq K_2 \leq 2$; $0,5 \leq T_2 \leq 5$.

По кривым рис.4 для заданной величины $T_{2\min}=0,5$ находим : $T_3=0,8$.

1. Определяем коэффициент K_3 (1):

$$K_3 = \frac{1}{K_1 K_{2\min}} = \frac{1}{0,5 * 0,2} = 10$$

Передаточная функция аналогового регулятора (без нелинейного звена и коэффициента K_3) имеет вид:

$$K_{pez}(p) = \frac{100(T_1 p + 1)(T_3 p + 1)}{(0,1 T_1 p + 1)^2} \quad (8)$$

Определим критическое значение коэффициента усиления линейной модели системы (3) – то есть то значение, при котором в нелинейной системе возникают автоколебания:

$$K_{скр} \approx \frac{20 T_{2\min}}{T_1 T_3} = \frac{20 \times 0,5}{0,01 \times 0,8} = 1250$$

Так как при расчете управляющего устройства общий коэффициент системы принят равным 100, очевидно, в данном примере система имеет достаточно большой запас устойчивости по коэффициенту усиления, что обеспечивает отсутствие автоколебаний при любых возможных значениях параметров объекта.

2. Сделав подстановку (5) в непрерывную передаточную функцию регулятора (8), получим дискретную передаточную функцию цифрового вычислительного устройства регулятора:

$$K_{pez}(z) = \frac{r_2 z^2 + r_1 z + r_0}{g_2 z^2 + g_1 z + g_0}$$

где $r_2=3,232404$; $r_1=-6,99992$; $r_0=3,167604$; $g_2=4,84e-006$; $g_1=-7,92e-006$; $g_0=3,24e-06$; $T_0=0,001$.

Схема набора модели в системе Simulink приведена на рис.5.

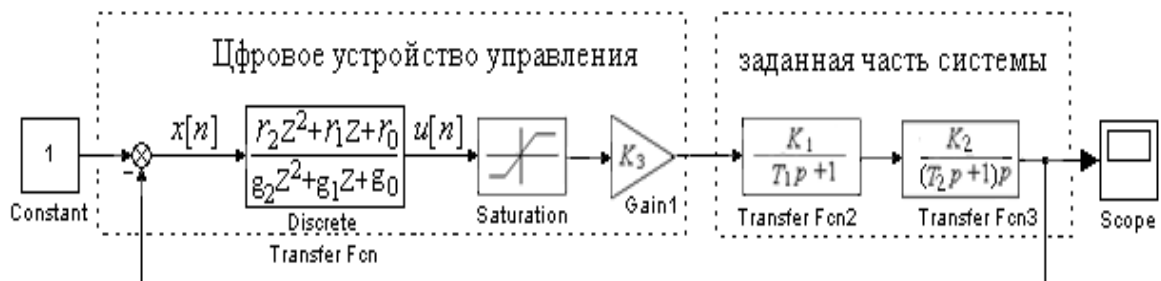


Рис. 5. Схема набора модели в системе Simulink

Результаты моделирования приведены на рис.6.

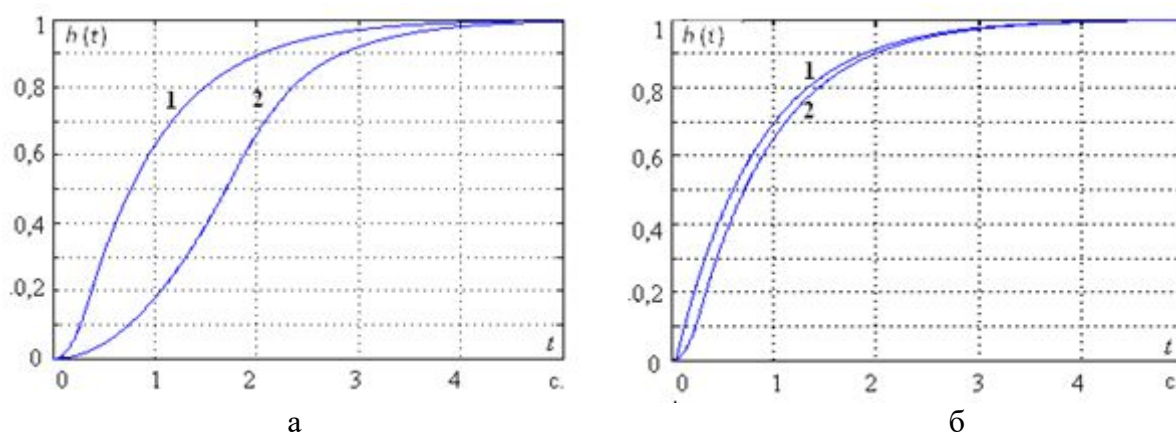


Рис. 6. Результаты моделирования системы с цифровым регулятором: а – $K_2=0,2$ ($1 - T_2=0,5$; $2 - T_2=5$); б – $K_2=2$ ($1 - T_2=0,5$; $2 - T_2=5$)

Выводы

Разработано цифровое управляющее устройство для системы, заданная часть которой содержит усилитель мощности (исполнительное устройство) с неизменяющимися параметрами и объект управления, параметры которого могут в процессе нормальной работы системы изменяться в широких пределах (1:10). Показано, как получить дискретную передаточную функцию регулятора по известной непрерывной передаточной функции. Приведен пример расчета цифрового регулятора.

Список литературы

1. Ядыкин, И.Б. Оптимальное адаптивное управление на основе беспойсковой самонастраивающейся системы с обучаемой эталонной моделью/ Автоматика и телемеханика, 1979. – № 2. – С. 65–79
2. Уткин, В.А. Задача слежения в линейных системах с параметрическими неопределенностями при неустойчивой нулевой динамике / В.А.Уткин, А. В. Уткин// Автоматика и телемеханика, 2014. – № 9. – С. 45–64
3. Рутковский, В.Ю. Стабилизация упругих колебаний конструкции крупногабаритных спутников с переменными параметрами методами адаптации / В.Ю.Рутковский, В. М. Суханов, В. М. Глумов// Автоматика и телемеханика, 2011. – № 12. – С. 91–103
4. Земляков, С.Д. Алгоритм функционирования адаптивной системы с эталонной моделью, гарантирующий заданную динамическую точность управления нестационарным динамическим объектом в условиях неопределенности/ С. Д. Земляков, В. Ю. Рутковский // Автоматика и телемеханика, 2009. – № 10. – С. 35–44.
5. Глумов, В.Ю. Адаптивное управление ориентацией деформируемых космических аппаратов с изменяющимися параметрами/ В. М. Глумов, В. Ю. Рутковский, В. М. Суханов// // Автоматика и телемеханика, 1999. – № 4. – С. 90–102
6. Кринецкий, И.И. Исследование автоматического управления курсом судна с учетом нелинейных характеристик системы / И.И.Кринецкий, Е.Д.Пичугин // Судовождение и связь. Труды ЦНИИ морского флота, 1967. – №.83.-С.13-16.
7. Бобриков, С.А. Синтез и моделирование регулятора для объекта с изменяющимися параметрами / С.А. Бобриков, Е.Д. Пичугин, С.И. Кысса // Информатика и математические методы в моделировании, 2017. – № 1-2. – С.54-61.
8. Батоврин, А. А., Цифровые следящие системы судовой автоматики / [Батоврин А. А., Дашевский П. Г., Лебедев В. Д. и др.]. – Л. : Судостроение, 1972. – 445 с.
9. Бесекерский, В.А. Теория систем автоматического регулирования / В.А.Бесекерский, Е.П.Попов. – М.: Наука, 1972. – 719с.

10. Краснопрошина, А.А. Современный анализ систем управления с применением MATLAB, Simulink, ControlSistem / А. А.Краснопрошина, Н. Б.Репникова, А. А.Ильченко. – К : Корнійчук, 1999. – 141 с

СИНТЕЗ І МОДЕЛЮВАННЯ ЦИФРОВОГО ПРИСТРОЮ УПРАВЛІННЯ ДЛЯ НЕСТАЦІОНАРНОГО ОБ'ЄКТА

С.О. Бобріков, Є.Д. Пічугін, М.М. Дикий

Одеський національний політехнічний університет,
просп.Шевченко, 1, Одеса, 65044, Україна; e-mail: bobrikov1932@gmail.com

Проведено синтез цифрового керуючого пристрою для об'єкта, параметри якого - коефіцієнт посилення і постійна часу - можуть змінюватися в широких межах. Задана частина системи включає в себе виконавчий пристрій (ланка першого порядку) з параметрами, які не змінюються, і двигун - ланка другого порядку зі змінними параметрами. Керуючий пристрій забезпечує сталість показників якості системи при будь-яких значеннях змінних параметрів об'єкта в заданому діапазоні їх значень. Показниками процесу прийняті максимальне перерегулювання в перехідній характеристиці і час перехідного процесу. Розроблено структурну схему цифрового регулятора та метод розрахунку його параметрів. Робота виконана шляхом моделювання системи в пакеті MATLAB-Simulink.

Ключові слова: регулятор, система управління, передавальні функції, моделювання, перехідна характеристика, показники якості управління, об'єкт управління, виконавчий механізм, підсилювач, зворотний зв'язок, адаптивна система

SYNTHESIS AND SIMULATION OF DIGITAL MANAGING DEVICE FOR NON-STATIONARY OBJECT

S.A. Bobrykov, E.D. Pichugin, N.N. Dikiy

Odesa National Politecnic University,
1 Shevchenko Ave., Odesa, 65044, Ukraine; e-mail: bobrikov1932@gmail.com

Synthesis of a digital control device for an object whose parameters - gain and time constant - can vary within wide limits. The predetermined portion of the system includes an actuator (first-order unit) with unchanging parameters and an engine-second-order link with varying parameters. The control device ensures the consistency of the system's quality indicators for any values of the object's variables in the specified range of their values. As indicators of the process, the maximum overshoot in the transient response and the transient time are taken. A block diagram of the digital regulator and a method for calculating its parameters have been developed. The work was done by modeling the system in the MATLAB-Simulink package.

Keywords: regulator, control system, transfer functions, simulation, transient response, control quality indicators, control object, actuator, amplifier, feedback, adaptive system

УПРАВЛЕНИЕ РИСКАМИ ПОТЕРЬ КОНТРОЛЯ НАД СЛОЖНЫМИ ТЕХНИЧЕСКИМИ СИСТЕМАМИ

В.Д. Бойко

Одесский национальный морской университет,
ул. Мечникова, 34, Одесса, 65029, Украина; e-mail: boyko-work@ukr.net

В статье предлагается расширенная когнитивно-имитационная модель сложной технической системы, предназначенная для моделирования аспекта потери контроля над системой из-за внешних неблагоприятных воздействий и поражающих факторов. Описаны элементы, расширяющие существующую модель и позволяющие эмулировать кибернетический аспект живучести. Рассматриваются возможности практического применения расширенной модели в соответствии со стандартом управления рисками ISO 31000:2009.

Ключевые слова: управление рисками, risk management, живучесть, сложные технические системы, когнитивно-имитационное моделирование.

Введение

Как было показано в [1-4] при функционировании сложных технических систем (СТС) внешние неблагоприятные воздействия и поражающие факторы (НВ и ПФ) могут выводить из строя отдельные компоненты или целые подсистемы, а также влиять на первичную и вторичную работоспособность СТС. НВ и ПФ, как правило, несут сложнопрогнозируемый либо непрогнозируемый характер (например, ошибки персонала, стихийные бедствия и т. д.), при этом их воздействие может иметь различные по степени тяжести последствия — вплоть до полного разрушения СТС [5]. Живучесть СТС в условиях НВ и ПФ зависит не только от структурной и функциональной составляющей СТС, но и от целого ряда дополнительных факторов: скорости принятия и реализации решений по борьбе за живучесть, быстроты ликвидации вторичных последствий НВ и ПФ, сохранения управляемости СТС.

Разработка систем поддержки принятия решений (СППР) для управления рисками в условиях борьбы за живучесть СТС при НВ и ПФ является одним из перспективных направлений в обеспечении безопасности функционирования СТС [6]. Такие СППР могут быть реализованы как в виде отдельных stand-alone решений, так и в виде модулей, дополняющих необходимым функционалом готовые системы управления и принятия решений общего назначения. Они позволяют не только быстро принимать решения на этапе устранения последствий НВ и ПФ, но и увеличивают устойчивость СТС благодаря возможности идентификации, анализа и оценивания существующих рисков поражения агрегатов и подсистем СТС [7].

В перечисленных выше работах живучесть рассматривалась, в основном, как показатель способности системы сохранять свою структурную и функциональную составляющие. При этом, кроме непосредственно технической исправности и работоспособности СТС при НВ и ПФ, важным фактором является сохранение управляемости СТС. Как правило, СТС представляют собой сочетание множества различных по назначению, связности и топологии агрегатов и межагрегатных связей, объединенных в подсистемы, которые взаимодействуют между собой в определенных режимах. Поэтому в целом системы управления СТС можно рассматривать как сеть или сочетание сетей, различных по характеру, компонентам, топологии и режимам

работы. Такие управляющие системы, наряду с прочими компонентами СТС, также находятся в условиях НВ и ПФ, а значит, требуется учитывать и их уязвимость.

Целью исследования является расширение концепции существующей когнитивно-имитационной модели, позволяющее моделировать сценарии потери и сохранения контроля над СТС при НВ и ПФ, а также рассмотрение возможностей практического применения полученной модели в соответствии со стандартом управления рисками ISO 31000:2009.

Кибернетическая составляющая живучести

Будем называть «кибернетическим аспектом живучести» способность СТС сохранять наблюдаемость и управляемость при выходе из строя систем, подсистем и отдельных агрегатов либо межагрегатных и межсистемных связей в условиях НВ и ПФ. Таким образом, кибернетический аспект живучести СТС можно представить в виде сочетания таких свойств СТС, как:

- *наблюдаемость* — способность системы предоставлять полную и достоверную информацию о состоянии ее агрегатов и межагрегатных связей;

- *управляемость* — способность компонентов СТС должным образом и за конечное время реагировать на команды управления.

Оба свойства зависят как от исправности рабочих компонентов СТС, так и от функционального состояния непосредственно задействованных в системе контроля и управления агрегатов СТС, которые также находятся в условиях НВ и ПФ, а следовательно, наряду с прочими системами могут выходить из строя. В этом случае как наблюдаемость, так и управляемость СТС может деградировать, вплоть до полной потери контроля над СТС.

Сенсоры и контроллеры

Когнитивно-имитационная модель СТС (КИМ СТС), описанная в [2] и используемая в качестве базовой для предлагаемой системы, представляет собой оргграф, имитирующий поведение СТС, в котором агрегатам СТС соответствуют узлы оргграфа, а межагрегатным связям (материального «энергия-вещество-информация» либо причинного характера) — ветви оргграфа.

Моделирование влияния на систему НВ и ПФ происходит путем вывода из строя отдельных узлов и связей графа в соответствии с заранее заданной или сгенерированной по определенному закону распределения случайной величины последовательностью. После чего выполняется оценка состояния КИМ СТС и сравнение с ее исходным состоянием.

Для когнитивно-имитационного моделирования наблюдаемости и управляемости СТС предлагается дополнить когнитивно-имитационную модель СТС узлами, которые либо получают информацию о состоянии агрегатов и межагрегатных связей СТС (*узел-сенсор*), либо передают сигналы управления (*узел-контроллер*), либо выполняют обе функции.

Совокупность всех данных, получаемых от сенсоров, определяет объем доступной информации о текущем состоянии СТС, а совокупность возможностей влияния на работу агрегатов СТС — степень контроля над СТС. Оценка влияния внешних НВ и ПФ на кибернетический аспект живучести СТС может быть проведена как с помощью традиционных критериев, например, критерия Калмана [8], так и с помощью методов моделирующих импульсов и критерия Бирнбаума, описанных в [2].

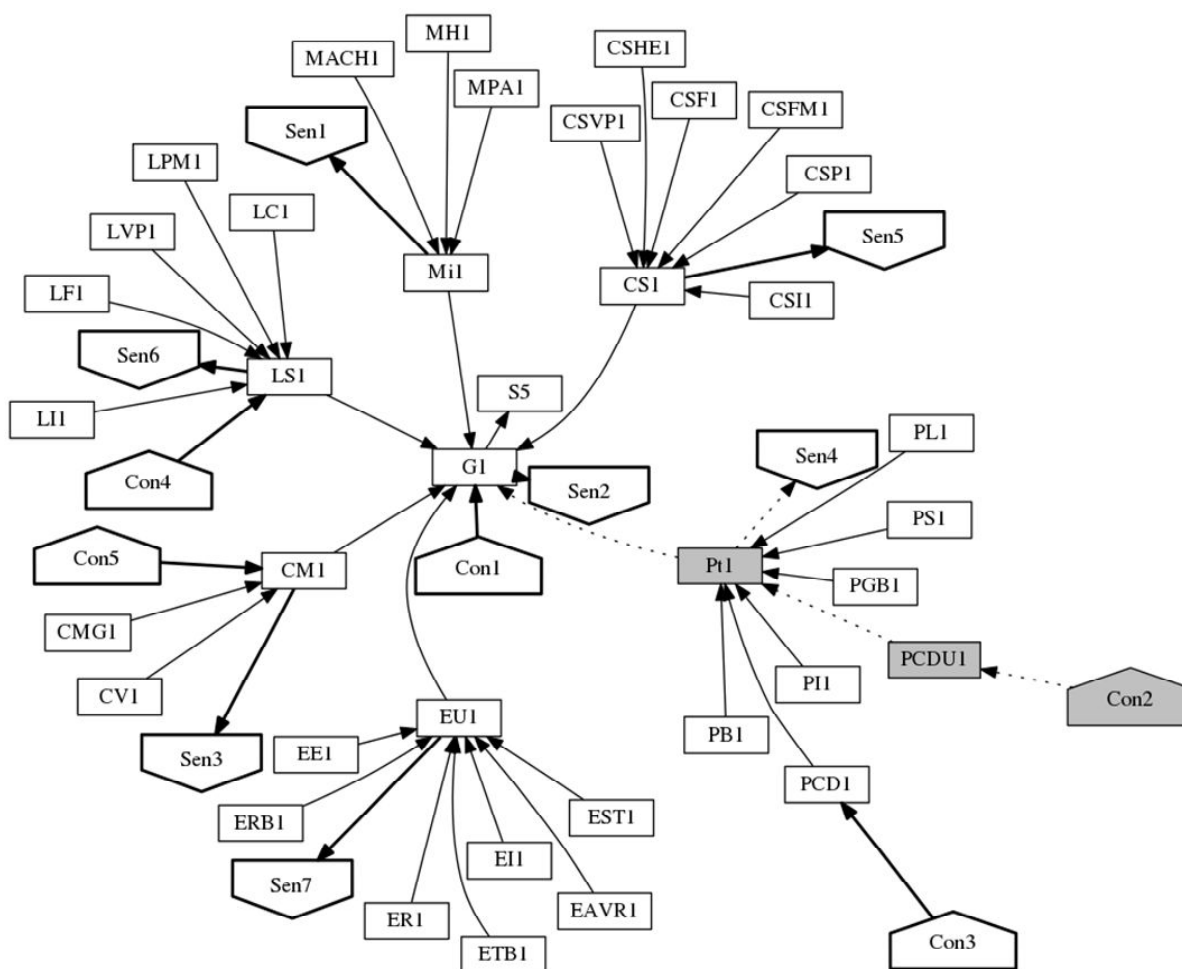


Рис. 1. Фрагмент КИМ СТС, снабженной узлами-сенсорами и узлами-контроллерами.

Рис. 1 демонстрирует граф с фрагментом КИМ системы электроснабжения судна [9]. Управляющие узлы обозначены пятиугольниками и промаркированы как *Con1*, ..., *Con5*. Узлы-сенсоры обозначены перевернутыми пятиугольниками и обозначены как *Sen1*, ..., *Sen7*. Информационные связи «агрегат-сенсор» и «контроллер-агрегат» выделены жирным начертанием. Граф, приведенный на рис. 1, иллюстрирует ситуацию, в которой ПФ вывел из строя узлы PCDU1, Pt1 и контроллер Con2 (соответствующие узлы закрашены серым цветом). При этом дополнительно вышли из строя межагрегатные связи — они выделены пунктиром.

Возможности практического использования КИМ СТС для управления рисками при борьбе за живучесть СТС

Стандарт управления рисками ISO 31000:2009 [10] определяет риск как «влияние неопределённости на цели» в противовес старому определению «вероятность или возможность потерь». Основным источником риска считается состояние неопределённости, а причиной такого состояния — недостаточность информации, понимания или знания о событии и его последствиях. Согласно стандарту, процедура управления рисками должна включать в себя следующие этапы: определение контекста, оценку риска и воздействие на риск. При борьбе за живучесть судна *определение контекста* происходит на основе информации, поступающей от систем технической диагностики, и экспертных оценок состояния СТС судна персоналом, принимающим решение [3,4]. *Воздействие на риск* осуществляется как персоналом,

ответственным непосредственно за борьбу за живучесть, так и всем персоналом судна (в случае возникновения чрезвычайной ситуации).

Оценка риска может производиться как персоналом, так и СППР, использующей КИМ СТС. Такое применение КИМ СТС возможно на стадии непосредственно борьбы за живучесть судна и на стадии проведения профилактических мероприятий по выявлению и снижению рисков — в том числе рисков кибернетической составляющей живучести СТС. *Оценка рисков* включает в себя следующие стадии: идентификацию риска, анализ риска и оценивание риска. На этапе *идентификации рисков* должен быть составлен максимально полный перечень вероятных рисков. При этом важно идентифицировать риски, связанные с решением не использовать те или иные благоприятные возможности. Риски включаются в список независимо от того, контролируется их источник или нет, даже если источник или причина могут быть неочевидными. Одним из преимуществ информационной системы на основе КИМ СТС является возможность отслеживания последствий и реакции СТС на риски с неочевидными источниками и причинами, а также проработка сценариев различной вероятности, отвечающих на вопрос «Что, если?». Этап *анализа рисков* заключается в рассмотрении причин и источников риска. При этом должны приниматься во внимание существующие средства управления, их результативность и эффективность. В ISO 31000:2009 подчёркивается, что последствия рисков могут быть выражены в виде материальных или нематериальных потерь. В некоторых случаях требуется более одного численного значения или описывающий параметр для указания вероятностей и последствий рисков для различных моментов времени, местоположения, групп или ситуаций. На этапе анализа рисков КИМ СТС позволяет определить последствия решений по управлению рисками и рассмотреть реализации различных сценариев развития событий. Этап *оценивания рисков* заключается в подготовке к принятию решений, основанных на исходных результатах анализа риска с точки зрения необходимости воздействия на риск и распределения рисков по приоритетности воздействия на них. На этой стадии КИМ СТС может быть использована как «динамическая интерактивная карта» возможных альтернативных состояний СТС, ранжированных по критериям категориальной рамки рисков — структурной, функциональной и кибернетической устойчивости. Это сокращает время и упрощает процесс принятия решений по борьбе за живучесть.

Таким образом, КИМ СТС может использоваться в процессе управления рисками на всех трех стадиях этапа оценки риска при борьбе за живучесть судна. Это позволит увеличить эффективность деятельности персонала, сократить время принятия решений и увеличить процент правильных решений по борьбе за живучесть. Кроме того, использование системы повысит наглядность и прозрачность процессов идентификации, анализа и оценки рисков живучести судна.

Выводы

Использование предложенной расширенной КИМ СТС позволяет дополнить структурный и функциональный аспекты оценки живучести, приведенные в [1] и [2], кибернетическим (управляющим) аспектом и исследовать поведение СТС при НВ и ПФ с точки зрения сохранения контроля и управляемости СТС. Определены возможности использования расширенной КИМ СТС на этапе оценки риска согласно стандарту ISO 31000:2009 и для определения систем, у которых управляемость и наблюдаемость являются избыточными либо недостаточными. В процессе моделирования были выявлены сценарии, когда при относительной исправности система теряет либо управляемость, либо наблюдаемость, либо оба свойства сразу.

Список литературы

1. Бойко, В.Д. Метод поражающего импульса для оценки влияния состояния межагрегатных связей на структурную живучесть сложных технических систем / В.Д. Бойко // Научно-практическая конференция «Інформаційні управляючі системи та технології» (ІУСТ-2013). – Одеса, 2013. – С. 234-236.
2. Бойко, В.Д. Методика оценки живучести судовых технических систем / В.Д. Бойко – Одесса: Сборник научных трудов SWorld. «Современные проблемы и пути их решения в науке, транспорте, производстве и образовании `2012», 2012. – С. 37–39.
3. Рудниченко, Н.Д.. Оценки структурного и функционального рисков сложных технических систем / Н.Д. Рудниченко, В.В. Вычужанин // Восточно-Европейский журнал передовых технологий, Інформаційні технології. Системи управління, 2014. –Том1. – №2(67) . – С. 18-22.
4. Вычужанин, В.В. Технические риски сложных комплексов функционально взаимосвязанных структурных компонентов судовых энергетических установок / В.В. Вычужанин //Вісник Одеського національного морського університету, збірник наукових праць, 2014. – Том 41. – №2. – С. 68-77
5. Siepermann, M. Risk Cost Accounting and Bottom Price Calculation–A Risk Management Information System //International Conference on the Economics of Grids, Clouds, Systems, and Services. – Springer, Cham, 2017. – С. 43-55.
6. Boyko, V. et al. Concept implementation of decision support software for the risk management of complex technical system //Advances in Intelligent Systems and Computing. – Springer International Publishing, 2017. – С. 255-269.
7. Vychuzhanin, V. et al. Devising a method for the estimation and prediction of technical condition of ship complex systems // Восточно-Европейский журнал передовых технологий, 2016. – №. 6 (9). – С. 4-11.
8. Калман Рудольф Э., Очерки по математической теории систем. / Р.Э. Калман, П.Л. Фалб, М.А. Арбиб // Пер. с англ. / под ред. Я.З.Цыпкина. Изд. 2-е, стереотипное. – М: Едториал УРСС, 2004. – С. 198-204.
9. Бойко, В.Д. и др. Модель оценки живучести технических систем / В.Д. Бойко, В.В. Вычужанин – Przemysł. Nauka i studia: VIII Międzynarodowej naukowo-praktycznej konferencji «Perspektywiczne opracowania są nauką i technikami - 2012», 2012. — С. 26–29.
10. Leitch, M. ISO 31000: 2009 – The new international standard on risk management // Risk Analysis, 2010. – Т. 30, №. 6. – С. 887-892.
11. Siepermann, M. Risk Cost Accounting and Bottom Price Calculation–A Risk Management Information System. In International Conference on the Economics of Grids, Clouds, Systems, and Services, September, Springer, Cham. 2017. – Pp.. 43-55.
12. Boyko, V., Rudnichenko, N., Kramskoy, S., Hrechukha, Y., & Shibaeva, N. Concept implementation of decision support software for the risk management of complex technical system. In Advances in Intelligent Systems and Computing, Springer International Publishing, 2017. – Pp. 255-269.
13. Vychuzhanin, V., Rudnichenko, N., Boyko, V., Shibaeva, N., & Konovalov, S. Devising a method for the estimation and prediction of technical condition of ship complex systems: Восточно-Европейский журнал передовых технологий, 2016. – Т6 (9). – С.4-11.
14. Leitch, M. (2010). ISO 31000: The new international standard on risk management. Risk Analysis, 2009. – Т30(6). – Pp. 887-892.

УПРАВЛІННЯ РИЗИКАМИ ВТРАТ КОНТРОЛЮ НАД СКЛАДНИМИ ТЕХНІЧНИМИ СИСТЕМАМИ

В.Д. Бойко

Одеський Національний Морський Університет,
вул. Мечнікова, 34, Одеса, 65029, Україна; e-mail: boyko-work@ukr.net

У статті пропонується розширена когнітивно-імітаційна модель складної технічної системи, призначена для моделювання аспекту втрати контролю над системою через зовнішніх несприятливих впливів і вражаючих факторів. Описано елементи, що розширюють існуючу модель і дозволяють емулювати кібернетичний аспект живучості. Розглядаються можливості практичного застосування розширеної моделі відповідно до стандарту управління ризиками ISO 31000: 2009.

Ключові слова: управління ризиками, risk management, живучість, складні технічні системи, когнітивно-імітаційне моделювання.

RISK MANAGEMENT FOR SCENARIOS OF LOSS CONTROL OVER COMPLEX TECHNICAL SYSTEMS

V.D. Boyko

Odessa National Maritime University
34, Mechnikova Str., Odessa, 65029, Ukraine; e-mail: boyko-work@ukr.net

The paper considers an expanded cognitive-imitation model of a complex technical system. This model can be used for modeling the loss of complex system control scenarios under pressure of external adverse effects and damaging factors. The extension of the model is proposed in the form of adding elements that allow to emulate the cybernetic aspect of system survivability and reliability. Also the possibilities of practical application of the extended model in accordance with the standard of risk management ISO 31000:2009 are considered.

Keywords: risk management, reliability, survivability, complex technical systems, cognitive-simulation modeling.

ПАРАЛЕЛЬНІ АЛГОРИТМИ РОЗВ'ЯЗАННЯ ПРОСТОРОВОЇ ЗАДАЧІ ЦИФРОВОЇ ФІЛЬТРАЦІЇ ДАНИХ

М. С. Яджак

Інститут прикладних проблем механіки і математики ім. Я.С. Підстригача НАН України,
вул. Наукова, 3-Б, м. Львів, 79060, Україна; e-mail: yadzhak_ms@ukr.net

У роботі запропоновано паралельні алгоритми з автономними гілками для розв'язання просторової задачі цифрової фільтрації. Наведено оцінки прискорення, які підтверджують високу ефективність цих алгоритмів. Запропоновані паралельні алгоритми зорієнтовані для реалізації на сучасних широкодоступних високопродуктивних обчислювальних засобах – багатоядерних комп'ютерах, кластерах та системах з гібридною архітектурою. Одержані в роботі результати можуть бути використані під час дослідження в режимі реального часу стану та якості функціонування складних динамічних систем, зокрема транспортних.

Ключові слова: паралельний алгоритм, цифрова фільтрація, складна система, обмежений паралелізм, прискорення обчислень, кластер.

Вступ

У роботах [1–4] описано методику комплексного детермінованого оцінювання складних систем (СС) із ієрархічно-мережевою структурою. Цю методику використано для оцінювання стану та якості функціонування біомеханічних і робототехнічних систем локомоційного типу [5], а також для оцінювання окремих підсистем залізничної транспортної системи України [6]. У більшості випадків оцінювання СС необхідно здійснювати у режимі реального часу. Однією із важливих складових згаданої методики є попереднє оброблення великих масивів даних (Big Data) [7, 8], які використовуються під час дослідження системи. Такі вхідні дані можуть бути різних типів: числові, текстові, звукові, графічні (плоскі або просторові зображення), відеодані тощо. У [9, 10] запропоновано оптимальні за швидкодією (у заданих класах) паралельно-конвеєрні алгоритми розв'язання задач фільтрації різної вимірності. Ці алгоритми зорієнтовані на реалізацію на відповідних спеціалізованих обчислювальних засобах – квазісистолічних структурах. Тому актуальною є проблема розробки ефективних паралельних алгоритмів цифрової фільтрації даних на сучасних широкодоступних високопродуктивних обчислювальних системах – багатоядерних комп'ютерах та кластерах.

Метою цієї роботи є розробка та дослідження паралельних алгоритмів з автономними гілками для числового розв'язання просторової задачі цифрової фільтрації (ЗЦФ) даних.

Задача цифрової фільтрації та послідовний алгоритм її розв'язання

Загалом розглядувана просторова задача фільтрації полягає у виконанні S переобчислень згладжування масиву значень N змінних $x_{i,j,k}$ ($i = \overline{1, l_1}$; $j = \overline{1, l_2}$; $k = \overline{1, l_3}$) через рухоме вікно розміром M [9]. Для розв'язання цієї задачі можна скористатися послідовним алгоритмом, який має наступний вигляд:

FOR $l=1, C$ DO

{ FOR ALL $(i, j, k) \in \{(i', j', k') : 1 \leq i' \leq l_1; 1 \leq j' \leq l_2; 1 \leq k' \leq l_3\}$ DO

{ $p = 0$

FOR ALL $(s_1, s_2, s_3) \in \{(s'_1, s'_2, s'_3) : -m_1 \leq s'_1 \leq m_1; -m_2 \leq s'_2 \leq m_2; -m_3 \leq s'_3 \leq m_3\}$ DO (1)

{ $p = p + x_{i+s_1, j+s_2, k+s_3}^{(l-1)} * f_{s_1, s_2, s_3}$ }

$x_{i, j, k}^{(l)} = p$ } }.

У наведеному алгоритмі $f_{-m_1, -m_2, -m_3}, \dots, f_{0, 0, 0}, \dots, f_{m_1, m_2, m_3}$ – задані вагові коефіцієнти; $x_{i, j, k}^{(l)}$ – l -те переобчислення значення змінної $x_{i, j, k}$. Згідно з (1) для переобчислення на l -му кроці значень змінних використовуються виключно значення, переобчислені на $(l-1)$ -му кроці, при цьому $N = l_1 l_2 l_3$; $M = (2m_1 + 1)(2m_2 + 1)(2m_3 + 1)$. Зазначимо, що величини

$$\begin{aligned} & x_{1-m_1, j^*, k^*}^{(l)}, x_{2-m_1, j^*, k^*}^{(l)}, \dots, x_{0, j^*, k^*}^{(l)}; \quad x_{l_1+1, j^*, k^*}^{(l)}, x_{l_1+2, j^*, k^*}^{(l)}, \dots, x_{l_1+m_1, j^*, k^*}^{(l)}; \\ & x_{i, 1-m_2, k^*}^{(l)}, x_{i, 2-m_2, k^*}^{(l)}, \dots, x_{i, 0, k^*}^{(l)}; \quad x_{i, l_2+1, k^*}^{(l)}, x_{i, l_2+2, k^*}^{(l)}, \dots, x_{i, l_2+m_2, k^*}^{(l)}; \\ & x_{i, j, 1-m_3}^{(l)}, x_{i, j, 2-m_3}^{(l)}, \dots, x_{i, j, 0}^{(l)}; \quad x_{i, j, l_3+1}^{(l)}, x_{i, j, l_3+2}^{(l)}, \dots, x_{i, j, l_3+m_3}^{(l)}; \\ & (j^* = \overline{1-m_2, l_2+m_2}; k^* = \overline{1-m_3, l_3+m_3}; i = \overline{1, l_1}; j = \overline{1, l_2}; l = \overline{0, C-1}) \end{aligned}$$

є заданими константами.

Розробка паралельних алгоритмів

Для (1) розглянемо простір ітерацій I [11], що є наступною множиною цілочисельних векторів:

$$I = \{(i, j, k, l) : 1 \leq i \leq l_1; 1 \leq j \leq l_2; 1 \leq k \leq l_3; 1 \leq l \leq C\}.$$

Результуючими у наведеному просторі будуть N ітерацій, що утворюють його деяку підмножину I_r :

$$I_r = \{(i, j, k, C) : 1 \leq i \leq l_1; 1 \leq j \leq l_2; 1 \leq k \leq l_3\}.$$

Зазначимо, що на кожній ітерації виконуються обчислення, задані в (1) фрагментом із чотирьох останніх операторів.

На підставі використання методу пірамід [12] для розпаралелювання циклів із (1) одержуємо паралельний алгоритм з автономними гілками для розв'язання просторової ЗЦФ, який можна описати конструкцією:

$$\begin{aligned}
& \text{FOR ALL } (k_1, k_2, k_3) \in \{(k_1', k_2', k_3') : 1 \leq k_1' \leq l_1; 1 \leq k_2' \leq l_2; 1 \leq k_3' \leq l_3\} \text{ DO PAR} \\
& \quad \{ \text{FOR } l=1, C \text{ DO} \\
& \quad \quad \{ \text{FOR ALL } (i, j, k) \in \{(i_t, i_2, i_3) : \max\{1, (l-C)m_t + k_t\} \leq i_t \leq \min\{l_t, (C-l)m_t + k_t\};} \\
& \quad \quad \quad 1 \leq t \leq 3 \} \text{ DO} \\
& \quad \quad \{ p = 0 \\
& \quad \quad \quad \text{FOR ALL } (s_1, s_2, s_3) \in \{(s_1', s_2', s_3') : -m_1 \leq s_1' \leq m_1; -m_2 \leq s_2' \leq m_2; -m_3 \leq s_3' \leq m_3\} \text{ DO} \\
& \quad \quad \quad \{ p = p + x_{i+s_1, j+s_2, k+s_3}^{(l-1)} * f_{s_1, s_2, s_3} \} \\
& \quad \quad \quad x_{i, j, k}^{(l)} = p \} \} \}.
\end{aligned} \tag{2}$$

У наведеному алгоритмі тип паралельності *PAR* є *AUTON* [13] і задає паралельне виконання N гілок, які не взаємодіють між собою. Очевидно, що на практиці це є можливим, якщо можна залучити N процесорів (ядер) або обчислювальних вузлів. Однак, кожен багатоядерний комп'ютер або кластер має наперед визначену кількість обчислювальних елементів, яка зазвичай є значно меншою, ніж N . Тому для ефективного розв'язання просторової ЗЦФ нами запропоновано алгоритм з обмеженим паралелізмом [14], який дозволяє враховувати обсяг наявних ресурсів обчислювального засобу:

$$\begin{aligned}
& \text{FOR ALL } (r_1, r_2, r_3) \in \{(p, r, s) : 1 \leq p \leq P_1; 1 \leq r \leq P_2; 1 \leq s \leq P_3\} \text{ DO PAR} \\
& \{ \text{FOR } l=1, C \text{ DO} \\
& \{ \text{FOR ALL } (i, j, k) \in \{(i_1, i_2, i_3) : \max\{1, (l-C)m_t + (r_t-1)l_t / P_t + 1\} \leq i_t \leq \\
& \leq \min\{l_t, (C-l)m_t + r_t l_t / P_t\}; 1 \leq t \leq 3\} \text{ DO} \\
& \{ p = 0 \\
& \text{FOR ALL } (s_1, s_2, s_3) \in \{(s'_1, s'_2, s'_3) : -m_1 \leq s'_1 \leq m_1; -m_2 \leq s'_2 \leq m_2; -m_3 \leq s'_3 \leq m_3\} \text{ DO} \\
& \{ p = p + x_{i+s_1, j+s_2, k+s_3}^{(l-1)} * f_{s_1, s_2, s_3} \} \\
& x_{i, j, k}^{(l)} = p \} \} \}.
\end{aligned}
\tag{3}$$

Тут P – кількість паралельних гілок, які можна реально одночасно виконати на кластері або багатоядерному комп'ютері; $P = P_1 P_2 P_3$, $P < N$ і l_1, l_2, l_3 є кратними відповідно до P_1, P_2, P_3 . Тип паралельності PAR в (3) є $AUTON$.

Твердження. Алгоритми (1), (2) та (3) є еквівалентними за інформаційним графом.

Доведення цього твердження впливає із структури терм-історій (дерев) алгоритмів (1), (2) та (3) обчислення значення деякої змінної $x_{i,j,k}$ на заданому кроці [9].

Аналогічно, як і в [15], нами встановлено, що згідно із цими деревами обчислюється один і той же вираз.

Зазначимо, що у (2) та (3) процес згладжування можна дещо покращити, якщо останні чотири рядки в них замінити фрагментом:

$$\{ p_{i,j,k} = 0$$

$$FOR \ ALL \ (s_1, s_2, s_3) \in \{(s'_1, s'_2, s'_3) : -m_1 \leq s'_1 \leq m_1; -m_2 \leq s'_2 \leq m_2; -m_3 \leq s'_3 \leq m_3\} \ DO$$

$$\{ p_{i,j,k} = p_{i,j,k} + x_{i+s_1, j+s_2, k+s_3} * f_{s_1, s_2, s_3} \}$$

$$x_{i,j,k} = p_{i,j,k} \} \} \}.$$

Одержані унаслідок цього паралельні алгоритми дозволять у кожній автономній гілці під час переобчислення значення деякої змінної на заданому кроці використовувати значення, які є вже переобчисленими на цьому ж кроці.

Оцінювання алгоритмів фільтрації

Використовуючи сформульоване вище твердження, одержимо прискорення для запропонованих паралельних алгоритмів фільтрації (2) та (3). Припустимо, що t_{op} – це час виконання подвійної операції додавання-множення. Тоді для виконання алгоритмів (1)–(3) потрібен відповідно такий час:

$$T_1 = t_{op} MNC;$$

$$T_2 = t_{op} MC[1 + (2C(C-1)m_1m_2m_3 + (2/3)(2C-1)(m_2m_3 + m_1m_3 + m_1m_2) + m_1 + m_2 + m_3)(C-1)];$$

$$T_3 = t_{op} MC \left[\frac{N}{P} + \left(m_1 \frac{l_2}{P_2} \frac{l_3}{P_3} + m_2 \frac{l_1}{P_1} \frac{l_3}{P_3} + m_3 \frac{l_1}{P_1} \frac{l_2}{P_2} + (2/3) \left(m_1m_2 \frac{l_3}{P_3} + m_1m_3 \frac{l_2}{P_2} + \right. \right. \right.$$

$$\left. \left. + m_2m_3 \frac{l_1}{P_1} \right) (2C-1) + 2m_1m_2m_3(C-1)C \right) (C-1) \right].$$

Зауважимо, що наведені оцінки для часу виконання алгоритмів (1)–(3) враховують лише час виконання арифметичних операцій додавання та множення. На підставі цих оцінок одержуємо прискорення паралельних алгоритмів (2) та (3) порівняно з послідовною реалізацією:

$$S_2 = \frac{T_1}{T_2} = \frac{N}{1 + (2C(C-1)m_1m_2m_3 + (2/3)(2C-1)(m_2m_3 + m_1m_3 + m_1m_2) + m_1 + m_2 + m_3)(C-1)};$$

$$S_3 = \frac{T_1}{T_3} = \left[\frac{1}{P} + \left(\frac{m_1}{l_1P_2P_3} + \frac{m_2}{l_2P_1P_3} + \frac{m_3}{l_3P_1P_2} + \frac{2}{3} \left(\frac{m_1m_2}{l_1l_2P_3} + \frac{m_1m_3}{l_1l_3P_2} + \frac{m_2m_3}{l_2l_3P_1} \right) (2C-1) + \right. \right.$$

$$\left. \left. + \frac{2m_1m_2m_3}{N} (C-1)C \right) (C-1) \right]^{-1}.$$

Зазвичай на практиці $l_i \gg m_i$, $l_i \gg C \quad \forall i: i = \overline{1,3}$, а також l_i відрізняється ($l_i > m_i C^3$) від $m_i C^3 \quad \forall i: i = \overline{1,3}$ не менш, як на декілька порядків, тому прискорення S_2 буде значним, а $S_3 \approx P$. Отже, S_3 за зроблених припущень є близьким до свого оптимального значення. У разі $l_1 = l_2 = l_3 = 1000$; $C = 10$; $m_1 = m_2 = m_3 = 1$ одержуємо, що $S_2 \approx 502512.56$, а для параметрів задачі фільтрації $l_1 = 100$; $l_2 = 500$; $l_3 = 200$; $C = 5$; $m_1 = 2$; $m_2 = m_3 = 3$ маємо: $S_2 \approx 1425.11$.

Розроблені паралельні алгоритми (2) та (3) зорієнтовані для ефективної реалізації на багатоядерних комп'ютерах (засоби зі спільною пам'яттю), кластерах (засоби з розподіленою пам'яттю) та обчислювальних засобах з гібридною архітектурою (кластери, що залучають для обчислень блоки графічних процесорів) [16, 17].

Висновки

У роботі розроблено та досліджено паралельні алгоритми з автономними гілками для розв'язання просторової ЗЦФ на сучасних високопродуктивних обчислювальних засобах. Наведено оцінки прискорення, які підтверджують високу ефективність запропонованих алгоритмів фільтрації. Одержані результати можуть бути використані для попереднього оброблення в режимі реального часу просторових зображень та експериментальних даних для дослідження багатовимірних об'єктів СС.

Подальші дослідження автор вбачає у виявленні особливостей застосування одержаних результатів на практиці для конкретних предметних областей, зокрема і під час оцінювання якості функціонування таких складних динамічних систем, як транспортні системи, системи газо-, водо-, енергопостачання тощо.

Список літератури

1. Поліщук, Д. О. Комплексне детерміноване оцінювання складних ієрархічно-мережових систем. Частина I. Опис методики / Д. О. Поліщук, О. Д. Поліщук, М. С. Яджак // Системні дослідження та інформаційні технології, 2015. – № 1. – С. 21 - 31.
2. Polishchuk, D. About Evaluation of Complex Dynamical Systems / D. Polishchuk, O. Polishchuk // Journal of Complex Systems, 2013. – Article ID 204304, 6 p. [Електронний ресурс]. Режим доступу: <http://dx.doi.org/10.1155/2013/204304> (дата звернення: 5.08.2017).
3. Polishchuk, D. Complex Evaluation of Hierarchically-Network Systems / D. Polishchuk, O. Polishchuk, M. Yadzhak // Automatic Control and Information Sciences, 2014. – 2, № 2. – Pp. 32 - 44.
4. Поліщук, Д. О. Інформаційна технологія комплексного детермінованого оцінювання складних ієрархічно-мережових систем / Д. О. Поліщук. – Автореф. дис. к. т. н., спеціальність 05.13.06 – інформаційні технології. – Львів: Українська академія друкарства, 2017. – 21 с.
5. Поліщук, О. Д. Оптимізація оцінки функціонування опорно-рухового апарату людини / О. Д. Поліщук // Комп'ютерна математика. Оптимізація обчислень: Зб. наук. праць. – Київ: Інститут кібернетики ім. В. М. Глушкова НАН України, 2001. – Т. 2. – С. 360 - 367.
6. Поліщук, Д. О. Оцінювання стану колійного господарства Укрзалізниці / Д. О. Поліщук // Вісник Дніпропетровського національного університету залізничного транспорту імені акад. В. Лазаряна, 2012. – Вип. 41. – С. 203 - 211.
7. Polishchuk, O. Big Data Processing in Complex Hierarchical Network Systems I: Structures and Information Flows / O. Polishchuk, D. Polishchuk, M. Tyutyunnyk, M. Yadzhak // AASCIT Communications, 2016. – 3, № 3. – Pp. 112 - 118.
8. Polishchuk, O. Big Data Processing in Complex Hierarchical Network Systems II: Computer Environments and Parallelization / O. Polishchuk, D. Polishchuk, M. Tyutyunnyk, M. Yadzhak // AASCIT Communications, 2016. – 3, № 3. – Pp. 119 - 124.
9. Анисимов, А. В. Построение оптимальных алгоритмов массовых вычислений в задачах цифровой фильтрации / А. В. Анисимов, М. С. Яджак // Кибернетика и системный анализ, 2008. – № 4. – С. 3 - 14.

10. Яджак, М. С. Високопаралельні алгоритми та засоби для розв'язання задач масових арифметичних і логічних обчислень / М. С. Яджак. – Автореф. дис. д. ф.-м. н., спеціальність 01.05.03 – математичне та програмне забезпечення обчислювальних машин і систем. – Київ: КНУ імені Тараса Шевченка, 2009. – 33 с.
11. Lamport, L. The parallel Execution of DO Loops / L. Lamport // Communications of ACM, 1974. – 17, № 2. – Рр. 83 - 93.
12. Вальковський, В. О. Проблеми подальшого розвитку та модифікації методу пірамід для розпаралелювання циклів / В. О. Вальковський, М. С. Яджак // Мат. методи та фіз.-мех. поля, 2000. – 43, № 1. – С. 68 - 75.
13. Вальковский, В. А. Распаралеливание алгоритмов и программ. Структурный подход / В. А. Вальковский. – М.: Радио и связь, 1989. – 176 с.
14. Яджак, М. С. Алгоритмы с ограниченным параллелизмом для решения одной задачи цифровой фильтрации / М. С. Яджак // Проблемы управления и информатики, 2001. – № 6. – С. 109 - 118.
15. Яджак, М. С. Об оптимальном в одном классе алгоритме решения трёхмерной задачи цифровой фильтрации / М. С. Яджак // Проблемы управления и информатики, 2000. – № 6. – С. 66 - 81.
16. Інформаційно-аналитический центр по параллельным вычислениям [Електронний ресурс]. Режим доступа: www.parallel.ru (дата звернення: 10.08.2017).
17. Український національний грід. Базовий координаційний центр [Електронний ресурс]. Режим доступа: www.ung.in.ua (дата звернення: 12.08.2017).

ПАРАЛЛЕЛЬНЫЕ АЛГОРИТМЫ РЕШЕНИЯ ПРОСТРАНСТВЕННОЙ ЗАДАЧИ ЦИФРОВОЙ ФИЛЬТРАЦИИ ДАННЫХ

М. С. Яджак

Институт прикладных проблем механики и математики им. Я. С. Пидстригача НАН Украины,
ул. Научная, 3-Б, г. Львов, 79060, Украина; e-mail: yadzhak_ms@ukr.net

В работе предложены параллельные алгоритмы с автономными ветвями для решения пространственной задачи цифровой фильтрации. Приведены оценки ускорения, подтверждающие высокую эффективность этих алгоритмов. Предложенные параллельные алгоритмы ориентированы для реализации на современных широкодоступных вычислительных средствах – многоядерных компьютерах, кластерах и средствах гибридной архитектуры. Полученные в работе результаты могут быть использованы для исследования состояния и качества функционирования сложных динамических систем, в том числе и транспортных.

Ключевые слова: параллельный алгоритм, цифровая фильтрация, сложная система, ограниченный параллелизм, ускорение вычислений, кластер.

PARALLEL ALGORITHMS FOR SOLVING THE SPATIAL PROBLEM OF DATA DIGITAL FILTERING

M. S. Yadzhak

Ya. S. Pidstryhach Institute for Applied Problems of Mechanics and Mathematics, NAS Ukraine,
3B, Naukova Str., Lviv, 79060, Ukraine; e-mail: yadzhak_ms@ukr.net

In the work the parallel algorithms with autonomous branches for solving the spatial of digital filtering problem are proposed. The speed up estimates, which confirm high effectiveness of these algorithms, are pointed. The proposed parallel algorithms are oriented for implementation on modern widely-accessible computation means such as multicore computers, clusters and means with the hybrid architecture. The results of this work can be used for research of the state and operation quality of complex dynamical systems, including transport ones.

Keywords: parallel algorithm, digital filtering, complex system, limited parallelism, speed up of computations, cluster.

СЕРВІС-ОРІЄНТОВАНИЙ ІНФОРМАЦІЙНИЙ РЕСУРС КАФЕДРИ ВНЗ В ГІБРИДНІЙ ХМАРНІЙ ІНФРАСТРУКТУРІ

В.Є. Малахов, Л.А. Волощук

Одеський національний університет імені І.І. Мечнікова,
вул. Дворянська, 2, Одеса, 65026, Україна; e-mail: lavstumbre@gmail.com

Розглянуто питання створення інформаційного ресурсу кафедри як хмарної інформаційної системи для автоматизації процесів формування і управління документацією кафедри та інформаційної підтримки прийняття управлінських рішень. Запропоновано модель кафедрального документа, розроблена сервіс-орієнтована архітектура інформаційного ресурсу кафедри, яка реалізована на гібридній хмарній платформі. Розглянуто підхід до інтеграції бази даних документації в базу даних хмарного файлового сервісу.

Ключові слова: сервіс-орієнтована архітектура, інформаційна система, гібридна хмарна платформа.

Вступ

У сучасних умовах конкуренції в сфері вищої освіти особливого значення набуває поняття ефективної діяльності вищих навчальних закладів (ВНЗ), яке в значній мірі залежить від якості управління науково-педагогічним колективом вищого навчального закладу.

Одним з варіантів оптимізації адміністративної діяльності у ВНЗ і його підрозділах є впровадження інформаційних технологій в управління. Інформатизація управління може бути, зокрема, представлена як автоматизація діяльності окремих підрозділів і процесів.

Випускова кафедра, як найважливіший підрозділ ВНЗ, виконуючи навчальну, методичну, наукову та організаційну роботу зі студентами в ході навчального процесу, стикається з великим обсягом відповідної документації, яку необхідно формувати, супроводжувати, зберігати, а для прийняття управлінських рішень - аналізувати.

Можна виділити низку проблем, які виникають, коли опрацювання документів ведеться традиційним способом:

- втрата документів;
- накопичення величезної кількості невикористовуваних документів;
- відсутність місця для нормативного зберігання документів;
- дотримання конфіденційності документів та інформації в цілому;
- великі трудовитрати на пошук потрібного документа і формування тематичної добірки документів;
- дублювання одного і того ж документа з подальшими його виправленнями і складністю відстеження останніх, «правильних» копій;
- трудовитрати на підготовку і узгодження документів.

Впровадження автоматизованої системи для роботи з документацією кафедри дозволяє вирішити всі ці проблеми, а також:

- спрощує роботу з документами, підвищує її ефективність;

- підвищує продуктивність праці співробітників за рахунок скорочення часу створення, обробки і пошуку документів;
- підвищує оперативність доступу до інформації;
- розмежовує права доступу співробітників до інформації.

Реалізація такої повнофункціональної автоматизованої системи являє собою процес створення спеціалізованого програмного забезпечення, що є досить складним завданням та вимагає залучення великих матеріальних та інтелектуальних ресурсів, тому застосування сучасних інформаційних технологій, вибір ефективної архітектури створюваної системи, які безпосередньо впливають на необхідний обсяг витрат при її реалізації, є актуальними [1].

Особливе місце в сучасних напрямках розвитку інформаційних технологій займають хмарні технології і платформи. Вони реалізують економічність експлуатації додатків, масштабованість, мобільність доступу клієнтів, дозволяють використовувати безліч різних хмарних сервісів і служб, що полегшують процес створення програмного забезпечення сервіс-орієнтованої архітектури в різних предметних областях.

Мета роботи – розробка інформаційного ресурсу кафедри ВНЗ на гібридній хмарній платформі з інтеграцією до нього хмарних сервісів.

Основна частина

При проектуванні інформаційного ресурсу кафедри була побудована модель даних, яка відображає інформаційні процеси, що пов'язані з формуванням, обліком та зберіганням документації кафедри.

Схематичне зображення моделі даних представлено на рис.1.

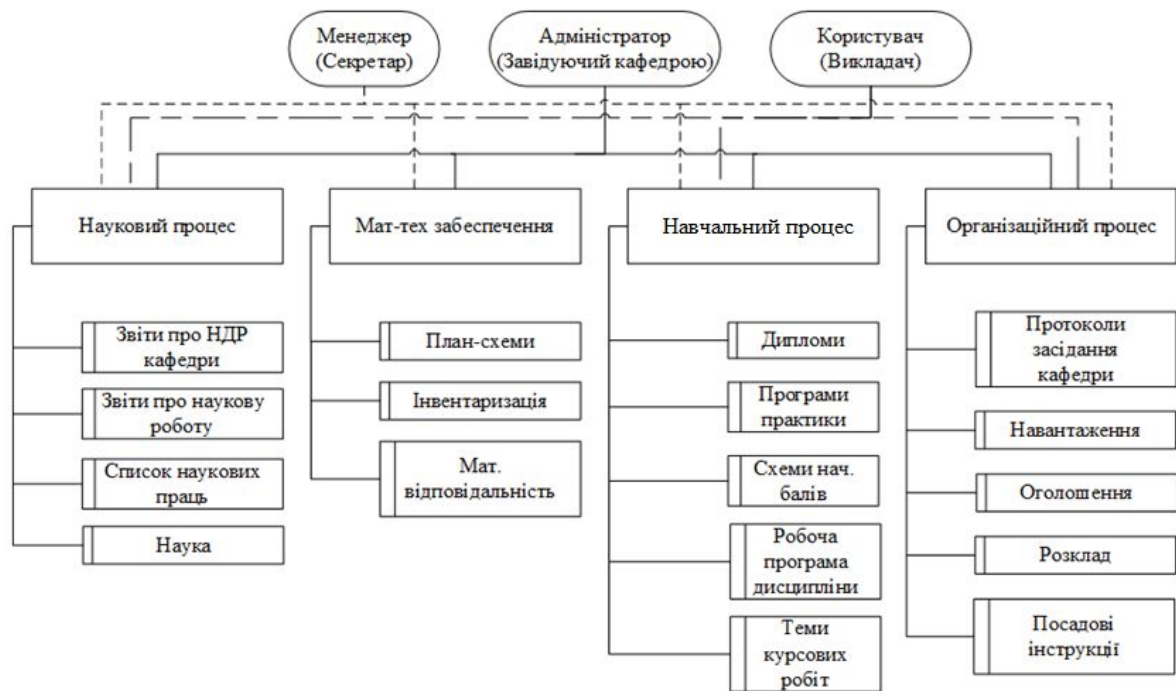


Рис. 1. Схематичне зображення моделі даних

У моделі виділено чотири основні типи процесів, до яких можуть належати документи [2]:

1. Навчальний процес – містить документи, пов'язані з навчальною діяльністю кафедри;

2. Науковий процес – у даному розділі представлені документи, які пов'язані з науково-дослідною роботою кафедри;

3. Організаційний процес містить у собі документи, що відображають організаційну роботу кафедри;

4. Матеріально-технічне забезпечення – даний розділ містить у собі документи, пов'язані з матеріальною відповідальністю кафедри.

Проведений аналіз структури документів дозволив визначити кілька типових документів для кожного із процесів.

Головною відмінністю простого набору текстових файлів від документів є наявність певної структури та атрибутів у документів. Грунтуючись на моделі, описаної вище, для кожного типу документів визначений ряд загальних і індивідуальних атрибутів.

Зокрема, до загальних атрибутів можна віднести автора документа, тип документа і його назву.

Індивідуальні атрибути можуть бути описані стандартним форматом представлення, а можуть описуватися різними, як по кількості атрибутів, так і по їхньому змісту.

Так до навчального процесу можна віднести такі документи та їх атрибути:

1. Дипломи і їх теми (автор роботи; науковий керівник; тема; навчальний рік; анотація);

2. Курсові роботи і їх теми (автор роботи; науковий керівник; тема; навчальний рік);

3. Навчальні плани спеціальностей (рік затвердження; назва спеціальності; рівень (бакалавр/магістр); форма навчання стаціонар/заочне);

4. Робочі навчальні плани (навчальний рік; назва спеціальності; рівень бакалавр/магістр; форма навчання стаціонар/заочне; різні документи по дисциплінах).

До наукового процесу можна віднести:

1. Списки наукових праць співробітників і студентів кафедри:

– тези конференцій (автори; науковий керівник; назва доповіді);

– статті (автори; назва; найменування видання; рік; категорія видання; індексованість);

– монографії (автори; назва; найменування видання; рік);

– навчальні посібники (автори; тема;

– навчальні видання (тип; видавництво; вид);

– патенти (назва; автор; рік; номер);

2. Проведені конференції (назва; дата);

– програма конференції;

– збірники тез конференції;

3. Звіти про наукову працю кафедри:

– науково-дослідна робота кафедри;

– заявка на НДР;

– звіт про наукову працю кафедри;

4. Протоколи наукових семінарів кафедри.

До організаційного процесу виділено такі типові документи, як:

– протоколи засідань кафедри (дата; номер);

– витяги з протоколів (дата; номер; призначення витягу);

– посадові інструкції (посада; ПІБ викладача);

– анкети викладачів (ПІБ викладача; дата формування анкети;

– штатний розклад (навчальний рік);

– план роботи кафедри (календарний рік);

– звіт роботи кафедри (календарний рік);

- розклад (семестр; викладач; день тижня; тиждень парний/непарний; пари);
- журнал про виконання аудиторного навантаження;
- індивідуальний план викладача;
- стажування;
- оголошення.

У результаті аналізу предметної області було виділено п'ять типів користувачів з відповідними рівнями доступу до інформаційного ресурсу кафедри в цілому. Три рівня доступу пов'язані з моделями користувач, менеджер, адміністратор і два рівня технічні – це гість та системний адміністратор.

Розглянемо кожного користувача окремо:

- гість – не авторизований користувач ресурсу, який може переглядати оголошення або перейти до файлової системи;
- користувач – авторизований співробітник кафедри, який має доступ до всіх сторінок і більшої частини функціонала;
- менеджер – співробітник кафедри, методист, що здійснює процес адміністрування користувальницького клієнта і файлової системи;
- адміністратор – менеджер із правами суперкористувача, завідувач кафедри, що дозволяють редагувати будь-які дані та налаштовувати конфігурації в ІС;
- системний адміністратор – суперкористувач, інтерфейс якого крім базової інформації містить повідомлення логів режиму налагодження.

Будь-який авторизований користувач такої інформаційної системи повинен мати можливість:

- переглянути список доступних йому документів і їх атрибутів;
- зберегти або завантажити документи на хмарне сховище;
- редагувати існуючі документи;
- скачати шаблон документа.

Користувачі, авторизовані з роллю адміністратора і менеджера, можуть:

- переглядати журнал активності користувачів;
- створювати нові аккаунти користувачів;
- створювати оголошення;
- редагувати календар зайнятості.

При проектуванні інформаційного ресурсу кафедри була обрана клієнт-серверна сервіс-орієнтована архітектура.

Сервіс-орієнтована архітектура (SOA) — це архітектура рівня підприємства, призначена для встановлення зв'язку з ресурсами на вимогу. Ці ресурси представлені у вигляді орієнтованих на задачі бізнесу сервісів, які можуть бути включені в пул ресурсів підприємства або напрямку бізнеса і модифіковані для задоволення відповідних бізнес-потреб [3].

Програмні комплекси (веб-сервіси), розроблені відповідно до сервіс-орієнтованої архітектури, звичайно реалізуються як набір веб-служб, взаємодіючих по протоколу SOAP, але існують і інші реалізації на основі REST.

Інтерфейси компонентів у сервіс-орієнтованій архітектурі інкапсулюють деталі реалізації (операційну систему, платформу, мову програмування) від інших компонентів, у такий спосіб забезпечуючи комбінування та багаторазове використання компонентів для побудови складних розподілених програмних комплексів, сприяючи масштабованості і керованості створюваних систем.

Схематичне зображення архітектури додатка представлено на рис. 2.

При проектуванні архітектури, було виділено чотири основні компоненти:

- клієнти являють собою користувачів, які можуть використовувати даний додаток із усіх основних пристроїв;

- у сервері додатку розташована основна логіка роботи інформаційного ресурсу кафедри і підключених підсистем, а також їх взаємодія зі сторонніми сервісами;
- сервер баз даних містить у собі БД зі схемами, необхідними для інформаційного ресурсу та підсистем архівації, обліку та зберігання документації;
- сторонні сервіси це незалежні від платформи, об'єктної моделі і клієнта програмні компоненти, які можна викликати з веб-додатків а також з інших сторонніх сервісів.

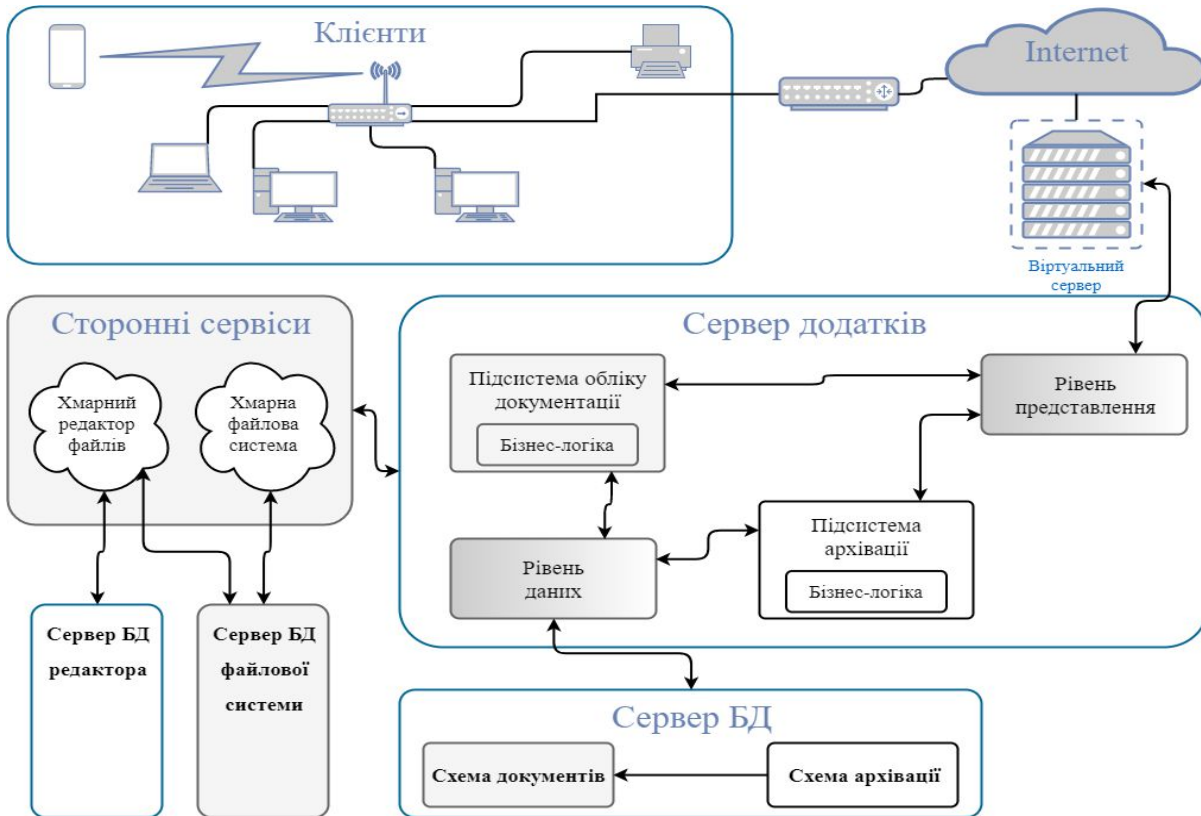


Рис. 2. Схема архітектури інформаційного ресурсу кафедри.

Для даного додатка було ухвалене рішення використовувати такі сторонні сервіси, як хмарна файлова система ownCloud[6] для візуалізації і розширення можливостей роботи з підсистемою ведення документів, а також хмарний редактор файлів OnlyOffice[8] для спільної роботи з файлами.

Хмарний сервіс редагування документів OnlyOffice — з 2014 року, SaaS проект із відкритим доступом команди фахівців з Ascensio System SIA. Версія, що окремо поставляється, OnlyOffice «Сервер документів» — це офісний пакет для роботи онлайн, який містить у собі переглядачі та редактори текстових документів, електронних таблиць і презентацій, повністю сумісні з форматами Office Open XML: .docx, .xlsx, .pptx, що і дозволяють спільно редагувати документи в режимі реального часу.

Сервіс функціонує під управлінням ОС Ubuntu. Взаємодія із зовнішнім середовищем здійснюється за допомогою сервера додатків Nginx.

Для генерації і розгортання бази даних, що містить тимчасову інформацію про файли, що редагуються, була використана єдина підтримувана СУБД — PostgreSQL.

Основним сервісом, інтегрованим у проект, є хмарна файлова система ownCloud. ownCloud — система для організації зберігання, синхронізації і обміну даними, розміщеними на зовнішніх серверах, некомерційна версія якої, розробляється ownCloud Community. Від інших подібних систем, ownCloud відрізняється наданням користувачеві повного контролю над своїми даними — інформація розміщується на

підконтрольних користувачеві системах. Доступ до даних в ownCloud може здійснюватися за допомогою web-інтерфейсу або протоколу WebDAV. Сервіс функціонує під управлінням ОС Ubuntu. Взаємодія із зовнішнім середовищем здійснюється за допомогою сервера додатків Apache2.

Для генерації і розгортання бази даних, ownCloud підтримує три СУБД: Mysql, Mariadb і Postgresql. В зв'язку з тим, що інформаційний ресурс кафедри працює з останньою, для ownCloud так само була використана дана СУБД. Для свого функціонування, хмарний сервіс ownCloud створює 42 таблиці на сервері БД.

Для підсистеми обліку та зберігання документації випускаючої кафедри була спроектована власна база даних, заснована на моделі даних, у якій зберігається уся інформація про документи.

Дані про файли повинні зберігатися в БД зовнішнього сервісу файлової системи, а дані про документи і їх властивостях — у БД спроектованій для підсистеми обліку та зберігання документації, у якій були виділені наступні сутності і їх властивості

Таблиця **document** є основною таблицею для підсистеми ведення документації, тому що в ній зберігаються атрибути документа, назва документа, дата пов'язана з ним та короткий опис.

Таблиця **type** містить перелік усіх типів документів.

Таблиця **proc** містить назви виділених процесів документів і розташування документів у файловій системі за замовчуванням.

У таблицю **author** винесено один з атрибутів документа — автор і співавтори документа.

Для підсистеми обліку і зберігання документації логічна схема була побудована у вигляді діаграми сутність-зв'язок (ER-діаграма) (рис.3).

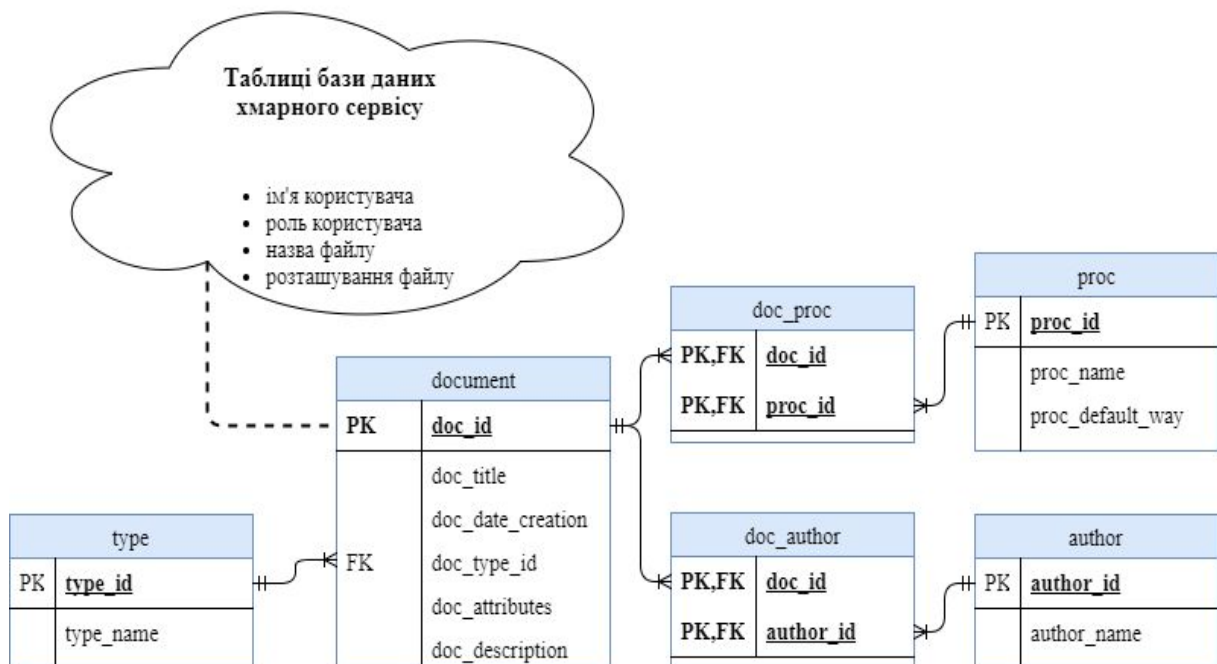


Рис. 3. Логічна схема БД

У базу даних ownCloud у вигляді самостійної додаткової схеми були інтегровані елементи БД підсистеми обліку і зберігання документації та реалізовані безпосередні зв'язки із чотирма таблицями ownCloud.

Дане об'єднання системи ownCloud і підсистеми обліку і зберігання документації було виконано вручну, однак у перспективі для подібної інтеграції предметної області передбачається використання методів викладених у статті [7].

Зв'язки між таблицями ownCloud і таблицями підсистеми обліку та зберігання документації представлені на діаграмі (рис. 4).

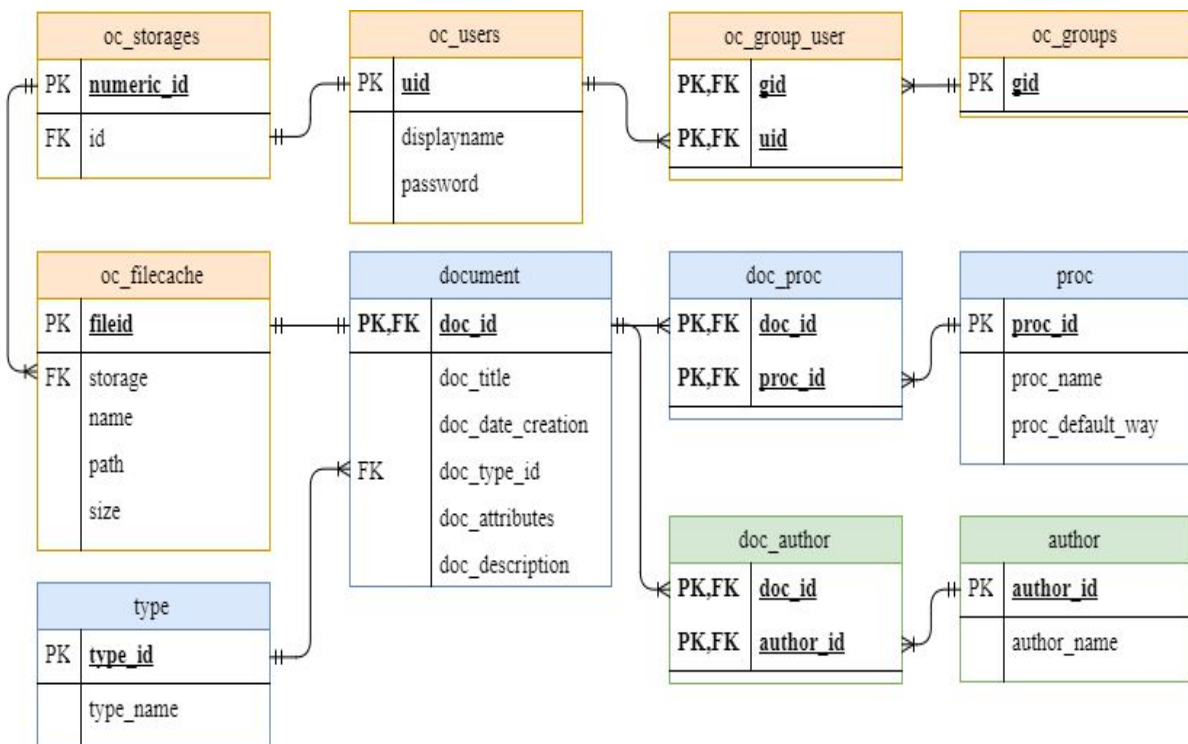


Рис. 4. Діаграма зв'язків між таблицями БД ownCloud і підсистеми обліку та зберігання документації кафедри

Для роботи підсистеми обліку і зберігання документації випускаючої кафедри був реалізований модуль, відповідальний за формування атрибутів документів з файлів (рис.5).

До даного модуля були висунуті наступні функціональні вимоги:

- одержання файлу як із сервісної файлової системи, так і через клієнтський додаток;
- при одержанні файлу хмарним сервісом, внесення інформації про основні атрибути файлу в таблиці відповідної схеми БД сервісу файлової системи;
- при одержанні файлу БД сервісу файлової системи, сформувані властивості документа за замовчуванням і додати дану інформацію в БД підсистеми обліку і зберігання документації;
- при одержанні файлу через клієнтський додаток, автоматично перенести файл у сервіс файлової системи і дати можливість користувачеві ввести базові атрибути будь-якого типу документа, такі як:
 - назва документа, яка не обов'язково повинна збігатися з назвою файлу;
 - автор і, якщо існують, співавтори документа;
 - тип документа і процес;
 - рік пов'язаний з документом, може бути, як календарним, так і навчальним;
 - коротка замітка до документа.

Після чого внести отримані атрибути в таблиці відповідної схеми БД сервісу файлової системи ownCloud.

Реалізація описаної бізнес-логіки, а також сполучення даних двох схем БД було реалізовано триггерами, доданими до таблиць БД хмарного сервісу ownCloud.

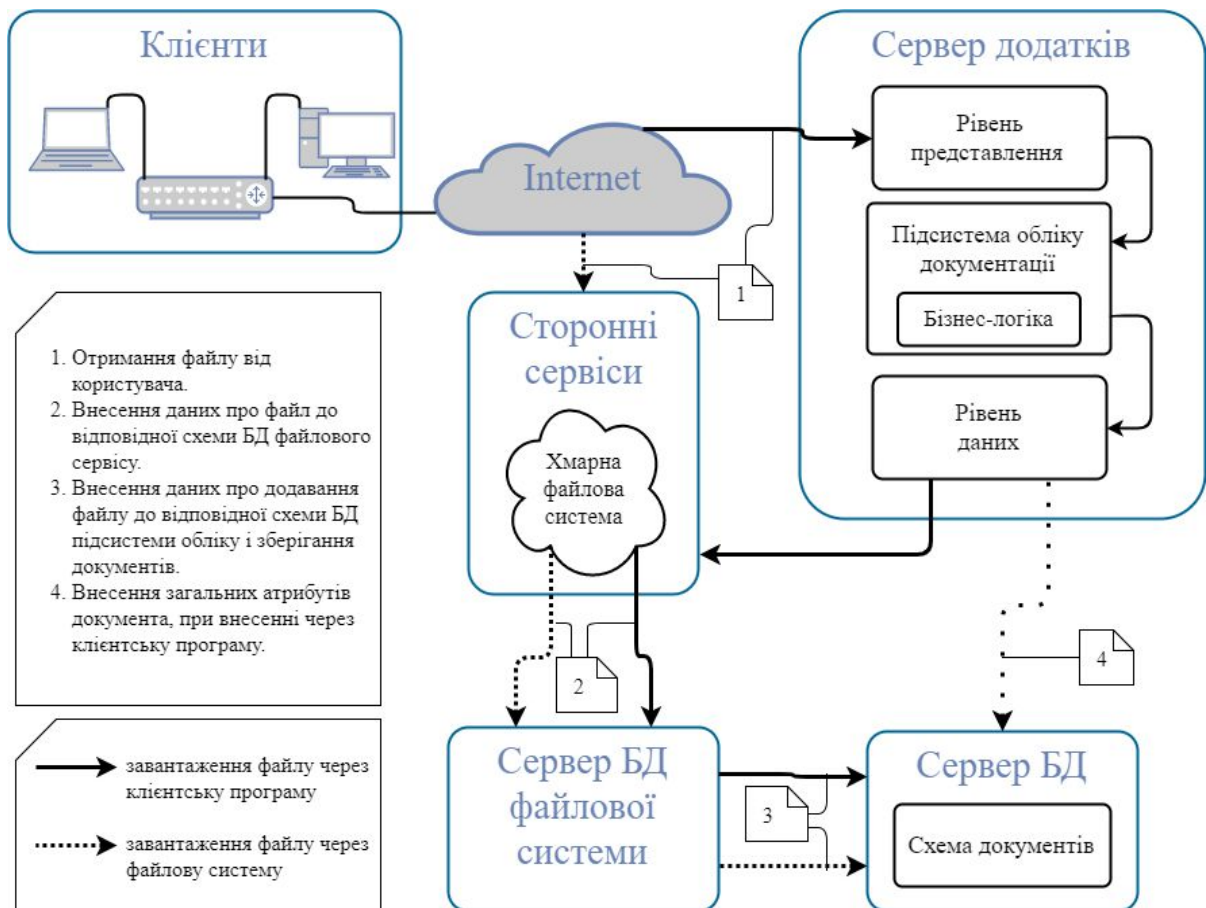


Рис. 5. Схема потоків даних при додаванні документа в інформаційний ресурс кафедри.

Для розгортання бази даних інформаційного ресурсу кафедри обрана вільна об'єктно-реляційна СУБД PostgreSQL, для роботи з якої використано фреймворк Spring JDBC, відповідальний за взаємодію Java-додатків з різними серверами СУБД[5].

Реалізація інформаційного ресурсу кафедри в розробленій архітектурі виконано з використанням патерну Spring-MVC фреймворка Spring [4]. Для розв'язання задач авторизації і автентифікації вирішено використати фреймворк Spring Security, який забезпечує мультисесійність і захист від атак.

Висновки

Запропонована модель документу дозволяє виконувати автоматизований аналіз, предметний пошук, систематизацію та архівне зберігання необхідних матеріалів за рахунок визначення для кожного документу його типу, структури, назви і сукупності загальних і спеціальних атрибутів.

Сервіс-орієнтована клієнт-серверна архітектура, розглянута в статті, дозволила реалізувати інформаційний ресурс кафедри на гібридній хмарній платформі. При цьому в публічній хмарі розміщуються хмарні сервіси для зберігання і редагування документів як файлів з можливістю необмеженого мобільного доступу до них користувачів системи, а на сервері додатка ВНЗ реалізується бізнес-логіка роботи зі структурованими документами. Для сполучення локальної та публічної частини платформи в БД хмарного файлового сервісу ownCloud інтегровано елементи БД локальних підсистем інформаційного ресурсу кафедри. Перетворення файлу в структурований документ реалізує спеціальний модуль формування атрибутів.

Крім безпосереднього використання для адміністративного управління кафедрами ВНЗ, даний ресурс розглядається як макет для дослідження, аналізу та налагодження технології побудови сервіс-орієнтованих гібридних хмарних архітектур і оптимізації розподіленого зберігання інформації.

Список літератури

1. Малахов, В.Е., Анализ систем управления высшими учебными заведениями / Малахов В.Е, Драбинка В.В, Волощук Л.А // Тезисы докладов 14 Всеукраинской конференции студентов и молодых учёных «Информатика, информационные системы и технологии». – Одесса, 2017. – С.167-168.
2. Драбинка, В.В., Модель данных информационного ресурса кафедры / Драбинка В.В, Малахов В.Е, Волощук Л.А // Тезисы докладов 14 Всеукраинской конференции студентов и молодых учёных «Информатика, информационные системы и технологии». – Одесса, 2017. – С.151-152.
3. Мамду Ибрахим. Сервис-ориентированная архитектура и архитектура предприятия. [Електронний ресурс]. Режим доступа: <https://www.ibm.com/developerworks/ru/library/ws-soa-enterprise1/index.html/> (дата звернення 25.03.2016)
4. Spring MVC — основные понятия, архитектура. [Електронний ресурс]. Режим доступа: <http://javastudy.ru/spring-mvc/spring-mvc-basic/> (дата звернення 9.12.2016)
5. Jon Ellis, Linda Ho. JDBC 3.0 Specification // Символ науки, 2001 – С.190.
6. ownCloud Documentation Overview. [Електронний ресурс]. Режим доступа: <https://doc.owncloud.org/> (дата звернення 17.05.2017)
7. Maria, G. Glava, Information systems reengineering approach based on the model of information systems domains. / Maria G. Glava, Valery E. Malakhov // International Journal of Software Engineering & Computer System. – Kuantan, Malaysia, 2017.
8. Установка версии Сервера документов для Linux. [Електронний ресурс] – Режим доступа : <http://helpcenter.onlyoffice.com/ru/server/linux/document/linux-installation.aspx> (дата звернення 31.05.2017)

**СЕРВИС–ОРИЕНТИРОВАННЫЙ ИНФОРМАЦИОННЫЙ РЕСУРС КАФЕДРЫ ВУЗа В
ГИБРИДНОЙ ОБЛАЧНОЙ ИНФРАСТРУКТУРЕ**

В.Є. Малахов, Л.А. Волощук

Одесский национальный университет имени И.И.Мечникова
ул. Дворянская, 2. Одесса, 65026, Украина; e-mail: lavstumbre@ gmail.com

Рассмотрены вопросы создания информационного ресурса кафедры как облачной информационной системы для автоматизации процессов формирования и управления документацией кафедры и информационной поддержки принятия управленческих решений. Предложена модель кафедрального документа, разработана сервис-ориентированная архитектура информационного ресурса кафедры, которая реализована на гибридной облачной платформе. Рассмотрен подход к интеграции базы данных документации в базу данных облачного файлового сервиса.

Ключевые слова: сервис-ориентированная архитектура, информационная система, гибридная облачная платформа.

**SERVICE - ORIENTED INFORMATION RESOURCE OF THE UNIVERSITY CHAIR IN THE
HYBRID CLOUD INFRASTRUCTURE**

V.E. Malakhov, L.A. Voloshchuk

Odessa I.I. Mechnikov National University,
2, Dvoryanskaya Str, Odessa, 65026, Ukraine; e-mail: lavstumbre@ gmail.com

The problems of the department information resource creation as a cloud information system for automation of the processes of the department documentation formation and management, information support for making managerial decisions are considered. The department document model is offered. The service-oriented architecture of the department information resource, which is implemented on a hybrid cloud platform, is developed. The approach to the documentation database integration into the cloud file service database is considered.

Keywords: service-oriented architecture, information system, hybrid cloud platform.

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

Том 7, номер 3, 2017. Одеса – 100 с., іл.

ИНФОРМАТИКА И МАТЕМАТИЧЕСКИЕ МЕТОДЫ В МОДЕЛИРОВАНИИ

Том 7, номер 3, 2017. Одесса – 100 с., ил.

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Volume 7, No. 3, 2017. Odesa – 100 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 №1 від 26.09.2017)

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, 2017