

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеський національний політехнічний університет

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ
МЕТОДИ В МОДЕЛЮВАННІ

INFORMATICS AND MATHEMATICAL
METHODS IN SIMULATION

Том 8, № 1

Volume 8, No. 1

Одеса – 2018
Odesa – 2018

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:

*Г.В. Ахмаметєва, Т.О. Банах, П.І. Бідюк,
Н.Д. Вайсфельд, А.Ф. Верлань, Г.М. Востров,
В.Б. Дудикевич, М.Б. Копитчук,
О.Ю. Лебедева, 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,
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:

*A. Akhmametiyeva, T. Banakh, P. Bidyuk,
V. Dudykevich, V. Khoroshko, N. Kopytchuk,
O. Lebedeva, S. Lenkov, I. Marakova,
S. Nesterenko, N. Nikitchenko, S. Polozhaenko,
J. Rubio, V. Rusov, O. Rybalsky, M. Shelest,
I. Tkachenko Gorski, A. Usov, N. Vaysfeld,
A. Verlan, G. Vostrov, M. Yadzhak*

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

Оригінал-макет виготовлено редакцією журналу

Адреса редакції: просп. Шевченка, 1, Одеса, 65044, Україна

Телефон: +38 048 705 8506

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

E-mail: immm.ukraine@gmail.com

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

Tel.: +38 048 705 8506

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

E-mail: immm.ukraine@gmail.com

© Одеський національний політехнічний університет, 2018

ЗМІСТ / CONTENTS

ПЛАНУВАННЯ ДІАГНОСТИЧНОГО ЕКСПЕРЕМЕНТУ ПРИ ЛОКАЛІЗАЦІЇ НЕСПРАВНОСТЕЙ ПІДСХЕМ БЕЗІНЕРЦІЙНИХ СИСТЕМ С.А. Положаєнко, Л.Л. Прокоф'єва	5	PLANNING OF THE DIAGNOSTIC EXPERIMENT IN THE LOCALIZATION OF TROUBLESHOOTING FAIURES OF SINGLE-FREE SYSTEMS Polozhaenko S., Prokofieva I.
АНАЛІЗ ТА ПРОГРАМУВАННЯ РИЗИКІВ ШАХРАЙСТВА З КРЕДИТНИМИ КАРТКАМИ Н.В. Кузнєцова	16	ANALYSIS AND FORECASTING OF CREDIT CARDS' FRAUD RISKS Kuznietsova N.
УДОСКОНАЛЕННЯ МЕТОДУ ВІДОКРЕМЛЕННЯ КЛОНУ ВІД ПРООБРАЗУ В ЦИФРОВОМУ ЗОБРАЖЕННІ І.І. Бобок, А.А. Кобозєва	26	IMPROVEMENT OF THE METHOD OF SEPARATING THE CLONE FROM THE PROTOTYPE IN DIGITAL IMAGE Bobok I., Kobozeva A.
САМОДІАГНОСТИКА КОМПЛЕКСНИХ СИСТЕМ З ПРОГРАМНО-КОНФІГУРОВАНОЮ СТРУКТУРОЮ І.В. Коробійчук, Р.В. Грищук, В.О. Хорошко, Ю.Є. Хохлачова	36	SELF-DIAGNOSTICS OF COMPLEX SYSTEMS WITH A SOFTWARE-CONFIGURABLE STRUCTURE Korobiichuk I., Hryshchuk R., Horoshko V., Hokhlacheva Yu.
СИНТЕЗ І МОДЕЛЮВАННЯ КОМБІНОВАНОЇ СИСТЕМИ УПРАВЛІННЯ З ВІМІРЮВАННЯМ ЗБУРЕННЯ ПО МОДЕЛІ ОБ'ЄКТА С.А. Бобріков, Е.Д. Пічугін, А.Г. Кисель	48	SYNTHESIS AND SIMULATION OF COMBINED CONTROL SYSTEMS WITH MEASUREMENTOF PERTURBATION BY MODEL OF THE OBJECT Bobrikov S., Pichugin E., Kisel A.
ПРОГНОЗУВАННЯ ТЕХНІЧНОГО СТАНУ ОДНОТИПНИХ ПРОГРАМНО-АПАРАТНИХ ЗАСОБІВ В.В. Кузавков, П.В. Хусаїнов	57	FORECASTING THE TECHNICAL STATE OF THE SAME TYPE SOFTWARE AND HARDWARE EQUIPMENT Kuzavkov V., Khusainov P.

УДОСКОНАЛЕННЯ РЕАЛІЗАЦІЇ
КРИПТОАЛГОРИТМУ ЕЛЬ-ГАМАЛЯ
НА ОСНОВІ СИСТЕМИ
ЗАЛИШКОВИХ КЛАСІВ

І.В. Якименко

69

IMPROVING THE IMPLEMENTATION
EL-GAMAL CRYPTOALGORITHM ON
THE BASIS OF THE SYSTEM OF
RESIDUE CLASSES

Yakymenko I.

ОПТИМІЗАЦІЯ МЕТОДІВ
ПРОГНОЗУВАННЯ, ОБРОБКИ ТА
АНАЛІЗУ ІНФОРМАЦІЇ В
РІЗНОСТРУКТУРНИХ СХОВИЩАХ
ДАНИХ

Д.С. Шибасєв, В.В. Вичужанін,
Н.О. Шибасєва, Н.Д. Рудніченко

78

OPTIMIZATION OF PREDICTION
METHODS, PROCESSING AND
ANALYSIS OF INFORMATION IN
DIFFERENT STRUCTURE DATA

Shibaiev D., Vichuzhanin V.,
Shibaieva N., Rudnichenko N.

ПІДТРИМКА ПРИЙНЯТТЯ РІШЕНЬ
ПРО РЕАЛІЗАЦІЮ ДОДАТКІВ В
ГІБРИДНІЙ ХМАРНІЙ
ІНФРАСТРУКТУРІ

Л.А. Волощук, О.І. Розновець,
Д.Д. Волощук

86

SUPPORT FO THE DECISION MAKING
ON IMPLEMENTATION OF
APPLICATIONS IN THE HYBRID
CLOUD INFRASTRUCTURE

Voloshchuk L., Roznovets O.,
Voloshchuk D.

**PLANNING OF THE DIAGNOSTIC EXPERIMENT IN THE LOCALIZATION OF
TROUBLESHOOTING FAILURES OF SINGLE-FREE SYSTEMS****S.A. Polozhaenko, L.L. Prokofieva**

Odesa National Polytechnic University,
1, Shevchenko Ave., Odesa, 65044, Ukraine; e-mail: sanp@gmail.com, prokofieva1957@gmail.com

Formalized conditions for carrying out a diagnostic experiment associated with the identification of faulty fragments (subschemes) of inertial-free systems are obtained. The diagnostic experiment is reduced to computational procedures for localization of faulty subschemes, which are based on testing hypotheses that the characteristics of the allocated subschemes have changed. Hypotheses are formulated in such a way as to ensure the detection of parametric and structural faults. The first, for example, may include changing the resistance of the circuit, and the second - an open or short circuit. When the system is divided into subschemes, the latter are selected from the condition of their parametric identifiability, i.e. The situation when, based on the known parameters of the remaining subschemes, as well as the input and output signals in the whole system, it is possible to determine the parameters of the subscheme under consideration. Planning a diagnostic experiment is as follows.

Assuming a linear relationship between the parameters of the allocated subscheme S_i and the output signals of the system, a verification matrix F is created in advance, which determines the interrelation of the indicated parameters and signals, considering the serviceability of the subscheme under consideration. In the event of a malfunction, the verification matrix F changes, which allows to determine the nonconformity matrix q , on the basis of which analysis it is possible to obtain an estimate $\Delta\hat{\rho}_i$ of the parameters $\Delta\rho_i$ of the subscheme S_i under consideration, as a result of which it is concluded that it is serviceable. Procedures for testing hypotheses on the health of the subschemes of the inertial-free system for cases of parametric and structural faults are of an identical nature. The principal difference between experiment planning and structural faults from planning for parametric faults is that for parametric faults the value $\Delta\rho_i$ does not depend on the input signals of the system, while for structural faults – the value $\Delta\rho_i$ depends on the input signals of the system, in an unknown way.

Keywords: diagnostics, diagnostic experiment, fault location, inertial-free systems, estimation of subschemes parameters

Introduction

To solve a wide range of problems in the study of systems (identification, control of operability, preventive maintenance), methods of the theory of experimental design are widely used, allowing, in the presence of measurement noise, to obtain estimates of the parameters of the system model that are best in some sense. It should also be taken into account that the features of the dynamic behavior of systems, for example, their lack of inertia, do not have a significant effect on the procedures for carrying out these experiments [1].

When diagnosing, even in the case of the most simple parametric faults in the subschemes, it is necessary first of all not to get the parameter estimates, but to establish the faulty subschemes. This formulation of the problem presupposes the need to ensure the best distinguish ability of the subschemes [2-4].

Objective of this article is formalization of the conditions for planning a diagnostic experiment in problems of determining the operability of inertial-free systems in the localization of parametric and structural faults in their subschemes.

Main part

Suppose that in one of the subschemes only parametric faults are possible. In this case, the description of the faulty subscheme S_i has the following form $Z_i = \varphi_i^*(V_i, \rho_i)$; $i = \overline{1, N}$, where Z_i – is the vector of the subschemes S_i parameters, $\rho_i = \rho_i^* + \Delta\rho_i$; $\rho_i \in D_p$, D_p – the area of the values of the subscheme S_i parameters, ρ^* – the vector of the nominal values of the dimension r_i parameters, N – the number of subschemes to be checked.

A subscheme S_i is parametrically identifiable if, with known parameters of the remaining subschemes, the input and output signals in the system as a whole can be determined by its subscheme S_i parameters.

Consider the subscheme S_i for which the relationship between the parameters and the output signals of the system is linear. In this case, the description of a system with a defective subscheme S_i can be represented as follows:

$$y = F^*(u) + \frac{\partial F^*(u)}{\partial \rho_i^m} \Delta\rho_i, \quad i = \overline{1, N}, \quad (1)$$

where y – the vector of the output signals of the system, u – the vector of the input signals of the system, $F^*(u)$ – a verification matrix composed of the elements of the fault dictionary.

Denoting $\left\{ \left[\frac{\partial F^*(u)}{\partial \rho_i^m} \right] \right\} = q_i(u)$, we rewrite (1) in the form

$$\Delta y = y - F^*(u) = q_i(u) \Delta\rho_i, \quad i = \overline{1, N}. \quad (2)$$

If there is such a value $u \in D_u$ as $\text{rank } q_i(u) = r_i$, then from (2) we can obtain an estimate $\Delta\hat{\rho}_i$ of the parameters $\Delta\rho_i$. In this case, the identification task is solved with one set of input signals of the system. If the $\text{rank } q_i(u) < r_i$, then the task of identification can be solved only if on the diagnosed system it is possible to give sets of input signals

$$U^\kappa = (u^1, \dots, u^\kappa)^T, \text{ in which } \text{rank } Q_i(U^\kappa) = \text{rank} \begin{bmatrix} q_i(u^1) \\ \vdots \\ q_i(u^\kappa) \end{bmatrix} = r_i.$$

Estimation of the parameters of the subsysteme S_i is determined from equation

$$\Delta Y(U^\kappa) = Q_i(U^\kappa) \Delta\rho_i, \quad i = \overline{1, N}, \quad (3)$$

where $\Delta Y(U^\kappa) = [\Delta y(u^1), \dots, \Delta y(u^\kappa)]^T$.

The problem of diagnosing will be solved by testing hypotheses H_{ρ_i} . The hypothesis H_{ρ_i} , $i = \overline{1, N}$ is the assumption that the parameters of the subscheme S_i have changed and the description of the system has the form (1).

The hypothesis H_{ρ_i} is verified by testing the compatibility of equation (3), whose matrix $Q(U^\kappa)$ must be rectangular.

Subschemes S_i , S_j ; $i \neq j$ are not distinguishable under the hypothesis H_{ρ_i} , if for a given value $\Delta\rho_j$ there exists such a value $\Delta\rho_i \in D_p$ that

$$q_i(u) \Delta\rho_i = q_j(u) \Delta\rho_j, \quad u \in D_u. \quad (4)$$

The criteria for the distinguish ability of the subschemes S_i , S_j parameters are determined from the conditions under which equality (4) is not satisfied.

The parameters of the subschemes S_i , S_j are distinguishable under the hypothesis H_{ρ_i} if and only if there exists a value U^κ such that

$$\text{rank} \left[Q_i(U^\kappa) \middle| Q_j(U^\kappa) \right] = r_i + \text{rank } Q_j(U^\kappa). \quad (5)$$

In this case, the subscheme S_j parameters can be unidentifiable due to the fact that $\text{rank } Q_j(U^\kappa) < r_j$.

Let us write down the necessary condition for the distinguish ability of the parameters of the subschemes S_i , S_j , under the hypothesis H_{ρ_i} $\text{rank} \left[Q_i(U^\kappa) \middle| Q_{j,s}(U^\kappa) \right] = r_i + 1$; $s = \overline{1, r_j}$, where $Q_{j,s}(U^\kappa)$ — is the s -th column of the matrix Q_j .

If only one parameter in the system is allowed to change, then condition (5) with respect to the distinguish ability of all the system parameters reduces to the existence of input signals of the system ensuring pair wise linear independence of the columns of the matrix $[Q_1(U^\kappa), \dots, Q_N(U^\kappa)]$, where N is the total number of parameters tested [5]. And linear independence of different columns can be achieved with different input signals of the system.

Planning a diagnostic experiment when estimating the subscheme parameters. Let the scalar output of y be measured with an error. Assuming that only parametric faults can exist in the subscheme S_i and the system model is linear in the parameters of the subsystems under test, the description of the faulty system is similar to (2) in the form $\Delta y + \xi = q_i(u) \Delta \rho_i$. Changing the values of the input signals of the system, we form, similarly to (3), a system of algebraic equations for obtaining estimates $\Delta \hat{\rho}_i$ of the parameters $\Delta \rho_i$:

$$\Delta \Lambda = Q_i \Delta \rho_i, \quad (6)$$

where $\Delta \Lambda = [\Delta y(u^1) + \xi^1, \dots, \Delta y(u^\kappa) + \xi^\kappa]^T$, $Q_i = Q_i(U^\kappa)$.

Suppose that the measurement error values ξ^r have a normal distribution with zero expectation $E[\xi^r] = 0$ and the same variance σ^2 , are not correlated with each other, and also with $q_i(u^r)$, $\Delta \rho_i$. In this case, the quantities $\Delta y(u^r) + \xi^r$, $r = \overline{1, K}$ are independent, normally distributed, with mathematical expectation $\Delta y(u^r)$ and the same variance σ^2 .

The assumptions made allow us to use the method of least squares to obtain an estimate $\Delta \hat{\rho}_i$:

$$\Delta \hat{\rho}_i = (Q_i^T Q_i)^{-1} Q_i^T \Delta \Lambda. \quad (7)$$

It is assumed that the matrix $Q_i^T Q_i = F_i$, called the information matrix (the Fisher matrix), is no degenerate.

If the vector were measured without errors, then from (3) it would be possible to obtain exact (errors of computation are not considered) parameter values $\Delta \rho_i = (Q_i^T Q_i)^{-1} Q_i^T \Delta Y$. The covariance matrix of estimates of the subscheme S_i parameters is as follows:

$$\text{cov}[\Delta\hat{\rho}_i] = E[(\Delta\hat{\rho}_i - \Delta\rho_i)(\Delta\hat{\rho}_i - \Delta\rho_i)^\tau] = \sigma^2 F_i.$$

Criteria for the optimal choice of input signals of the system are related to the form of the information matrix F_i and are aimed at minimizing any of its characteristics, for example, the value of the determinant [6].

The foregoing experimental planning assumes that the faulty subscheme is known and it is only necessary to determine its parameters. If the faulty subscheme is unknown, then when evaluating the parameters of the scanned subscheme, it is necessary to ensure that the parameters of the subschema are discernible with the subscheme parameters, which can in fact be faulty.

Planning a diagnostic experiment for parametric faults. Consider the planning of an experiment aimed at ensuring the distinguish ability of the parameters of subsystems S_i, S_j , when estimating the parameters of the subsystem S_i .

We divide the diagnostic equation (6) into two parts:

$$\Delta\Lambda_a = Q_{i,a} \Delta\rho_i, \quad (8)$$

$$\Delta\Lambda_b = Q_{i,b} \Delta\rho_i. \quad (9)$$

The compatibility of equation (6) can be checked by checking the unbiasedness of the estimates $\Delta\hat{\rho}_i^a, \Delta\hat{\rho}_i^b$, the parameters $\Delta\rho_i$ obtained from equations (8) and (9), respectively. Analogously to (7) from (8) we obtain an estimate of the parameters

$$\Delta\hat{\rho}_i^a = (Q_{i,a}^\tau Q_{i,a})^{-1} Q_{i,a}^\tau \Delta\Lambda_a = F_{i,a} Q_{i,a}^\tau \Delta\Lambda_a.$$

From (9) we obtain $\Delta\hat{\rho}_i^b = F_{i,b} Q_{i,b}^\tau \Delta\Lambda_b$.

If the subscheme S_j is faulty, the matrices $\Delta\Lambda_a, \Delta\Lambda_b$ are determined by expressions $\Delta\Lambda_a = Q_{j,a} \Delta\rho_j, \Delta\Lambda_b = Q_{j,b} \Delta\rho_j$.

Because of measurement errors $\Delta\hat{\rho}_i^a, \Delta\hat{\rho}_i^b$, estimates are random quantities with some areas of distribution of their values.

Depending on which of the subscheme (S_i or S_j) is faulty, the mathematical expectation $E[\Delta\hat{\rho}_i^a]$ and the covariance matrix $\text{cov}[\Delta\hat{\rho}_i^a]$ of the estimate $\Delta\hat{\rho}_i^a$ obtained under the hypothesis H_{ρ_i} are as follows:

$$E[\Delta\hat{\rho}_i^a] = \begin{cases} F_{i,a} Q_{j,a}^\tau \Delta\rho_j, & \text{at } j \neq i, \\ \Delta\rho_i, & \text{at } j = i, \end{cases}$$

If any of the subschemes is faulty: $\text{cov}[\Delta\hat{\rho}_i^a = \sigma^2 F_{i,a}] = \sigma^2 F_{i,a}$. Similar expressions are also obtained for $E[\Delta\hat{\rho}_i^b], \text{cov}[\Delta\hat{\rho}_i^b]$, by substituting in the expressions for $E[\Delta\hat{\rho}_i^a], \text{cov}[\Delta\hat{\rho}_i^a]$, the index «a» by «b».

The bias in the estimate $\Delta\hat{\rho}_i$ is determined by the magnitude

$$\rho_i = \Delta\hat{\rho}_i^a - \Delta\hat{\rho}_i^b. \quad (10)$$

The mathematical expectation and the covariance matrix of the vector ρ_i are as follows:

$$E[\rho_i] = \begin{cases} m_{i,i} = (F_{i,a} Q_{i,a}^T Q_{j,a} - F_{i,b} Q_{i,b}^T Q_{j,b}) \Delta \rho_j, & \text{at } j \neq i, \\ m_{i,j} = 0, & \text{at } i = j, \end{cases} \quad (11)$$

$$C_i = \text{cov}[\rho_i] = \sigma^2 (F_{i,a} + F_{i,b}). \quad (12)$$

As follows from (12), the covariance matrix of the vector ρ_i does not depend on which of the subschemes is faulty.

Let the system change only one parameter, i.e. $\Delta \rho_i$ – is a scalar. If the system of diagnostic equations (8), (9) consists of two scalar equations:

$$\Delta \Lambda_{i,a} = q_{i,a} \Delta \rho_i,$$

$$\Delta \Lambda_{i,b} = q_{i,b} \Delta \rho_i,$$

then

$$E[\rho_i] = \begin{cases} m_{i,i} = (\frac{q_{j,a}}{q_{i,a}} - \frac{q_{j,b}}{q_{i,b}}) \Delta \rho_j, & \text{at } j \neq i, \\ m_{i,j} = 0, & \text{at } j = i, \end{cases}$$

$$\beta_i = D[\rho_i] = \delta^2 (\frac{1}{q_{i,a}^2} + \frac{1}{q_{i,b}^2}).$$

For this distinction of subschemes S_i, S_j , it is necessary that the distribution areas of the quantities $\rho_{i,i}$ (ρ_i with a faulty subscheme S_i) and $\rho_{i,j}$ (ρ_j with a faulty subscheme S_j) do not overlap.

As an example, Fig. 1 shows the distribution of two-dimensional quantities $\rho_{i,i}, \rho_{i,j}$. The situation shown in Fig. 1, a, is characterized with respect to the situation shown in Fig. 1, b, higher accuracy of parameter estimates $\Delta \hat{\rho}_i$, but lower distinguish ability of subschemes S_i, S_j .



Fig. 1. Areas of distribution of two-dimensional quantities $\rho_{i,i}, \rho_{i,j}$: a – situation with higher accuracy of parameter estimates $\Delta \hat{\rho}_i$; b – situation with higher distinguish ability of subschemes S_i, S_j .

In the present paper, the problem of determining the optimal input signals of a system in the planning of a diagnostic experiment that ensure the distinguish ability of subschemes S_i, S_j is considered as the problem of obtaining the maximum distance between the regions of distribution of the values of $\rho_{i,i}$ and $\rho_{i,j}$.

In the theory of pattern recognition, the distance of the Mahalanobis is widely used as a measure of the distance between sets [7]. Assume that the distribution of values $\rho_{i,i}, \rho_{i,j}$, obey the normal laws $N(m_{i,i}, C_i), N(m_{i,j}, C_i)$, where $m_{i,i}, m_{i,j}$ – are the vectors of mathematical expectation, C_i – is the covariance matrix of dimension. In this case, the

generalized Mahalanobis distance between the regions of distribution $\rho_{i,i}$ and $\rho_{i,j}$ is determined by the expression

$$I_{i,j} = M_{i,j}^T C_i^{-1} M_{i,j}, \quad (13)$$

then $M_{i,j} = m_{i,i} - m_{i,j}$.

If the covariance matrix C_i – is a single matrix, then $I_{i,j}$ it characterizes the quadratic distance between the mathematical expectations $\rho_{i,i}$ and $\rho_{i,j}$.

For one-dimensional normally distributed sets of values $\rho_{i,i}$ and $\rho_{i,j}$, expression (13) takes the form

$$I_{i,j} = \frac{(m_{i,i} - m_{i,j})^2}{\beta_i}. \quad (14)$$

Since according to (11) $m_{i,i} = 0$, then (13), (14) can be written accordingly:

$$I_{i,j} = m_{i,j} C_i^{-1} m_{i,j}, \quad (15)$$

$$I_{i,j} = \frac{m_{i,j}^2}{\beta_i}. \quad (16)$$

For calculations using formulas (15), (16), it is necessary to know the value $m_{i,j}$, which, according to (12), depends on the unknown value $\Delta\rho_j$.

If $\Delta\rho_j$ – is a scalar, i.e. only one parameter in the system is allowed to change, the maximum value $I_{i,j}$ obtained for an arbitrary value $\Delta\rho_j \neq 0$ of for $u = u^0$ is the maximum (but different in magnitude) for any value $\Delta\rho_j$. It follows from this that the optimal input signals u^0 , at which the best distinguish ability of the subschemes S_i , S_j is achieved, can be determined before the diagnostic experiment at an arbitrary value $\Delta\rho_j$ by maximizing the value $I_{i,j}$.

If $\Delta\rho_j$ – is a vector, then it is impossible to obtain optimal values u^0 beforehand before the diagnostic experiment, delivering a maximum $I_{i,j}$ for any values $\Delta\rho_j$. This is due to the fact that the value $m_{i,j}$ depends on the combination of the values of the components of the vector $\Delta\rho_j$. In this case, the choice of input signals aimed at ensuring the distinguish ability of subschemes S_i , S_j can be carried out during the diagnostic experiment. Consider one of the variants of the experiment, consisting of two stages.

At the first stage, the estimates of the parameters of all subsystems are determined successively $\Delta\hat{\rho}_1, \dots, \Delta\hat{\rho}_N$. The input signals of the system at this stage are selected from the conditions of optimal experiment planning for identifying the parameters of the corresponding subsystem. Among the estimates obtained $\Delta\hat{\rho}_1, \dots, \Delta\hat{\rho}_N$, only one corresponds to the true values of the parameters of the faulty subsystem.

At the second stage, the optimal input signals of the system are determined, allowing selection of the obtained estimates $\Delta\hat{\rho}_1, \dots, \Delta\hat{\rho}_N$ under the appropriate hypothesis. In this case, the criterion of optimality under the hypothesis H_{ρ_i} is the maximum of the quantity

calculated by formula (13). In calculations according to formula (11), an estimate from $\Delta\hat{\rho}_1, \dots, \Delta\hat{\rho}_N$ the set corresponding to the subsystem is used, with respect to which the distinguishable subscheme S_i is distinguishable.

Use to test the hypothesis H_{ρ_i} of the magnitude of the bias of the estimate $\Delta\hat{\rho}_i$, determined by the expression (10), is possible only if for matrices $Q_{i,a}$, $Q_{i,b}$, there are minors of rank r_i . If for one of the matrices, for example $Q_{i,b}$, the matrix does not have a minor of rank r_i , then the reliability of the estimate $\Delta\hat{\rho}_i$ can be checked by the criterion of the forecast of the output signal of the system.

In this case, an estimate $\Delta\hat{\rho}_i = F_{i,a} Q_{i,a}^T \Delta\Lambda_a$ is determined from (7), and then, according to (10), the quantity $\Delta\hat{\Lambda}_b = Q_{i,b} \Delta\hat{\rho}_i$. Error forecast

$$\mu_i = \Delta\Lambda_b - \Delta\hat{\Lambda}_b, \quad (17)$$

is an indicator of the correctness of the hypothesis H_{ρ_i} . If $\mu_i < \varepsilon_i$ that hypothesis H_{ρ_i} is accepted, otherwise - it is rejected (ε_i – an acceptable value μ_i).

The value μ_i depends on which subsystem is actually faulty. If we consider subschemes S_i , S_j , then the mathematical expectation and variance of the quantities μ_i are determined by the expressions

$$E[\mu_i] = \begin{cases} \mu_{i,j} = Q_{i,b} F_{i,a} Q_{i,a}^T \Delta\rho_j, & \text{at } j \neq i, \\ \mu_{i,j} = 0, & \text{at } j = i, \end{cases} \quad (18)$$

$$\text{cov}[\mu_i] = \sigma^2 (1 + Q_{i,b}^T F_{i,a} Q_{i,b}), \quad (19)$$

where 1 – is the unit diagonal matrix.

The criterion of optimality of input signals for a hypothesis H_{ρ_i} oriented to the determination of a defective subschemes S_i , S_j in a pair can be the maximum of (15), where $m_{i,j}$ it should be put equal $\mu_{i,j}$, and $C_i = \text{cov}[\mu_i]$. Otherwise, for the criterion based on the expression (18), the reasoning given for the criterion based on the expression (10) can be repeated.

Planning a diagnostic experiment for structural faults. Let us consider subsystems with *independent observation*. When testing the hypothesis $H_i : \Delta y = L_i(u) \Delta Z_i$, $i = \overline{1, N}$ (where L_i – is the class of operators that specifies a class of faults in the subscheme S_i [1]), the compatibility of equations of the form is verified:

$$\Delta Y_a + \xi_a = L_{i,a} \Delta Z_i, \quad (20)$$

$$\Delta Y_b + \xi_b = L_{i,b} \Delta Z_i. \quad (21)$$

In this case ΔY_a , ΔY_b , as well ξ_a , ξ_b , are vectors whose dimensions are equal to or greater than the dimension of the vector ΔZ_i .

Let the decision on the reliability of the hypothesis H_i be made by the criterion of unbiasedness of the estimate $\Delta\hat{Z}_i$. Offsetting of the estimate $\Delta\hat{Z}_i$ is similar to (10) determined by the quantity

$$\tau_i = \Delta\hat{Z}_i^a - \Delta\hat{Z}_i^b. \quad (22)$$

If the matrix $L_{i,a}$ is rectangular and the method of least squares is used to obtain the estimate $\Delta\hat{Z}_i^a$ of the vector ΔZ_i from equation (20), then

$$E[\Delta\hat{Z}_i^a] = \begin{cases} \theta_{i,a} L_{i,a}^T L_{j,a} \Delta Z_j, & \text{at } j \neq i, \\ \Delta Z_i, & \text{at } j = i, \end{cases}$$

where $\theta_{i,a} = (L_{i,a}^T L_{i,a})^{-1}$.

The estimate $\Delta\hat{Z}_i^b$ of the vector ΔZ_i from equation (21) is determined in a similar way.

The value τ_i determined by the hypothesis H_i depends on which subscheme is actually faulty. Consider the case where only one of the subschemes S_i, S_j can be faulty. Analogously to (11), (12) we obtain

$$E[\tau_i] = \begin{cases} (\theta_{i,a} L_{i,a}^T L_{j,a} - \theta_{i,b} L_{i,b}^T L_{j,b}) \Delta Z_j, & \text{at } j \neq i, \\ \tau_{i,i} = 0, & \text{at } j = i, \end{cases} \quad (23)$$

$$\text{cov}[\tau] = \sigma^2 (\theta_{i,a} + \theta_{i,b}). \quad (24)$$

For the case when $\Delta Z_i, \Delta Z_j$ — are scalar quantities, that is, subschemes S_i, S_j , have one output, we get

$$E[\tau_i] = \begin{cases} \tau_{i,j} = \left(\frac{L_{j,a}}{L_{i,a}} - \frac{L_{j,b}}{L_{i,b}} \right) \Delta Z_j, & \text{at } j \neq i, \\ \tau_{i,i} = 0, & \text{at } j = i, \end{cases}$$

$$D[\tau_i] = \sigma^2 \left(\frac{1}{L_{i,a}^2} + \frac{1}{L_{i,b}^2} \right).$$

The principal difference between experiment planning and structural faults from planning for parametric faults $\Delta\rho_i$ is that for parametric faults the value does not depend on the input signals of the system, while for structural faults the value $\Delta\rho_i$ depends on the input signals of the system, in an unknown way.

Let the observability matrices $L_{i,a}, L_{i,\delta}, L_{j,a}, L_{j,\delta}$ — be constants and ΔZ_j — be a scalar quantity. In this case, when organizing a diagnostic experiment, two stages can be distinguished.

The first stage of the connection with the formation of observability matrices before the diagnostic experiment by means of an appropriate selection of control points. The choice of control points is carried out from the condition of maximum value (21), where $m_{i,j}$ it is replaced by $\tau_{i,j}$, and C_i by $\text{cov}[\tau_i]$. Since the maximum value $I_{i,j}$ obtained for the corresponding set of control points for arbitrary values $\Delta Z_j \neq 0$ remains the maximum (but

different in magnitude) for any values ΔZ_j , the choice of control points can be carried out at arbitrary values $\Delta Z_j \neq 0$.

The second stage is realized during the diagnostic experiment. Since the observability matrices are constant in this case, no increase in noise occurs when the input signals of the system change, which follows from (24). With a faulty subscheme S_j , we have $\Delta y_a = L_{j,a} \Delta Z_j$, $\Delta y_b = L_{j,b} \Delta Z_j$. In this case, the quantity $\tau_{i,j}$ in expression (23) corresponds to the quantity $\tau_{i,j}^* = \theta_{i,a} L_{i,a}^T \Delta y_a - \theta_{i,b} L_{i,b}^T \Delta y_b$.

The input signals of the system that ensure the best distinguish ability of the subschemes S_i , S_j under the hypothesis H_i are chosen in the second stage from the condition of the maximum of the quantity (21), where $m_{i,j}$ it is replaced by $\tau_{i,j}^*$, and C_i – by $\text{cov}[\tau_i]$.

When choosing control points, a table of coverings is usually constructed, the columns of which correspond to pairs of subsystems whose distinguishability is estimated, and the rows to checkpoints. At the intersection of a row and a column, there is one if some pair of subsystems are distinguishable by the introduction of the corresponding control point. The minimum set of control points corresponds to the minimum coverage of the table. There can be several minimal coverages, the choice of which is not formalized.

In some cases, for example, as described in this section, instead of one in the table of coverings, one can record the corresponding value of the Mahalanobis distance and from the minimal coverages choose a cover that provides a maximum, in some sense, distinguish ability of the subsystems. The criterion for choosing such a minimum coverage can be, in particular, the maximum value of the sum of all elements of the minimal coverage table.

If there is a limit on the number of channels of signal transmission from control points to the diagnostic system, the diagnostic system can be equipped with a diagnostic surveillance system. The diagnostic monitoring system is an adder whose inputs are connected to control points, and the output is to a communication channel. The weighting factors of the adder are chosen from the conditions for maximum discrimination of the subsystems on the basis of the Mahalanobis distance analysis for given ones.

Conclusion

For cases of parametric and structural faults obtained evaluation to test hypotheses about the distinctiveness of faulty subschemes in freewheeling systems. These estimates allow to identify faulty subscheme and plan their computational experiments based on the analysis of localization parameters subschemes diagnosable system to the test exposure. In this case, hypotheses are formulated from the assumption that the parameters of the diagnosed subscheme have changed. The localization of faulty system subschemes during the diagnostic experiment is carried out from the assumption of the distinguish ability of the subschemes, i.e. the partitioning of the system into subschemes must be carried out in such a way that the regions of distribution of the parameters of the subschemes do not intersect.

References

1. Верлань, А. Ф. Локализация неисправных фрагментов при диагностировании безынерционных систем / А. Ф. Верлань, С. А. Положаенко // *Електротехнічні та комп'ютерні системи: Теорія і практика. Спеціальний випуск. Астропрінт.* — 2017. — С. 439- 445.
2. Верлань, А. А. Декомпозиционный метод локализации неисправных электронных подсхем / А. А. Верлань, С. А. Положаенко, И. Х. Осман // *Электромашиностроение и*

3. Верлань, А. А. Формализация представления последовательности тестовых гипотез при диагностировании электронных схем / А. А. Верлань, Ю. Стертен, С. А. Положаенко // Информатика и математические методы в моделировании. — 2016. — Vol. 6, № 4. — Р. 315-321.
4. Положаенко, С. А. Локализация неисправных электронных подсхем методом обучающих и проверочных характеристик / С. А. Положаенко, А. А. Верлань, И. Х. Осман // Математичне та комп'ютерне моделювання. Серія: Технічні науки: зб. наук. пр. — Кам'янець-Подільський: Кам'янець-Подільськ. нац. ун-т, 2008. — Вип. 1. — С. 140-144.
5. Кулик, А. С. Диагностируемость линейных непрерывных систем / А. С. Кулик // Автоматика и телемеханика. — 1987. — № 6. — С. 148-155.
6. Круг, Г. К. Планирование эксперимента в задачах идентификации и экстраполяции / Г. К. Круг, Ю. А. Сосулин, В. А. Фатуев. — М.: Наука, 1997. — 208 с.
7. Ту, Дж. Принципы распознавания образов / Дж. Ту, Р. Гансалес. — М.: Мир, 1978. — 411 с.

ПЛАНУВАННЯ ДІАГНОСТИЧНОГО ЕКСПЕРИМЕНТУ ПРИ ЛОКАЛІЗАЦІЇ НЕСПРАВНОСТЕЙ ПІДСХЕМ БЕЗІНЕРЦІЙНИХ СИСТЕМ

С.А. Положаенко, Л.Л. Прокофьева

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: sanp277@gmail.com, prokofieva1957@gmail.com

Отримано формалізовані умови проведення діагностичного експерименту, пов'язаного з виявленням несправних фрагментів (підсхем) безінерційних систем. Діагностичний експеримент зведено при цьому до обчислювальних процедур локалізації несправних підсхем, в основу яких (процедур) покладено перевірку гіпотез про те, що змінилися характеристики виділених підсхем. Гіпотези формуються таким чином, щоб забезпечити виявлення параметричних та структурних несправностей. До перших, наприклад, можуть відноситися зміни опору ділянки ланцюга, а до других – обрив або коротке замикання. При розбитті системи на підсхеми, останні обираються за умови можливості їх параметричної ідентифікації. Тобто ситуації, коли по відомих параметрах інших підсхем, а також вхідних та вихідних сигналах системи в цілому, можна визначити параметри підсхеми, яка розглядається. Планування діагностичного експерименту полягає у наступному. Передбачаючи лінійну залежність між параметрами виділеної підсхеми S_i та вихідними сигналами системи, завчасно складається перевірна матриця F , яка визначає взаємозв'язок вказаних параметрів та сигналів, враховуючи справність підсхеми, що розглядається. При виникненні несправностей перевірна матриця F змінюється, що дозволяє визначити матрицю невідповідності q , на підставі аналізу якої можна отримати оцінку $\Delta \hat{\rho}_i$ параметрів $\Delta \rho_i$ підсхеми S_i , яка розглядається. В результаті даного аналізу робиться висновок щодо працездатності підсхеми S_i . Процедури перевірки гіпотез щодо справності підсхем без інерційної системи для випадків параметричних та структурних несправностей мають ідентичний характер. Принципова відмінність планування експериментів при структурних несправностях від планування при параметричних несправностях полягає у тому, що при параметричних несправностях величина $\Delta \rho_i$ не залежить від вхідних сигналів системи, а при структурних – величина $\Delta \rho_i$ залежить від вхідних сигналів системи, причому невідомим чином.

Ключові слова: діагностика, діагностичний експеримент, локалізація несправностей, безінерційні системи, оцінювання параметрів підсхем

ПЛАНИРОВАНИЕ ДИАГНОСТИЧЕСКОГО ЭКСПЕРИМЕНТА ПРИ ЛОКАЛИЗАЦИИ НЕИСПРАВНОСТЕЙ ПОДСХЕМ БЕЗЫНЕРЦИОННЫХ СИСТЕМ

С.А. Положаенко, Л.Л. Прокофьева

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: sanp277@gmail.com, prokofieva1957@gmail.com

Получены формализованные условия проведения диагностического эксперимента, связанного с выявлением неисправных фрагментов (подсхем) безынерционных систем. Диагностический эксперимент сводится при этом к вычислительным процедурам локализации неисправных подсхем, в основу которых (процедур) положена проверка гипотез о том, что изменились характеристики выделенных подсхем. Гипотезы формулируются таким образом, чтобы обеспечить выявление параметрических и структурных неисправностей. К первым, например, могут относиться изменение сопротивления участка цепи, а ко вторым – обрыв или короткое замыкание. При разбиении системы на подсхемы, последние выбираются из условия их параметрической идентифицируемости, т.е. ситуации, когда по известным параметрам остальных подсхем, а также входным и выходным сигналам в целом системы, можно определить параметры рассматриваемой подсхемы. Планирование диагностического эксперимента состоит в следующем. Предполагая линейную зависимость между параметрами выделенной подсхемы S_i и выходными сигналами системы, заранее составляется проверочная матрица F , определяющая взаимосвязь указанных параметров и сигналов, учитывая исправность рассматриваемой подсхемы. При возникновении неисправности проверочная матрица F изменяется, что позволяет определить матрицу несоответствия q , на основании анализа которой можно получить оценку $\Delta \hat{\rho}_i$ параметров $\Delta \rho_i$ рассматриваемой подсхемы S_i , в результате чего сделать заключение об ее исправности. Процедуры проверки гипотез об исправности подсхем безынерционной системы для случаев параметрических и структурных неисправностях имеют идентичный характер. Принципиальное отличие планирования эксперимента при структурных неисправностях от планирования при параметрических неисправностях состоит в том, что при параметрических неисправностях величина $\Delta \rho_i$ не зависит от входных сигналов системы, а при структурных – величина $\Delta \rho_i$ зависит от входных сигналов системы, причем неизвестным образом.

Ключевые слова: диагностика, диагностический эксперимент, локализация неисправностей, безынерционные системы, оценивание параметров подсхем

АНАЛІЗ ТА ПРОГНОЗУВАННЯ РИЗИКІВ ШАХРАЙСТВА З КРЕДИТНИМИ КАРТКАМИ

Н.В. Кузнєцова

Київський політехнічний інститут імені Ігоря Сікорського,
пр. Перемоги, 37, Київ, 03056, Україна; e-mail: natalia-kpi@ukr.net

У роботі досліджено основні підходи виявлення шахрайських операцій з кредитними картками та запропоновано комбіноване виконання поведінкового оцінювання клієнтів-власників кредитних карт та моніторингу операцій з кредитними картками з метою виявлення можливої спроби шахрайства. Було сформовано вхідну вибірку з 4 тисяч активних кредитних карт, за якими проводилось 55 тисяч транзакцій, класифіковано основні типи кредитних карт за їх поведінкою. За результатами проведеного дослідження поведінки клієнтів кредитних карток будується поведінкова модель, що описує, як вони будуть діяти в наступні моменти часу, які операції проводити, на яку суму та з якими лімітами, і таким чином дозволяє виявляти нетипові запити, що є свідченням спроби шахрайських операцій. Поряд зі стандартними характеристиками, що описують клієнта та кредитну карту, формувалися агреговані характеристики, які описували поведінку клієнта (баланс, доходи, витрати, ліміти) в динаміці, і за рахунок їх застосування вдалось отримати більш якісні моделі. При аналізі ризику шахрайських транзакцій використовувались операції за транзакціями за попередні періоди (типові та шахрайські), будувалися моделі на основі логістичної регресії, регресійного рівняння, регресії з інтегрованим ковзним середнім, а також застосовувались багатошаровий перцептрон та радіально-базисна функція. Такі моделі здійснювали класифікацію транзакції на предмет шахрайства, а далі прогнозували суму транзакції. Найкращим методом класифікації транзакцій виявився багатошаровий перцептрон, а найвищі значення точності прогнозу показала модель авторегресії з інтегрованим ковзним середнім (ARIMA) із значенням похибки 4.46% для прогнозування суми транзакції. Запропонований комбінований підхід виявився ефективним для аналізу та моніторингу кредитних карт та виявлення шахрайських операцій. Перспективним може бути його використання для інших типів фінансових ризиків (для білінгових та платіжних систем, систем переведення грошей та інших торгівельних операцій).

Ключові слова: ризики шахрайства, поведінковий скоринг, комбінований підхід, кредитні картки, моделі оцінювання ризиків, регресійні моделі

Вступ

Ризики шахрайських операцій з кредитними картками є одними з найбільш складно модельованих, оскільки характеризуються великою кількістю особливостей як самих операцій, транзакцій, які здійснюються, так і великою кількістю додаткових параметрів, які потребують урахування. Найчастіше моделюють ризики шахрайства, за якими доступні вже певні статистичні дані; цим займаються відділи моніторингу та протидії шахрайським операціям комерційних банків, трансфертних та білінгових систем, систем сплати послуг, перерахунку валют, платіжних систем тощо.

В Україні за даними Національного банку України у 2016 році було в обігу 31,1 млн. активних банківських карток (з 70 млн. виданих). Близько 5 млн. клієнтів мають негативну кредитну історію, яка пов'язана не тільки з шахрайством, а й з банкрутством неплатоспроможних банків. Ще донедавна вся відповідальність за можливі шахрайські операції з кредитними картками повністю лежала на плечах самих власників цих кредитних карток. Проте на вимогу найбільших світових платіжних систем (Visa,

Mastercard), які мають однакові правила обслуговування всіх клієнтів платіжних систем незалежно від країни, ця відповідальність була повністю перекладена на самі українські банки. І, якщо раніше моніторинг фінансових операцій здійснювався лише з точки зору використання в рамках ліміту, валюти та часу доби, то тепер набагато ретельніше перевіряються не лише великі операції, а й самі факти підняття ліміту.

Ризик шахрайських операцій з кредитними картками може розглядатися у декількох контекстах: підняття лімітів операцій, використання кредитних ліній з непогашеними заборгованостями, перевірка транзакцій за операціями – чи не є вони шахрайськими.

Метою даної роботи є аналіз існуючих методів та підходів до моделювання ризиків шахрайства та дослідження можливості застосування їх на реальних статистичних даних.

Для моделювання у роботі вирішувались завдання аналізу поведінки клієнтів з метою виявлення шахрайства з їх кредитними картками на прикладі українського банку, здійснювалось прогнозування шахрайської операції на основі вхідних характеристик для міжнародних кредитних карток.

Основна частина

Оцінювання ризиків банківської діяльності називають ще скорингом, оскільки при цьому розробляються скорингові моделі, за якими оцінюють власне клієнтів та кредити. Виділяють попередній скоринг, поведінковий скоринг, колекшн-скоринг, а також скоринг шахрайства [1,2].

Поведінковий скоринг (Behavioral scoring) – це динамічна оцінка стану кредитоспроможності існуючого позичальника, заснована на даних про історію операцій по його рахунках (графік погашення заборгованості, запити нових кредитів, оборот за поточними рахунками, і т. д.). Результатом поведінкового скорингу зазвичай є пропозиція банку скористатися іншими банківськими послугами: кредитна карта, кредит готівкою за зниженою процентною ставкою, автокредитування та ін. Схвалення наступних кредитів у банку для позичальника – це також результат успішного проведення поведінкового скорингу [1].

Скоринг шахрайства (Fraud scoring) – це вид скорингу, який надає статистичну оцінку ймовірності шахрайських дій з боку потенційного позичальника. Як правило, застосовується спільно з іншими видами дослідження клієнтів, такими як аплікаційний скоринг і поведінковий скоринг. Fraud-scoring використовується перш за все як певний бар'єр на шляху шахраїв при отриманні кредиту. Так, система в автоматичному режимі може порівнювати дані клієнтів з так званими «чорними» і «сірими» списками, робити запити в бюро кредитних історій і інші зовнішні бази даних. Ще одна функція fraud-scoring – перевірка наданих даних на протиріччя, причому як в рамках самої анкети, коли можуть порівнюватися відповіді на різні питання, так і через порівняння отриманих результатів з встановленими даними і статистикою (наприклад, про розміри доходів в різних галузях). Також цифри можуть порівнюватися з тими, які надали інші клієнти, з усередненими показниками по всьому портфелю кредитів банку [1].

Всі види скорингу обов'язково присутні у всіх банках на момент перевірки кредитних заявок, проте подальше дослідження і перевірка клієнтів, які вже користуються кредитними продуктами банку, і є доволі корисним, але було не дуже розповсюджено в українських банках. Зі зміною вимог Національного банку України до нормативів капіталу банку і забезпеченості кредитів ситуація дещо змінилась. Тепер все частіше банки перевіряють позичальників не лише на етапі обробки кредитних заявок, а й здійснюють відслідковування транзакцій з метою недопущення проведення шахрайських операцій, а також здійснюють поведінковий скоринг з метою забезпечити

лояльність клієнтів, вчасно збільшивши кредитні ліміти, або навпаки, заблокувавши кредитні карти, по яким проводяться підозрілі маніпуляції.

Для цього здійснюється відслідковування і класифікація позичальників за їх діями протягом певного періоду з кредитними лімітами, платежами, надходженнями тощо. Транзакція вважається шахрайською, якщо вона відрізняється від звичайної поведінки користувача. Це пов'язано з тим, що передбачається, що зловмисники будуть вести себе зовсім по-іншому, ніж власник облікового запису. Отже, спочатку необхідно напрацювати і виявити модель поведінки користувача кредитної карти, а потім вже виявляти шахрайство [3]. Іншим варіантом є класифікація самих транзакцій з метою виявлення, чи є вони нормальними (типовими), чи є шахрайськими. Для вирішення цієї задачі можуть використовуватись методи дерев рішень, нейронні мережі, правила виведення тощо [4,5].

Важливо підкреслити ключові відмінності між аналізом поведінки користувачів та підходами щодо аналізу шахрайства. Метод аналізу шахрайства дозволяє виявити відомі шахрайські хитрощі з низьким хибним позитивним рівнем. Проте, оскільки доля випадків шахрайських заявок є зазвичай доволі низькою, то сам класифікатор базується на обмежених записах про шахрайство і не може виявити нові фальсифікації. В результаті, пропуски шахрайства при класифікації можуть бути надзвичайно високими залежно від того, наскільки винахідливими є шахраї. Аналіз поведінки користувачів в цьому випадку справляється набагато краще з виявленням нових фальсифікацій. Будь-яка діяльність, яка суттєво відрізняється від моделі, буде розглядатися як можливе шахрайство.

Системи виявлення шахрайства також стикаються з певними труднощами та обмеженнями: незбалансовані дані, різне значення неправильної класифікації, відсутність адаптивності, тощо [3]. Незбалансованість даних пов'язана з невеликою кількістю шахрайських операцій в загальній вибірці. Різна вартість помилкового виявлення пов'язана з втратами. Так, шахрайська операція сприйнята як нормальна призведе до втрат, рівних сумі транзакції. Проте, якщо система сприймає нормальну транзакцію як шахрайську операцію і відхиляє її, то це призводить до незначних втрат, пов'язаних, наприклад, з уточненням і додатковою аутентифікацією клієнта. Відсутність адаптивності передбачає, що класифікаційні алгоритми, як правило, стикаються з проблемою появи та, відповідно, складнощами виявлення нових типів звичайних чи шахрайських зразків.

Далі ми виконаємо аналіз кредитних карток та порівняємо обидва підходи з точки зору поведінкового скорингу та виявлення шахрайства.

Аналіз поведінки клієнтів-власників кредитних карток з точки зору використання лімітів. Для аналізу поведінки клієнтів були використані реальні дані українського банку за кредитними картами, виданими у 2013-2015 роках. Були відібрані спостереження за 4 тисячами активних кредитних карт, які проводили різні транзакції. Загальна кількість транзакцій складає 55 тисяч записів. Наявні такі поведінкові параметри: залишок за тілом кредиту, залишок за комісією/відсотками, прострочена заборгованість за тілом, прострочена заборгованість за комісією/відсотками, кількість днів прострочки за тілом, тощо. Аплікаційні дані: тип клієнта, вік, рік видачі, тривалість угоди, ліміт на початку, сума при подачі заявки, ознака рівності ліміту та суми, адреса прописки, адреса місця постійного проживання, кількість дітей, і т.п. Агреговані дані: максимальна кількість прострочених місяців, середнє значення щомісячного зняття, максимальне значення відношення простроченої заборгованості до встановленого ліміту, і т.п.

У результаті попереднього аналізу можна виділити декілька типових кредитних карт: кредитні карти, що безперервно погашають заборгованості та картки, що перейшли в дефолт (за міжнародною практикою, коли кредитна заборгованість перевищує 90 днів). Для більшості недефолтних кредитних карт все ж спостерігалися

прострочені платежі протягом невеликого періоду в межах 1-7 днів. Тут можна виділити додаткову класифікацію: з постійним лімітом, зменшенням та збільшенням ліміту. Спільною рисою для цих трьох випадків є відносно постійний темп платежів, що залежить від величини ліміту та/або заборгованості. Разом з тим зняття з кредитної карти є певною випадковою величиною із очевидним математичним сподіванням, а структура в послідовності прострочених платежів взагалі не спостерігається. Також серед користувачів можна виділити тих, що залишали баланс кредитних карт на високому рівні та тих, що намагалися звести баланс до нуля якнайшвидше. Приклад кредитної карти без заборгованостей, проте зі збільшенням кредитного ліміту наведено на рис. 1.

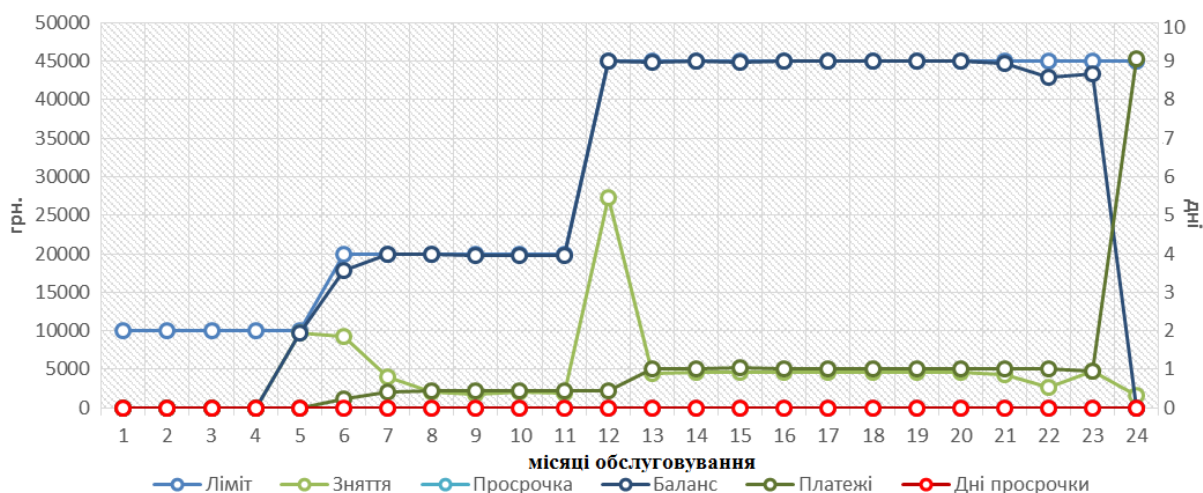


Рис. 1. Приклад кредитної карти без прострочених платежів (зі збільшення ліміту)

Приклад карти другого типу зі зведенням до мінімуму балансу наведено на рис. 2. Окремо можна виділити випадки простроченої комісії при нульовому балансі на карті, які не вважаються дефолтними, проте також є доволі типовими для клієнтів.

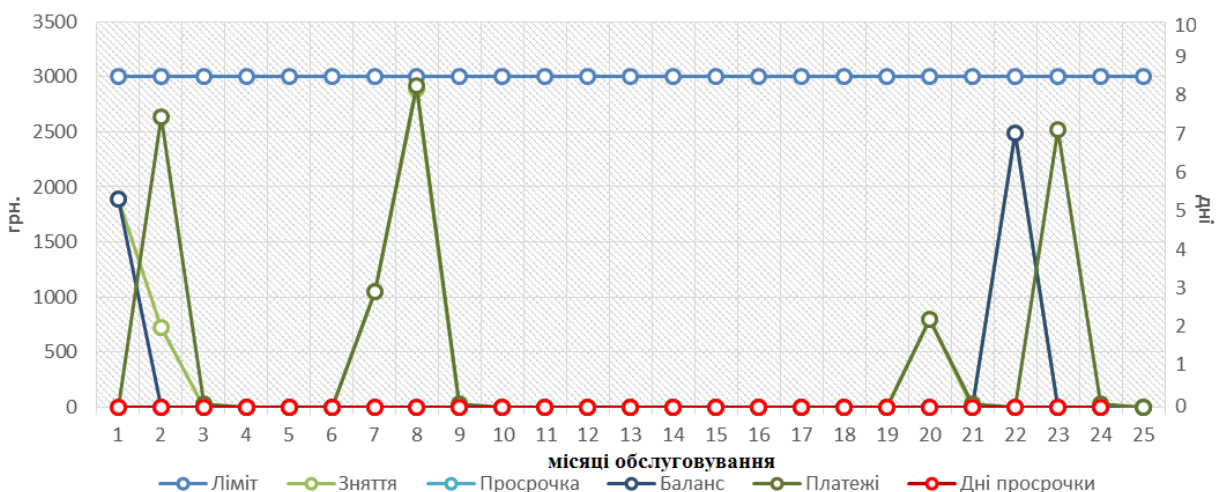


Рис. 2. Кредитна карта другого типу

Наступним варіантом є так звані дефолтні картки, які мають заборгованість більш ніж 3 місяці, і можуть характеризуватися постійним, збільшеним або навіть зменшеним кредитним лімітом. Для таких клієнтів необхідно виявити факт дефолту і заблокувати можливість використання кредитного ліміту в наступному місяці, щоб зменшити фінансові втрати банку.

Згідно з описаним критерієм кредитна карта на рис. 3 переходить у стан дефолту на 21-му місяці свого життя, при цьому довгий період власник карти був взірцем, дотримувався графіку виплат досить тривалий час.

Однак бувають випадки, коли кредитна карта переходить у заборгованість і прострочку, проте потім клієнт успішно покриває заборгованість та закриває карту.

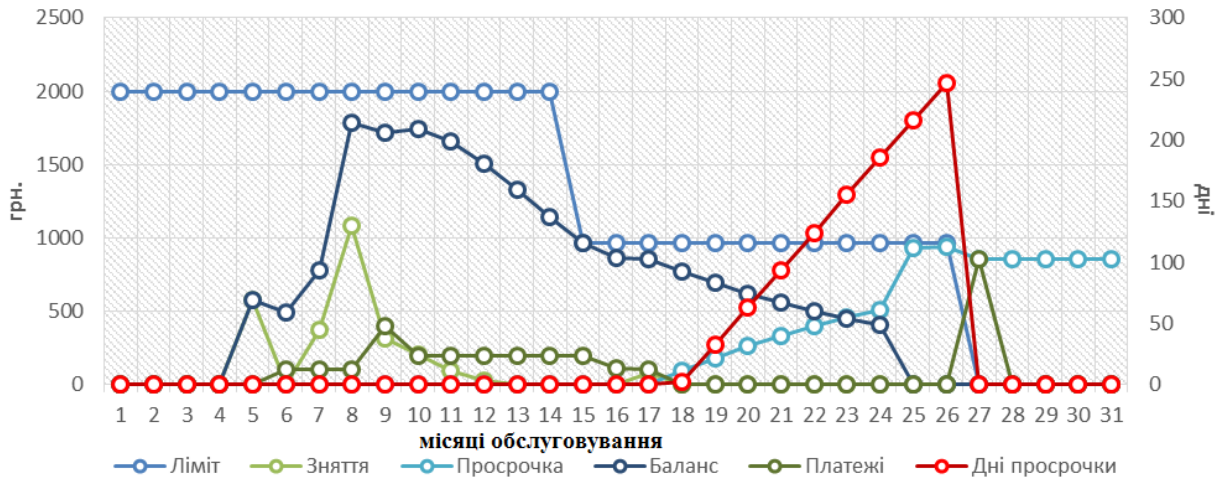


Рис. 3. Приклад дефолтної кредитної карти зі зменшення ліміту

За такими критеріями були відібрані і сформовані види поведінки клієнтів, і тепер можна безпосередньо виявляти атипову або шахрайську поведінку, яка суттєво відрізняється від описаної вище. Перейдемо до наступного етапу виявлення шахрайських операцій за кредитними картками.

Прогнозування шахрайської операції за кредитними картками

Вхідні дані: Набір даних містить єврооблігаційні транзакції, зроблені кредитними картками у вересні 2013 року. Набір даних дуже незбалансований, шахрайство становить 0.172% всіх транзакцій. Набір даних містить тільки числові вхідні змінні. Змінні V1, V2, ..., V29 є основними компонентами, отриманими за допомогою методу головних компонент, а єдиною неперетвореною функцією є «Час». Функція «Час» містить секунди, що минули між кожною транзакцією і першої транзакцією в наборі даних. Функція «Сума» – це сума транзакції, яка виступає в якості цільової змінної, наприклад, для навчання з урахуванням витрат. Функція «Клас» – є цільовою змінною відповіді, і вона приймає значення «1» в разі шахрайства, «0» – в іншому випадку.

1 Етап. Задача виявлення хибної транзакції є задачею класифікації, а тому доцільно перевіряти точність за основі індексу GINI та області під кривою точності (AUC). Для того, щоб визначити важливі змінні, які мають бути включені до аналізу, здійснюємо попередній аналіз змінних-характеристик [1]. В ідеалі ми маємо сформувати вибірку таким чином, щоб отримати збалансовані розподіли за кожною змінною класу. Графіки на рис. 4 показують, наскільки різноманітні обидва класи щодо кожного розподілу змінних. Тільки V13, V15, V22, V23, V24, V25 і V26 можна розглядати як беззмстовні змінні, а всі інші змінні – потенційно корисні змінні. Проте, на початковому етапі використаємо всі змінні для побудови класифікатора.

Для цього побудуємо логістичну регресію [6] в середовищі R як класифікатор з двома виходами (0 та 1) за допомогою вбудованої функції evalmod із пакету прегрес. Кількісну інтерпретацію ROC дає показник AUC – площа, обмежена ROC-кривою і віссю частки помилкових позитивних класифікацій. Чим вище показник AUC, тим якісніше класифікатор. В нашому випадку значення дорівнює 0.7589, тому дані та такий класифікатор можна використовувати для прогнозування суми по транзакціях.

2 Етап. Прогнозування суми транзакції з метою виявлення шахрайської операції.

Моделювання здійснювалось за допомогою пакету SPSS Statistic, налаштовуючи вихідну змінну (цільову або Target) як змінну V30 – загальна сума по транзакціям.

Прогнозування суми транзакції було виконано різними методами за допомогою регресійної моделі, нейронних мереж, тощо.

Було побудовано кілька різних моделей авторегресії, авторегресії з ковзним середнім, інтегрованої авторегресії з ковзним середнім. Для кожної з обраних моделей були побудовані статистичні критерії якості та таблиці залишків. Найкращі значення показала модель ARIMA ($R^2 = 0.987$, $BIC = 6.343$).

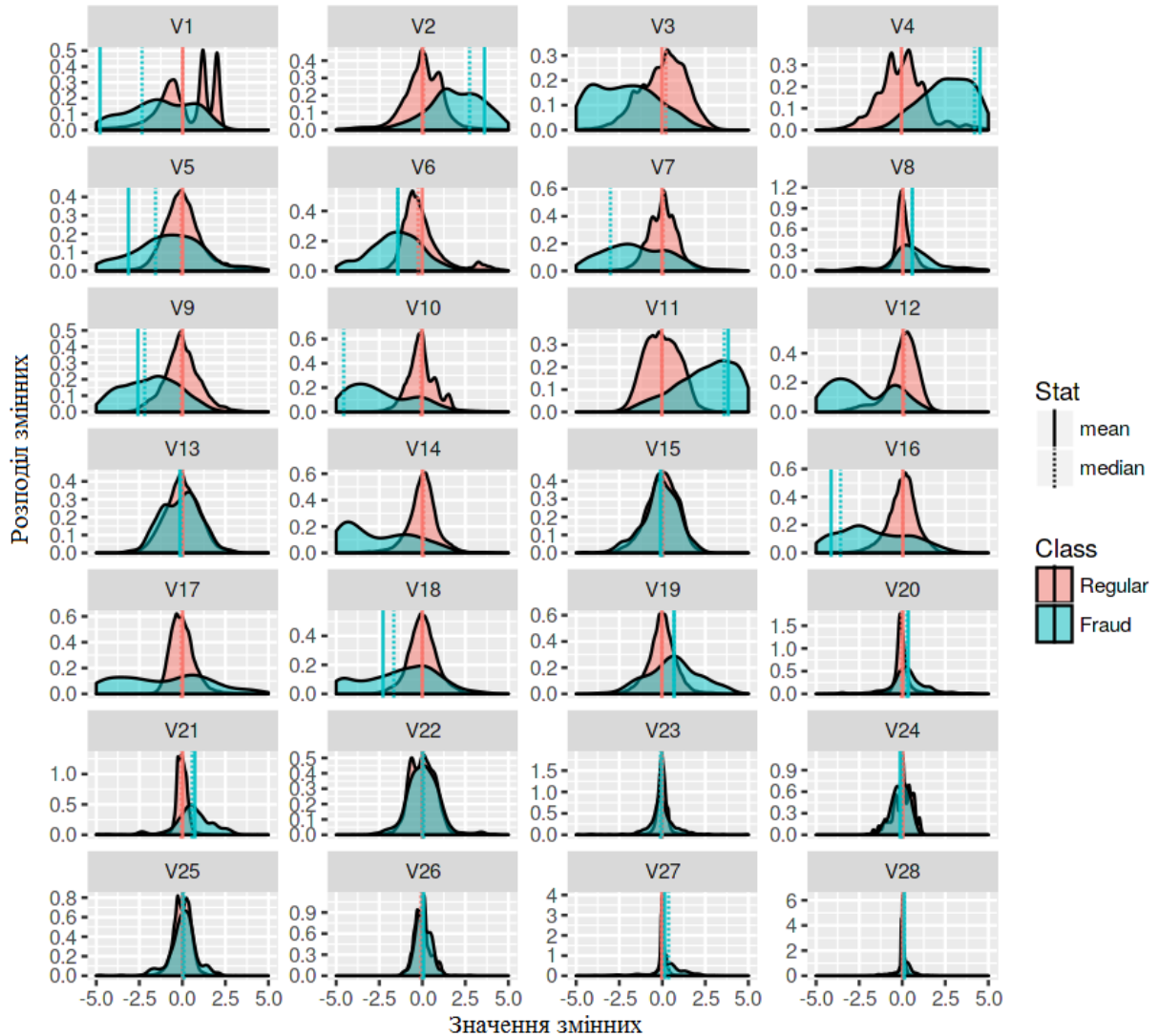


Рис. 4. Попередній аналіз вхідних характеристик

Для оцінювання якості побудови моделі та прогнозу застосовують критерії[7]:

1. Середня відсоткова похибка:
$$MPE = \frac{1}{N} \sum_{i=1}^N \frac{(y_i - \hat{y}_i)}{y_i} \times 100\%.$$
2. Середня відсоткова абсолютна похибка:
$$MAPE = \frac{1}{N} \sum_{i=1}^N \frac{|y_i - \hat{y}_i|}{|y_i|} \times 100\%.$$
3. Середня похибка:
$$ME = \frac{1}{N} \sum_{i=1}^N (y_i - \hat{y}_i).$$

4. Середня абсолютна похибка: $MAE = \frac{1}{N} \sum_{i=1}^N |y_i - \hat{y}_i|$.

5. Середньоквадратична похибка (Standard Error або RMSE – root mean square error): $SE = \sqrt{\frac{1}{N} \sum_{i=1}^T (y_i - \hat{y}_i)^2}$.

6. Середньоквадратична похибка (MSE – mean square error):

$$MSE = E((y - \hat{y})^2) = \frac{\sum_{i=1}^N (y_i - \hat{y}_i)^2}{N}.$$

7. Сума квадратів похибок: $\sum_{k=1}^N e^2(k) = \sum_{k=1}^N [\hat{y}(k) - y(k)]^2 \rightarrow \min_{\hat{\theta}}$.

Для моделі ARIMA були отримані наступні значення: $MAPE = 4.4469\%$, $MAE = 2.81$, $MSE = 7.89$, $SE = 62.24$.

Далі здійснювалась побудова регресійної моделі і були отримані такі показники якості моделі отримали такі: $R^2 = 0.996$, $R_{adj}^2 = 0.991$.

Надалі було здійснено побудову багатошарового перцептрону, де користувач може самостійно налаштувати мережу, вказавши кількість нейронів, прихованих шарів, тощо, для досягнення вищого результату (рис. 5).

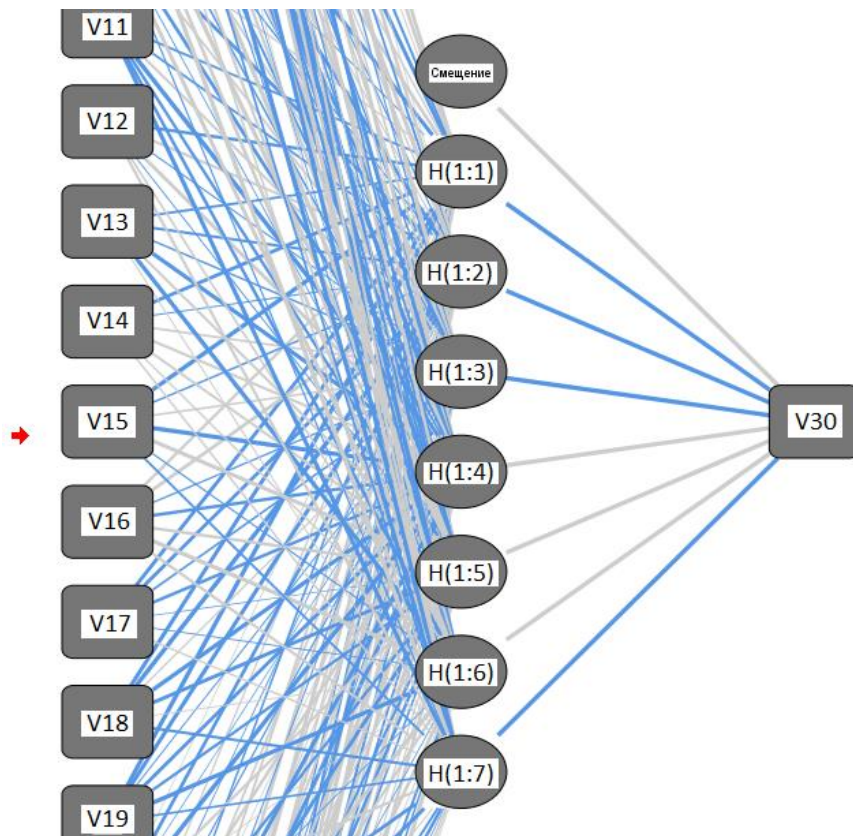


Рис. 5. Нейронна мережа із цільовою змінною

Вибірку було розділено на навчальну та перевірочну, здійснено оцінку суми квадратів похибок та відносної похибки, $ME = 0.06$ та $RMSE = 5.151$.

Також було здійснено моделювання на основі радіально-базисної функції (РБФ). Для налаштування функції було визначено 2 вхідних нейрона, функція активація для

прихованого шару Softmax, кількість нейронів, параметри моделі та прогнозу, додаткові графіки, тощо.

Зведені характеристики якості прогнозу на навчальній та перевіірочній вибірці наведено у таблиці 1.

Таблиця 1.

Зведена таблиця похибок прогнозу за всіма моделями

Відносна похибка	Навчальна вибірка	Перевіірочна вибірка
APIMA	0.987	0.044
Регресійне рівняння	0.1757	0.991
Багатошаровий перцептрон	0.148	0.060
Радіально-базисна функція	0.439	0.931

Таким чином, найкращою моделлю виявився багатошаровий перцептрон, за ним був побудований прогноз з доволі якісними показниками. Найкращою за значенням прогнозу виявилась модель APIMA із значення похибки 4.46%. Найгірше значення було отримано при застосуванні регресійної моделі.

Можна сказати, що якщо використовувати багатошаровий перцептрон або модель APIMA, то в нас буде найвище, найточніше значення прогнозу, тобто оптимістичний сценарій для 20% перевіірочної вибірки. Якщо ми будемо використовувати РБФ, то отримаємо базовий сценарій для результативних значень. Якщо ми будемо використовувати регресійну модель, то отримаємо значення прогнозу, які дуже сильно, з великою похибкою, будуть відрізнятися від реальних. В даному випадку ми будемо мати песимістичний прогноз і великий ризик того, що частина грошей буде загублена або отримана шахраями.

Повертаючись до початкових розподілених класів (де 0 – все добре, 1 – шахрайство), при застосуванні APIMA та багатошарового перцептрону ймовірність шахрайства буде мінімальною, при РБФ – середньою, а при регресії – найбільшою.

Висновки

Задача виявлення шахрайства є однією з найактуальніших у банківському та фінансовому секторі. Саме ризики шахрайства важко структурувати та формалізувати, а тому потрібні нові комбіновані підходи та методи. У роботі використано системний підхід до опрацювання ризиків шахрайства з кредитними картками, який передбачає комбінацію поведінкового оцінювання та виявлення шахрайства за транзакціями. Такий підхід із застосуванням аналізу поведінки власника кредитної карти дозволяє виявити спробу шахрайської операції ще на етапі її виникнення, а подальше застосування методів регресійного аналізу, нейронних мереж дозволяє спрогнозувати ймовірність такої операції. Це дозволяє також збалансувати вхідні дані, отримавши агреговані дані по заборгованостям, часу обслуговування, кількості днів прострочки кредитного ліміту, тощо, та отримати більш точні оцінки прогнозу. Наступним етапом для прогнозування ризиків шахрайства є прогнозування суми операції, оскільки всі засоби запобігання шахрайству також розподілені в залежності від суми операції, а прогнозування шахрайської операції на суму 1 грн. та запобігання їй є недоцільним. Проте сам факт виявлення такої шахрайської операції є важливим сигналом про можливу спробу подальших транзакцій та є сигналом для відслідковування таких кредитних карт.

Перспективним є подальше дослідження ризиків шахрайських операцій та розширення класу задач прогнозування, з використанням комбінації поведінкового скорингу та моніторингу шахрайських операцій, на торгівельні операції, платіжні

системи, системи перерахування грошей з точки зору виявлення типових та нетипових операцій та блокування можливих шахрайських дій.

Список літератури

1. Siddiqi, N. Credit Risk Scorecards: Developing and Implementing Intelligent Credit Scoring / N. Siddiqi // John Wiley & Sons, Hoboken. — 2005. — 208 p.
2. Kuznietsova, N.V. Scoring Technology for Risk Assessment of Fraud in Banking / Selected Papers of the XVI International Scientific and Practical Conference "Information Technologies and Security" (ITS 2016). — 2016. — Pp. 54-61.
3. Sorournejad, S. A Survey of Credit Card Fraud Detection Techniques: Data and Technique Oriented Perspective / S. Sorournejad, Z. Zojaji, R.E. Atani, Amir Hassan Monadjemi / Cornell University Library, 2016. Mode of access: <https://arxiv.org/ftp/arxiv/papers/1611/1611.06439.pdf>.
4. Воронцов, К. Математические методы обучения по прецедентам. Курс лекций / К. Воронцов. — М: МФТИ, 2006. — 58 с.
5. Чубукова, И. А. Data Mining / Чубукова И. А. — М.: Бином ЛБЗ, 2008. — 384 с.
6. Beninel, F. Transfer Learning Using Logistic Regression in Credit Scoring / F. Beninel, W. Bouaguel, G. Belmufti / Cornell University Library, 2012. Mode of access: <https://arxiv.org/pdf/1212.6167.pdf>.
7. Бідюк, П.І. Аналіз часових рядів: навч. Посіб / П.І. Бідюк, В.Д. Романенко, О.Л. Тимошук. — К.: НТУУ «КПІ», 2013. — 600 с.

АНАЛИЗ И ПРОГНОЗИРОВАНИЕ РИСКОВ МОШЕННИЧЕСТВА С КРЕДИТНЫМИ КАРТОЧКАМИ

Н.В. Кузнецова

Киевский политехнический институт имени Игоря Сикорского,
пр. Победы, 37, Киев, 03056, Украина; e-mail: natalia-kpi@ukr.net

В работе исследованы основные подходы к выявлению мошеннических операций с кредитными карточками и предложено комбинированное исполнение поведенческого оценивания клиентов-владельцев кредитных карт и мониторинга операций по кредитным картам с целью выявления возможной попытки мошенничества. Была сформирована входная выборка из 4 тысяч активных кредитных карт, по которым проводилось 55 тысяч транзакций, классифицированы основные типы кредитных карт по их поведению. По результатам проведенного исследования поведения клиентов кредитных карточек строится поведенческая модель, описывающая, как они будут действовать в последующие моменты времени, какие операции проводить, на какую сумму и с какими лимитами, и таким образом позволяющая выявлять нетипичные запросы, которые свидетельствуют о попытках мошеннических операций. Наряду со стандартными характеристиками, описывающими клиента и кредитную карту, формировались агрегированные характеристики, описывающие поведение клиента (баланс, доходы, расходы, лимиты) в динамике, и за счет их использования удавалось получить более качественные модели. При анализе риска мошеннических транзакций использовались операции по транзакциям за предыдущие периоды (типичные и мошеннические), строились модели на основе логистической регрессии, регрессионного уравнения, регрессии с интегрированным скользящим средним, а также применялись многослойный персептрон и радиально-базисная функция. Такие модели осуществляли классификацию транзакции на предмет мошенничества, а дальше прогнозировали сумму транзакции. Лучшим методом классификации транзакций оказался многослойный персептрон, а высокие значения точности прогноза показала модель авторегрессии с интегрированным скользящим средним (ARIMA) со значением погрешности 4.46% для прогнозирования суммы транзакции. Предложенный комбинированный подход оказался эффективным для анализа и мониторинга кредитных карт и выявления мошеннических операций, и перспективным может быть его использование для других типов финансовых рисков (для биллинговых и платежных систем, систем перевода денег и других торговых операций).

Ключевые слова: риски мошенничества, поведенческий скоринг, комбинированный подход, кредитные карточки, модели оценки рисков, регрессионные модели

ANALYSIS AND FORECASTING OF CREDIT CARDS' FRAUD RISKS

N.V. Kuznietsova

Igor Sikorsky Kyiv Polytechnic Institute,
37, Peremohy Ave., Kyiv, 03056, Ukraine; e-mail: natalia-kpi@ukr.net

The paper investigates the main approaches for detecting fraudulent operations with credit cards and proposes a combined implementation of behavioral assessment of credit card holders and credit card transactions in order to detect possible fraud attempts. An incoming sample of 4,000 active credit cards was generated, for which 55 thousand transactions were carried out, the main types of credit cards were distinguished by their behavior. According to the results of a study on the behavior of credit card clients, a behavioral model was built. It describes how they will act at the next moments, what transactions carry out, of what amount and with what limits, and thereby non-typical queries could be identified that are evidence of fraudulent attempts. Along with the standard characteristics describing the client and credit card, aggregated characteristics were formed for client's behavior describing (balance, income, expenses, limits) in dynamics and due to this managed to obtain more qualitative models. In analyzing the risk of fraudulent transactions, transaction transactions for previous periods (typical and fraudulent) were used, models based on logistic regression, regression equation, regression with integrated slip medium, and also a multi-layer perceptron and radial-basic function were used. Such models carried out the classification of the transaction for fraud, and then predicted the amount of the transaction. The best method of classification of transactions was a multilayer perceptron, and the highest accuracy values of the forecast showed autoregression integrated moving average (ARIMA) model with an error value of 4.46% for forecasting transaction amount. The proposed combined approach proved to be quite effective in analyzing and monitoring of credit cards and detecting fraudulent transactions, and it could be implemented on other types of financial risks (for billing and payment systems, money transfer systems and other trading operations).

Keywords: fraud risks, behavioral scoring, credit cards, combined approach, risk assessment models, regression models

УДОСКОНАЛЕННЯ МЕТОДУ ВІДОКРЕМЛЕННЯ КЛОНУ ВІД ПРООБРАЗУ В ЦИФРОВОМУ ЗОБРАЖЕННІ

І.І. Бобок, А.А. Кобозєва

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

Клонування залишається на сьогоднішній день одним з найбільш широко й часто використовуваних при фальсифікаціях цифрових зображень (ЦЗ) програмних інструментів. Розв'язанню задачі виявлення результатів клонування приділяється багато уваги, однак питання визначення, яка з виявлених попередньо областей ЦЗ є клоном, а яка прообразом, залишається актуальним. У роботі запропоноване вдосконалення методу відокремлення клону від прообразу, розробленого авторами раніше, ефективного в умовах відсутності будь-якої обробки клонованого ЦЗ. Метою вдосконалення є підвищення інформативності результатів виявлення клонування в ЦЗ шляхом забезпечення ефективної роботи відповідного методу в умовах додаткових збурних дій, зокрема, в умовах стиску з втратами клонованого зображення. Удосконалення методу забезпечується за рахунок виявлення й фіксації моменту стрибка значення модуля різниці норм відмітних околіїв відповідних блоків клону й прообразу, який має місце при досягненні цими блоками границь реальних областей клону й прообразу. У момент фіксації стрибка клону відповідає блок, норма відмітного околу якого більше. Процес фіксації стрибка відбувається для декількох (максимально 8) пар відповідних блоків, що виходять на границі клону й прообразу. Остаточний висновок робиться з врахуванням того, яка з виявлених областей визначалася як клон/прообраз більшу кількість разів. Результати проведеного обчислювального експерименту говорять про ефективність алгоритмічної реалізації запропонованого методу в умовах наявності додаткових збурних дій на клоноване ЦЗ.

Ключові слова: клонування, цифрове зображення, відокремлення клону від прообразу, відмітний окіл блоку, додаткові збурні дії

Вступ

Специфікою сьогоднішнього дня з урахуванням високого рівня розвитку інформаційних технологій є повсюдне використання цифрових інформаційних контентів. Якщо ці контенти використовуються з нерозважальною метою, надзвичайно важливою є умова збереження їх цілісності. Існує велика кількість сучасних наукових робіт, присвячених розробці методів виявлення порушень цілісності цифрових контентів, зокрема зображень (ЦЗ), яким присвячена дана стаття, заснованих на різних математичних підходах, з використанням різних технологій [1-3]. Дуже велика увага приділяється процесу виявлення результатів одного з найбільш широко й часто використовуваних при фальсифікаціях ЦЗ програмних інструментів - виявленню клонування, яке реалізовано у всіх сучасних графічних редакторах [4-7]. Тут отримані значимі результати, що дозволяють виявляти клони/прообрази в умовах додаткових збурних дій, у тому числі значних [6,7], клони/прообрази малих абсолютних, відносних розмірів [6] і т.д. Однак до цього моменту не отримала бажаного розвитку проблема відокремлення клону від прообразу, тобто визначення, яка саме з виявлених областей є клоном, а яка прообразом, розв'язок якої дозволить підвищити інформативність результатів зробленої експертизи. Існуючі підходи, що використовуються для розв'язання цієї задачі, різні. Основними з них є: використання технології цифрових

водяних знаків [8] (вбудова яких у ЦЗ сама по собі порушує його цілісність, що є небажаним), пошук результатів постобробки клону [9], яка відрізняється від обробки прообразу (але у випадку клону/прообразу малих розмірів постобробка клону часто відсутня, що робить методи цієї групи тут недієздатними). В [10] був запропонований метод відокремлення клону від прообразу в умовах відсутності обробки клонованого ЦЗ. І хоча умови, у яких вирішується ця задача (відсутність будь-якої постобробки), забезпечують її максимальну складність, на практиці, у випадку, якщо розміри клону/прообразу не можна назвати малими, без обробки клонованого ЦЗ, як правило, не обходяться: після клонування ЦЗ зазнає додаткових збурних дій, які змінюють елементи його матриці. Зокрема, враховуючи сучасні обсяги цифрової інформації, що пересилається по каналах зв'язку, ЦЗ буде збережено у форматі з втратами, що не приверне до його постобробки додаткової уваги, не вплине на візуальне сприйняття, але при цьому внесе зміни в матрицю, ускладнюючи процес виявлення клону й прообразу. У силу цього основна увага в даній роботі приділяється забезпеченню працездатності методу відокремлення клону від прообразу, що пропонується, в умовах стиску клонованого зображення з втратами. Для визначеності, не обмежуючи спільність міркувань, скрізь нижче як формат з втратами використовується формат Jpeg.

Мета статті й постановка досліджень

Метою статті є підвищення інформативності результатів виявлення клонування в ЦЗ шляхом удосконалення методу відокремлення клону від прообразу, запропонованого [10], яке забезпечує його ефективну роботу в умовах додаткових збурних дій на клоноване зображення.

Для досягнення мети в роботі вирішуються наступні *задачі*:

1. Визначити умову виходу відповідних блоків клону й прообразу, що належать їхнім внутрішностям, за межі реальних областей клону й прообразу з врахуванням постобробки клонованого ЦЗ;
2. Визначити величину відмінності норм відмітних околів відповідних блоків клону й прообразу у випадку, коли відмітні околи містять у собі інформацію про блоки, що мають непусте перетинання з областю ЦЗ, що відрізняється від клону/прообразу.

Основна частина

Основними об'єктами аналізу в методі відокремлення клону від прообразу в ЦЗ, запропонованому в [10], є відмітні околи відповідних блоків клону й прообразу, виявлених попереду.

Поняття відмітного околу 1×1 -блоку B ЦЗ радіуса k введено авторами раніше в [11]. Відмітний окіл представляє з себе $(2k+1) \times (2k+1)$ -матрицю, елементи якої відображають відмінність B від блоків ЦЗ, що знаходяться від B на відстані, що не перевищує k . При цьому сусідами блоку B , що знаходяться від нього на відстані k , називаються блоки ЦЗ, місце розташування яких отримується шляхом зсуву B на k пікселів вправо, вліво, вгору, вниз, вздовж головної й побічної діагоналей (вгору, вниз). Відмінність між будь-якими 1×1 -блоками $B^{(1)}, B^{(2)}$ ЦЗ визначається наступним чином:

$$\sum_{t,p=1}^l r_{tp}, \quad (1)$$

де r_{ip} , t , $p = \overline{1, l}$, — елементи $l \times l$ – матриці $R = |B^{(1)} - B^{(2)}|$, де останнє співвідношення розуміється в поелементному сенсі.

Очевидно, що при відсутності додаткових збурних дій на клоноване ЦЗ норми відмітних околів відповідних блоків клону й прообразу не будуть відрізнятися у випадку, коли ці блоки належать внутрішностям [10] клону й прообразу відповідно, а їх відмінність буде сигналізувати про вихід за межі внутрішностей реальних областей клону й прообразу розглянутою парою відповідних блоків з наступним визначенням області клону як такої, якій належить блок, норма відмітного околу якого більша. Таким чином, у випадку відсутності додаткових збурних дій на клоноване ЦЗ є явний «показчик» на блок клону. Якщо ж клоноване ЦЗ піддавалося постобробці, то норми відмітних околів відповідних блоків клону й прообразу будуть відрізнятися навіть у тому випадку, якщо вони точно належать внутрішностям клону й прообразу. Ці відмінності будуть результатом додаткових збурних дій на ЦЗ, не будучи інформативними з погляду розв'язуваної задачі відокремлення клону від прообразу. Вихід за межі реальних клону й прообразу тут не буде таким очевидним, як в умовах роботи методу, розробленого в [10].

Пропонується вдосконалення існуючого методу, засноване на наступних міркуваннях, метою якого є забезпечення його ефективної роботи в умовах постобробки клонованого ЦЗ. У межах внутрішностей областей клону й прообразу норми відмітних околів відповідних блоків повинні відрізнятися друг від друга менше, ніж у випадку, коли відбудеться вихід відмітних околів за межі реальних клону й прообразу, до того ж в межах внутрішностей клону й прообразу співвідношення між нормами відмітних околів (яка з них більше) не носить інформативного характеру, тому що відмінність між цими нормами визначається тільки наявністю додаткової збурної дії. При виході за межі внутрішностей клону й прообразу повинен відбутися кількісний стрибок у збільшенні величини відмінності між нормами відмітних околів, і тут вже показовим є порівняння норм околів: блоку клону повинен відповідати відмітний окіл, норма якого більше [11]. Невиконання цього твердження може мати місце в силу наступних причин. Одним з джерел висновку [10,11] про те, що норма відмітного околу блоку-клону повинна бути більше норми відмітного околу відповідного блоку-прообразу в момент виходу за межі реальних клону й прообразу, є наявність значної кореляції між значеннями яскравості пікселів-сусідів [11,12], яка «розривається» для граничних пікселів області клону. Відмітні околи відповідних блоків клону й прообразу в умовах додаткових збурних дій «несуть у собі інформацію» не тільки про відмінності в сенсі (1) конкретного блоку (клонованого ЦЗ) від його найближчих сусідів, але й про саму збурну дію, зокрема, про силу цієї дії. Чим сильніша збурна дія, що накладається на клоноване ЦЗ, тим сильніше змінюються значення яскравості його пікселів (незалежно від того, належать ці пікселі границі прообразу або границі клону). Зміни значень яскравості пікселів у результаті постобробки можуть бути настільки великі, що в деяких випадках «перекриють собою» наслідки розриву кореляційних зв'язків для пікселів, що лежать на границі області клону, що може привести до того, що норма відмітного околу блоку-прообразу виявиться більше норми відмітного околу блоку-клону. Найчастіше це відбувається тоді, коли за допомогою клонування з ЦЗ усувається деякий об'єкт (малих розмірів), що знаходиться в його «фоновій» (з незначними перепадами яскравості) області, з якої ж і обирається прообраз (рис.1).

З врахуванням цього момент виходу розглянутих відповідних блоків за межі реальних областей клону й прообразу повинен відслідковуватися в ході аналізу не по одному, а по декільком напрямкам, що й пропонується в удосконаленому в роботі методі.



Рис. 1. ЦЗ, для якого норма відмітного околу блоку-клону була менше норми відмітного околу блоку-прообразу в момент виходу за межі областей клону й прообразу в напрямку, паралельному осі ОУ: а – оригінальне ЦЗ; б – клоноване ЦЗ, збережене в форматі Jpeg з коефіцієнтом якості QF=55 (виділений прообраз)

Пропонується наступна модифікація методу, розробленого в [10].

Крок 1. Нехай $\bar{T}, \bar{\bar{T}}$ - виявлені деяким відповідним алгоритмом попередньо в аналізованому ЦЗ області клону й прообразу. Будемо вважати, що $\bar{T}, \bar{\bar{T}}$ є підобластями реальних областей $\bar{P}, \bar{\bar{P}}$ клону і прообразу: $\bar{T} \subseteq \bar{P}, \bar{\bar{T}} \subseteq \bar{\bar{P}}$.

1.1. Визначити: $\bar{T}_v, \bar{\bar{T}}_v$ - внутрішності $\bar{T}, \bar{\bar{T}}$ відповідно;

1.2. Визначити: $\bar{B}, \bar{\bar{B}}$ - пару відповідних 1×1 - блоків ЦЗ таких, що $\bar{B} \subseteq \bar{T}_v, \bar{\bar{B}} \subseteq \bar{\bar{T}}_v$.

1.3. Для $\bar{B}, \bar{\bar{B}}$ побудувати $\bar{O}, \bar{\bar{O}}$ - відповідні відмітні околи радіуса 1. Знайти $\|\bar{O}\|, \|\bar{\bar{O}}\|$ - матричні норми $\bar{O}, \bar{\bar{O}}$.

1.4. Обчислити: $G = \left| \|\bar{O}\| - \|\bar{\bar{O}}\| \right|$.

1.5. Покласти: $\bar{p} = 0, \bar{\bar{p}} = 0$ - лічильники, що показують, скільки разів у ході роботи методу як клон визначалася область $\bar{T}, \bar{\bar{T}}$ відповідно.

Крок 2. Для блоків $\bar{B}, \bar{\bar{B}}$:

2.1. Отримати відповідно $\bar{R}, \bar{\bar{R}}$ - блоки ЦЗ, розташування яких відповідає зсуву $\bar{B}, \bar{\bar{B}}$ на 1 піксель в обраному напрямку v .

2.2. Для блоків $\bar{R}, \bar{\bar{R}}$ побудувати $\bar{O}, \bar{\bar{O}}$ - відповідні відмітні околи радіуса 1. Знайти $\|\bar{O}\|, \|\bar{\bar{O}}\|$ - матричні норми $\bar{O}, \bar{\bar{O}}$.

2.3.

Якщо

$$\left| \|\bar{O}\| - \|\bar{\bar{O}}\| \right| \approx G, \quad (2)$$

то

$$\bar{R} \subseteq \bar{P}_v, \quad \bar{\bar{R}} \subseteq \bar{\bar{P}}_v,$$

де $\bar{P}_v, \bar{\bar{P}}_v$ - внутрішності $\bar{P}, \bar{\bar{P}}$ відповідно, границі клону й прообразу не досягнуті, покласти: $\bar{B} = \bar{R}, \bar{\bar{B}} = \bar{\bar{R}}, G = \left\| \bar{O} \right\| - \left\| \bar{\bar{O}} \right\|$; напрямок v зсуву залишається незмінним; перехід на крок 2.1;

інакше

якщо $\left\| \bar{O} \right\| > \left\| \bar{\bar{O}} \right\|,$

то $\bar{p} = \bar{p} + 1,$

інакше $\bar{\bar{p}} = \bar{\bar{p}} + 1.$

2.4.

Якщо потрібне уточнення отриманих результатів $\bar{p}, \bar{\bar{p}},$

то повернутися до первісних блоків $\bar{B}, \bar{\bar{B}},$ місця розташування яких визначені на кроці 1.2; змінити напрямок v їх зсува; перехід на крок 2.1.

Крок 3 (відокремлення клону від прообразу).

Якщо $\bar{p} > \bar{\bar{p}},$

то $\bar{T}$ - клон, $\bar{\bar{T}}$ - прообраз,

інакше $\bar{\bar{T}}$ - прообраз, $\bar{T}$ - клон.

Основна задача для забезпечення можливості побудови алгоритмічної реалізації запропонованого методу полягає в конкретизації наближеної рівності (2): визначенні кількісного показника того, що ця наближена рівність не має місця. Необхідно визначити, коли різницю між $\left\| \bar{O} \right\|, \left\| \bar{\bar{O}} \right\|$ можна назвати стрибком, що вказують на вихід за межі реальних клону, прообразу.

Експериментально було встановлено, що виходу за межі реальних клону й прообразу відповідає співвідношення $\left\| \bar{O} \right\| - \left\| \bar{\bar{O}} \right\| > 2G,$ яке й використовувалося при алгоритмічній реалізації вдосконаленого методу поряд з наступними значеннями параметрів, що фігурують у методі: як v використовуються 8 різних напрямків зсуву (додатний, від'ємний напрямки вздовж координатних осей, а також напрямки, що відповідають діагоналям (головній й побічній) блоків (вгору, вниз)), $l \geq 8.$

Зуваження 1. Специфіка запропонованого вдосконалення методу така (визначення й фіксація моменту стрибка значення модуля різниці норм відмітних околів розглянутих блоків), що для його ефективної роботи важливим є забезпечення того, щоб у розглянутих парах блоків ці блоки були відповідними в областях клону й прообразу.

Робота алгоритмічної реалізації запропонованого методу проілюстрована на рис. 2. Для попереднього виявлення областей клону й прообразу був використаний метод KL, розроблений в [6,7], у силу того, що ефективність цього методу в умовах постобробки клонованого ЦЗ перевищує ефективність сучасних аналогів. В результаті роботи методу KL ($l = 8$) для підобласті аналізованого ЦЗ (рис. 2(а)) розміром 120×120 пікселів (рис. 2(б)), що містить клон і прообраз, з урахуванням отриманої матриці мінімальних блокових відмінностей (ММБВ), що є основним об'єктом аналізу в методі KL (рис. 2(в) – графік інтерполяційного сплайна для елементів ММБВ), була обрана пара відповідних блоків (44,63) і (63,39) клону й прообразу (рис. 2(г)), яким у ММБВ відповідали рівні за значенням глобальні мінімуми (що дорівнювали 116).

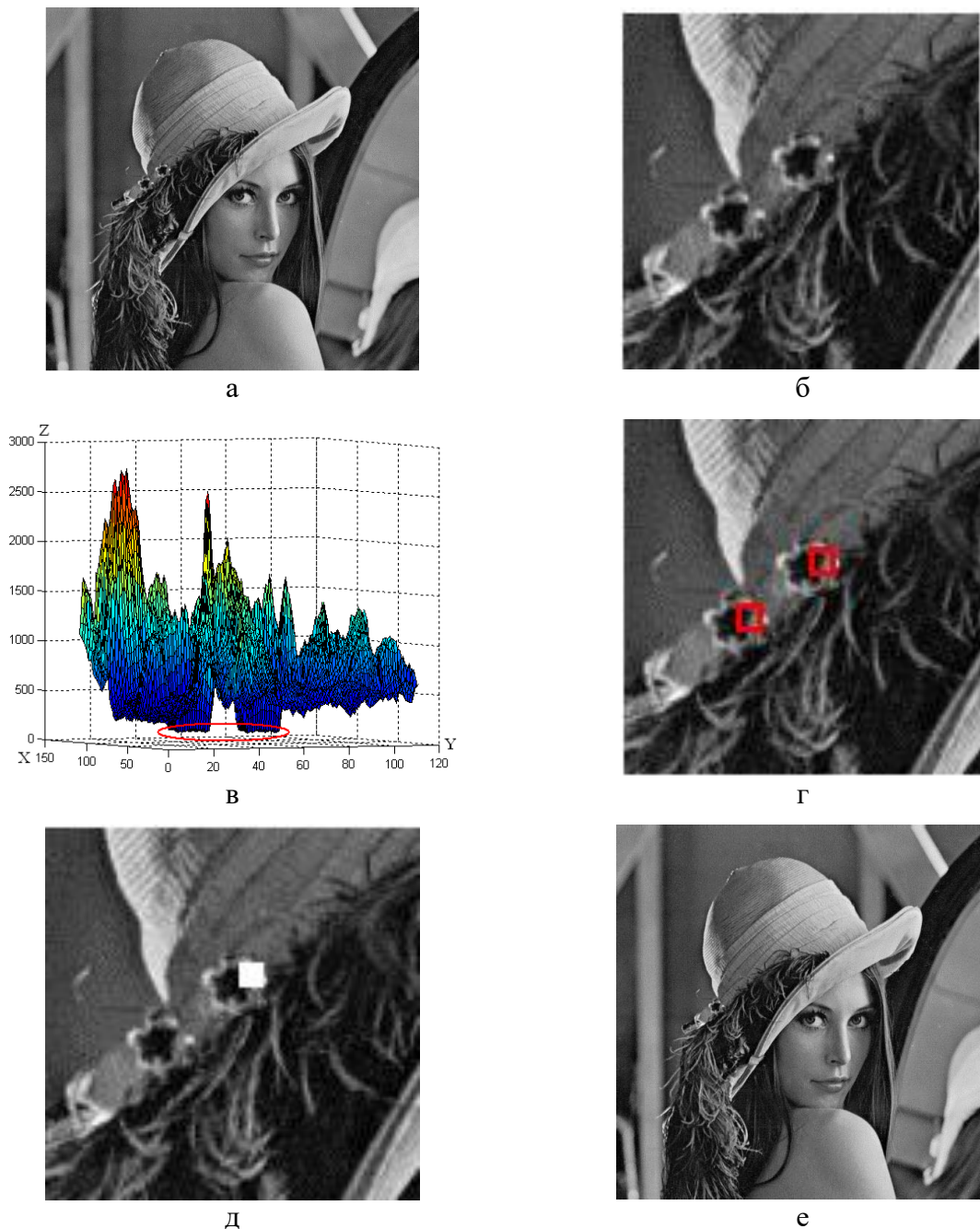


Рис. 2. Ілюстрація роботи розробленого методу для аналізу клонованого ЦЗ, що піддалося додатковим збурним діям: а – ЦЗ, піддане клонуванню з наступним збереженням у форматі з втратами (Jpeg, QF=75); б – підобласть ЦЗ, що містить клон і прообраз; в – ММБВ для підобласті ЦЗ з виділеними частинами, що відповідають клону й прообразу; г – відповідні 8×8–блоки клона і прообразу, що використовувалися для їх відокремлення; д – результат відокремлення клону від прообразу з визначенням місця розташування клону; е – оригінальне ЦЗ

Модуль різниці норм відмітних околів радіуса 1 для цих блоків склав 16. Результати застосування алгоритмічної реалізації розробленого методу відокремлення клону від прообразу наочно представлені на рис. 3, де зафіксовані значення модуля різниці норм відмітних околів відповідних блоків, місце розташування яких визначалося покроковим (на 1 піксель) зсувом блоків (44,63) і (63,39) в 8-мі напрямках (вліво, вправо, вгору, вниз, вздовж головної й побічної діагоналей (вгору, вниз)). Висновок про те, що має місце стрибок розглянутого значення, робився у випадку, якщо збільшення значення відбувалося не менш, ніж у два рази. Для таких значень визначалося, для якого блоку

норма відповідного околу більше (на рис. 3 у дужках ця інформація зазначена в наступних позначеннях: I - блок (44,63), II - блок (63,39)). В результаті в якості блоку, що належить клону, був визначений блок (44,63) (рис. 2(д)), оскільки він визначався таким в 5 напрямках виходу на границі областей клону й прообразу з 8 (рис. 3), що відповідає дійсності (рис. 2(е)).

		106 (I)			65 (I)	
			18		1	
				11	15	340 (I)
36 (I)	15	9	5	16	347 (I)	
			22	35(II)	308 (I)	
			25			
		26				
	33					
68 (II)						

Рис. 3. Числові значення модуля різниці норм відмітних околів відповідних блоків клону й прообразу (виділена комірка відповідає первісно виявленим блокам (44,63) і (63,39)), жирним шрифтом виділені значення, що характеризують стрибок, для ЦЗ, представленого на рис. 2(а)

Ілюстрація роботи алгоритму для ЦЗ, збереженого після клонування у форматі Jpeg з коефіцієнтом якості QF=60, представлена на рис. 4, де правильно виявлений клон позначений за допомогою відповідного блоку, використаного спочатку (рис. 4(г)).

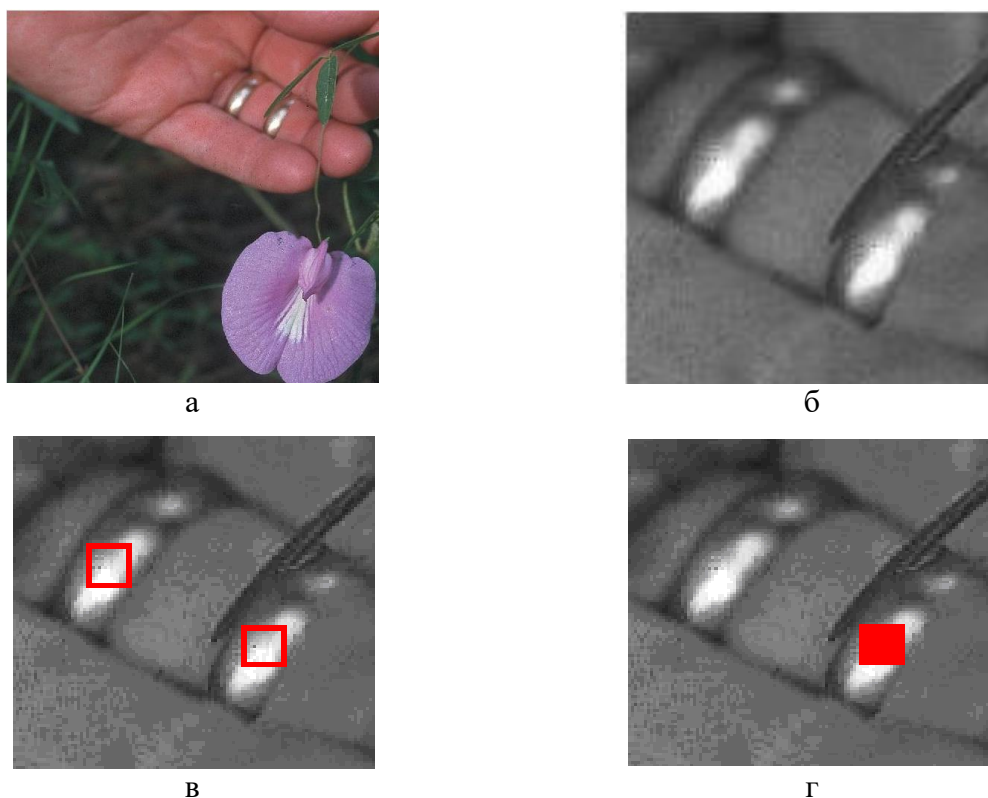


Рис. 4. Результат роботи алгоритмічної реалізації методу відокремлення клону від прообразу в умовах додаткових збурних дій: а – ЦЗ після клонування, збережене з втратами (Jpeg, QF=60); б – підобласть ЦЗ, що містить клон і прообраз, яка використовується для аналізу; в – відповідні блоки ЦЗ, що використовуються для відокремлення клону від прообразу; г – результат відокремлення клону від прообразу (позначений клон)

Зауваження 2. Вибір при проведенні обчислювального експерименту методу KL для попереднього виявлення областей клону й прообразу був зроблений не тільки завдяки високій ефективності методу в умовах наявності додаткових збурних дій. Для розробленого в даній роботі методу важливим є визначення пари *відповідних* блоків $\bar{B}, \bar{B}$ (крок 1.2) у внутрішностях клону й прообразу (зауваження 1). Специфіка методу KL дозволяє визначити ці блоки точно: їм у ММБВ будуть відповідати співпадаючі за значенням елементи, що представляють із себе локальні (глобальні) мінімуми ММБВ. У зв'язку з цим рекомендується при використанні запропонованого в даній статті методу надалі використовувати для попереднього виявлення клону й прообразу метод KL.

Висновки

У роботі вирішена важлива науково-практична задача вдосконалення методу відокремлення клону від прообразу, розробленого авторами раніше, метою якого було забезпечення ефективної роботи методу в умовах наявності додаткових збурних дій на клоноване ЦЗ. Запропоноване вдосконалення дозволило підвищити інформативність результатів виявлення клонування в ЦЗ.

У ході роботи отримана умова виходу відповідних блоків клону й прообразу, що належать їхнім внутрішностям, за межі реальних областей клону й прообразу з врахуванням постобробки клонованого ЦЗ: стрибок значення модуля різниці норм відмітних околів блоків $\bar{B}, \bar{B}$, що розглядаються в цей момент. Експериментально встановлено, що цей стрибок кількісно повинен не менше, ніж в 2 рази перевищувати значення розглянутого параметра для пари блоків, що розглядалися на попередньому кроці алгоритму (тобто тих блоків, зсув яких на 1 піксель у розглянутому в цей момент напрямку визначив місце розташування $\bar{B}, \bar{B}$).

Результати обчислювального експерименту підтверджують ефективність алгоритмічної реалізації запропонованого методу в умовах наявності додаткових збурних дій на клоноване ЦЗ.

Список літератури

1. Бобок, И.И. Метод организации скрытого канала связи, обеспечивающий проверку целостности контейнера / И.И. Бобок, А.А. Кобозева, Е.В. Малахов, А.Д. Шовкун // Сучасна спеціальна техніка. — 2012. — № 2 (29). — С. 76-85.
2. Vafaei, M. A Novel Digital Watermarking Scheme Using Neural Networks with Tamper Detection Capability/ M.Vafaei, H.Mahdavi-Nasab // J. Basic. Appl. Sci. Res. — 2013. — 3 (4). — Pp. 577-587.
3. Козина, М.А. Стеганографический метод организации скрытого канала связи, осуществляющий проверку целостности передаваемой информации / М.А. Козина. — Сучасна спеціальна техніка. — 2014. — № 4. — С. 98-106.
4. Singh, R. Copy Move Tampering Detection Techniques: A Review / R. Singh, Mandeep Kaur // International Journal of Applied Engineering Research. — 2016. — Vol. 11, No 5. — Pp. 3610–3615.
5. Rani, S. A Survey of Copy-Move Forgery Detection Techniques for Digital Images / S.Rani, M.Jayamohan, S.Sruthy // International Journal of Innovations in Engineering and Technology. — 2015. — Vol. 5, Iss. 2. — Pp. 419-426.
6. Кобозева, А.А. Задача обнаружения результатов клонирования в изображении и новый подход к ее решению в условиях дополнительных возмущений / А.А. Кобозева, С.Н. Григоренко // Информационные технологии в управлении, образовании, науке и промышленности: монография / под ред. В.С. Пономаренко. — Х.: Издатель Рожко С. Г., 2016. — С. 300-313.

7. Кобозева, А.А. Метод выявления нарушения целостности цифрового изображения, проведенного путем клонирования, робастный к сжатию с потерями / А.А. Кобозева, И.И. Бобок, С.Н. Григоренко // 17-я Международная научно-практическая конференция «Современные информационные и электронные технологии «СИЭТ-2016». — Одесса, 2016. — С. 127-128.
8. Кобозева, А.А. Выявление нарушений целостности цифрового изображения путем использования стеганографических алгоритмов / А.А. Кобозева, И.И. Бобок, Л.М. Дзюбинская // Информатика та математичні методи в моделюванні. — 2015. — Т.5, № 2. — С. 129-134.
9. Лебедева, Е.Ю. Метод локализации и идентификации оригинальной и клонированной областей изображения / Е.Ю. Лебедева // Информатика та математичні методи в моделюванні. — 2014. — Т.4, № 1. — С. 76- 84.
10. Бобок І.І. Метод відокремлення клону від прообразу в цифровому зображенні в умовах відсутності постобробки зображення / І.І. Бобок, А.А. Кобозева. — Вісник ЧДТУ. — 2018. — № 1. — С. 27-35.
11. Бобок, І.І. Теоретичні основи методу відокремлення клону від прообразу в цифровому зображенні / І.І. Бобок, А.А. Кобозева // Безпека інформації. — 2018. — Т.24, № 1. — С. 197-203.
12. Гонсалес, Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс; пер. с англ. П.А. Чочиа. — М.: Техносфера, 2006. — 1070 с.

УСОВЕРШЕНСТВОВАНИЕ МЕТОДА ОТДЕЛЕНИЯ КЛОНА ОТ ПРООБРАЗА В ЦИФРОВОМ ИЗОБРАЖЕНИИ

И.И. Бобок, А.А. Кобозева

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

Клонирование остается на сегодняшний день одним из наиболее широко и часто используемых при фальсификациях цифровых изображений (ЦИ) программных инструментов. Решению задачи выявления результатов клонирования уделяется много внимания, однако вопрос определения, какая из выявленных предварительно областей ЦИ является клоном, а какая прообразом, остается актуальным. В работе предложено усовершенствование метода отделения клона от прообраза, разработанного авторами ранее, эффективного в условиях отсутствия какой-либо обработки клонированного ЦИ. Целью усовершенствования является повышение информативности результатов выявления клонирования в ЦИ путем обеспечения эффективной работы соответствующего метода в условиях дополнительных возмущающих воздействий, в частности, в условиях сжатия с потерями клонированного изображения. Усовершенствование метода обеспечивается за счет выявления и фиксации момента скачка значения модуля разности норм отличительных окрестностей соответствующих блоков клона и прообраза, который имеет место при достижении этими блоками границ реальных областей клона и прообраза. В момент фиксации скачка клону отвечает блок, норма отличительной окрестности которого больше. Процесс фиксации скачка происходит для нескольких (максимально 8) пар соответствующих блоков, выходящих на границу клона и прообраза. Окончательный вывод делается с учетом того, какая из выявленных областей определялась как клон/прообраз большее количество раз. Результаты проведенного вычислительного эксперимента говорят об эффективности алгоритмической реализации предложенного метода в условиях наличия дополнительных возмущающих воздействий на клонированное ЦИ.

Ключевые слова: клонирование, цифровое изображение, отделение клона от прообраза, отличительная окрестность блока, дополнительные возмущающие воздействия

IMPROVEMENT OF THE METHOD OF SEPARATING THE CLONE FROM THE PROTOTYPE IN DIGITAL IMAGE

I.I. Bobok, A.A. Kobozeva

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

One of the widely and often used for falsifications of digital images of software tools remains cloning. Today much attention is paid to the task of revealing cloning, but the question of determining which of the identified areas of the image is a clone/prototype remains. There are different approaches that are used to solve this problem. One of the main approaches is the use of digital watermark technology. But embedding of digital watermarks in the image violates its integrity. It is undesirable. Another approach is to search for the results of the post-processing of the clone, which differs from the processing of the prototype. But in the case when the clone/prototype are small, clone postprocessing is often absent. This makes the methods of this group incompetent in this case. Previously the authors developed a method for separating the clone from the prototype in the absence of additional processing of the cloned digital image. This article proposes an improvement of this method. The goal of the improvement is to increase the informative value of cloning detection results in a digital image. The improved method is effective in conditions of additional perturbing effects, in particular, compression with losses of the cloned image. This method does not use digital watermark technology. Improvement of the method is provided by detecting and fixing the moment of the jump in the value of the modulus of the difference in the norms of the distinctive neighborhoods of the corresponding clone and prototype blocks. The distinctive neighborhood of the block B is $(2k + 1) \times (2k + 1)$ -matrix. Elements of this matrix reflect the difference of B from the image blocks, which are from B at a distance not exceeding k . This jump takes place when these blocks reach the boundaries of the real regions of the clone and the prototype. At the moment of fixing the jump, the clone is answered by a block whose norm of a distinctive neighborhood is larger. The process of fixing the jump occurs for several (max. 8) pairs of corresponding blocks. The final conclusion is made taking into account which of the identified areas was defined as a clone/prototype more times. The results of the computational experiment indicate the effectiveness of the proposed method in the presence of additional perturbing effects on the cloned digital image.

Keywords: cloning, digital image, separation of the clone from the prototype, distinctive neighborhood of the block, additional perturbations

SELF-DIAGNOSTICS OF COMPLEX SYSTEMS WITH A SOFTWARE-CONFIGURABLE STRUCTURE

I.V. Korobiichuk¹, R.V. Hryshchuk², V.O. Horoshko³, Yu.E. Hohlacheva³

¹Warsaw University of Technology,

1, pl. Politechniki, Warszawa, 00-661, Poland; e-mail: igor@mchtr.pw.edu.pl

²Sergey Korolyov Zhytomyr Military Institute,

22, Mira, Ave., building ZhVI, Zhytomyr, 10004, Ukraine; e-mail: dr.hry@i.ua

³National Aviation University,

1, Cosmonaut Komarova, Ave., Kiev, 03058, Ukraine; e-mail: professor_va@ukr.net, hohlachova@gmail.com

Using the method of simulation and statistical modeling, the operability was established and estimates of the effectiveness of the proposed algorithm for self-diagnostics of complex computer systems with a software-configurable structure were obtained. The structure of complex computational systems is the Cayley diagram of some finite abelian arc group in the Cayley diagram that have the markers of the generators of the group. The described graphs are called CAIS graphs (graphs for providing finite abelian isotropic and symmetric structures). Due to the limited number of intermodule connections of complex computing systems, it is necessary to use working links between modules to determine its state. Consequently, the diagnostic graph for complex computing systems is CAIS graph. The symmetry property of the CAIS graph means that adjacent modules of complex computer systems are mutually testable. It is possible to correctly determine the state of complex computing systems if it is performed by deliberately working tools that make up the core of complex computer systems. Define the diagnostic core as a collection of tools that have a higher reliability than the system checked with it. The reliability of the kernel is provided by means that do not belong to the system it checks. One method of automating the detection of the state of modern complex computing systems is the method of promotion. At each step of the promotion, the serviceability of some nodes is determined by the integrity of the others, which is set in the previous steps. The process of spinning has always started from the core of the system. The functional characteristics of the modules of complex computing systems are such that any of them can be used as a core. If, then the task of determining the state of the system can be clarified: by the results of mutual verification, identify at least one known serviceable module. Identified modules are used as the core of complex computer systems. The method of determining the state of serviceability of modular survivable complex computing systems is the modification of the known method of promotion. For complex computational systems with a software-configurable structure, the concept of a diagnostic kernel is concretized, a heuristic decentralized kernel allocation algorithm is described.

Keywords: complex computing systems, diagnostic model, diagnostic graph, algorithm, costs of diagnostics

Introduction

Complex computing systems (CCS) with software-configurable structure [1,2] are durable modular systems, the functioning of which is based on the use of decentralized control algorithms. Current state of microelectronics makes it possible to implement CCS on computational modules, each of which is a complete computer. Modules, in terms of diagnosis, are units of indivisible system. Their functional characteristics allow to perform a full check of neighboring modules. In this case, the state of serviceability or operability (hereinafter – “the state”) of CCS in conditions of multiple faults is determined by comparing the results during cross-checking of modules [3-11]. Multiplicity of faults is a maximum permitted number of faulty modules, under which still exists the ability to determine the state

of the system. Dependence of the multiplicity malfunctions on the number of modules and the structure of CCS is investigated in paper [3,4].

The CCS structure is a Cayley diagram of some finite abelian G groups. Arches in the Cayley diagram have markers of group generators. The described graphs are called FAIS graphs (graphs used for providing finite abelian isotropic and symmetric structures) [4, 5].

Considered CCS are t -diagnosed with repair, i.e. there is a sequence of execution of the set of all possible tests and repair of identified malfunctions in modules, that allows to identify all the problems initially present in the CCS, provided that their number does not exceed t . Paper [3,4] provides a method to determine the state of CCS, t -diagnosed with repair, which are presented by Cayley graphs. This paper describes a heuristic algorithm that solves this method, and evaluates its effectiveness.

Materials and methods

The diagnostic model of CCS is the digraph $G=(V,E)$, in which set $V=\{1,2,\dots,N\}$ represent modules of the system, and set E represents performing arc tests. For $i, j \in V$ an arc (i, j) (from i to j) exists, if and only if the module i can test the module j . The vertices of the graph have marks x , the values $x(i)=1$ of which determine the state and $x(i)=0$ if the module i is faulty. The test results for the CCS modules correspond to the weights of the graph arcs. For $(i, j) \in E$ the weight $a(i, j)=0$, if the module confirms the serviceability of the module j ; otherwise $a(i, j)=1$. The set of vertices, containing singular values of x marks, makes up an image of the system's malfunctions, and the totality of the values of the weights a of the graph forms its syndrome S . For any image of a malfunction F , $F \subseteq V$, the conditions for the formation (generation) of a syndrome S are as follows:

Condition 1. Performing $\forall (i, j) \in E \left\{ (i \in \bar{F} = V - F) \wedge (j \in F) \rightarrow a(i, j) = 1 \right\}$.

Condition 2. Performing $\forall (i, j) \in E \left\{ (i \in \bar{F}) \wedge (j \in \bar{F}) \rightarrow a(i, j) = 0 \right\}$.

Condition 3. Performing $\forall (i, j) \in E \left\{ (i \in F) \wedge (j \in \bar{F}) \text{ possible } a(i, j) = 1 \right\}$.

Condition 4. Performing $\forall (i, j) \in E \left\{ (i \in F) \wedge (j \in F) \text{ possible } a(i, j) = 0 \right\}$.

In the conditions the arrow is indicating an implication operator. The result of the test performed by a valid module determines the status of the module being tested (conditions 1 and 2), and when executed by the faulty module it does not depend on the state of the module being checked (conditions 3 and 4).

In the described model, the state of CCS is defined by identification of the graph vertices that form the set F , according to a given S syndrome.

Due to the limited number of inter-modular CCS links, it is necessary to use working links between the modules to determine its state. Therefore, the diagnostic graph $G=(V,E)$ for CCS is an FAIS graph. The symmetry property of the Cayley graph means that adjacent CCS modules are mutually testable.

It is possible to correctly determine the state of CCS, if it is carried out by knowingly effective means that make up the kernel of CCS. Define the diagnostic core as a collection of tools that have a higher reliability than the system checked with it. The reliability of the kernel is provided by means that do not belong to the system it checks.

One of the methods for automating the determination of the state of modern CCS is the method of promotion [3]. At each step of the promotion, the serviceability of some nodes is determined by the integrity of the others, which is in turn determined in the previous steps. The process of spinning has always started from the kernel of the system.

The functional characteristics of CCS modules are such that any of them can be used as a kernel. If $t < N$, then the task of determining the state of the system can be clarified: to reveal at least one known serviceable module by the results of a mutual check. Identified modules are used as the kernel of CCS.

It was shown in [3] that for a diagnostic graph $G = (V, E)$ with the symmetry property, the transformation

$$\forall i \in V \left\{ \left[(i, j) \in E \right] \wedge \left[a(i, j) = 1 \right] \rightarrow E = E - \{(i, j), (j, i)\} \right\}, \quad (1)$$

is being performed by a graph G_0 , in which the marks of x vertices of each connected component coincide. We choose as t such t^* that for any $F, |F| \leq t^*$, and any generated F syndrome, there exists at least one connected component of order at least $(t^* + 1)$, where t^* is the number of faults. Given the assumption of the multiplicity of faults, it includes vertices that represent serviceable modules, which can therefore be used as the diagnostic core of CCS.

It is necessary for CCS modules to have an ability of mutual transfer of the test results and their comparison in order to allocate the kernel. Any module can be part of the kernel, so the means for performing the specified functions must be in each module. In order to allocate actually serviceable modules as a kernel, the considered means should be serviceable irrespective of the serviceability of the modules being checked. These means constitute a cellular automaton with the CCS structure and form its distributed kernel. The homogeneity of the structure of the control automaton makes it possible to automate the verification of its own state. In relation to the means used, the control device acts as a verifiable system. Thus, the means for automating the determination of the state of CCS have a hierarchical structure. Reliability of means related to adjacent levels of the hierarchy increases from bottom to top. Finiteness of the number of hierarchy levels is assured by the assumption of absolute reliability of its upper level. This property is assigned to the operational staff of CCS.

Theory of algorithm for isolating the diagnostic core

Suppose we are given an Cayley graph $G = (V, E)$ that represents a G group with $g_0, g_1, \dots, g_{n-1}$ generators. By virtue of the symmetry property, each vertex of the G graph has $2n$ number of arcs with the generators and their inverses. Suppose that G is given a set of admissible images of faults and a set of syndromes generated by these images. In this case, the condition $0 \leq |F| \leq t^*$ holds for any $F \in F$. It is possible to find an algorithm by which for any $F \in F$ and any generated syndrome it is possible to determine the vertex markup $X = \{x(i)\}$ for some $W \subseteq V$ such that $W \cap \bar{F} \neq \emptyset$, singling out $W \cap \bar{F} \neq \emptyset$ at least one vertex i such that $i \in (W \cap \bar{F})$.

Let us describe some of the thesis's that form the basis of the kernel extraction algorithm. Any FAIS graph has a fundamental cycle, since the parity of the degrees of its vertices implies the existence of an Euler cycle for it. Consider the following algorithm for traversing the graph. (In the algorithms considered below, the $\leftarrow$ sign is the operator of the left assignment).

Algorithm 1.

Stage 1. Suppose $P(i), T(i), H(i)$ are the marks of the i -th vertex, $i \in V$, such that $P(i) \in \{0, 1, 2, \dots, n-1\}, T(i) \in \{0, 1\}, H(i) \in \{0, 1\}$. The $P(i)$ and $T(i)$ values determine the bypass sequence G , and $H(i) = 1$ selects an arbitrarily chosen initial vertex. The initial value of the indicated marks is determined by the conditions $\forall i \in \{P(i) = 0, T(i) = 1\}; \exists k \in V \{H(k) = 1\}; \forall i \in (V - k) * \{H(i) = 0\}$. $k \in V$ will be the vertex of the graph G considered in the current pass of the algorithm.

Stage 2. If $T(k) = 1$, then $T(k) \leftarrow 0$, otherwise $P(k) \leftarrow P(k) + 1 \pmod{n}$.

Stage 3. Go to the vertex j , which is incident to the arc emanating from k , and has a mark of the generator g_l such that $l = P(k); k \leftarrow j$.

Stage 4. If $\left[\exists k \in V \{T(k) = 1\} \wedge [H(k) = 0] \right]$, then go to stage 2, otherwise end.

The condition of the operator 4 is fulfilled when the sequence generated by Algorithm 1 contains all the vertices of G and is closed. Only if this condition is fulfilled, Algorithm 1 is completed.

Assertion 1. Algorithm 1 provides the formation of the main cycle for the FAIS graph G .

Corollary 1. The length of the main cycle of the CAIS graph G formed by algorithm 1 is less than the length of the Euler cycle of this graph.

The proofs of Assertion 1 and Corollary 1 are not given in the paper.

Assertion 2. $G = (V, E)$ - is a random diagnostic graph possessing the symmetry property:

$\forall i, j \in V \{(i, j) \in E \rightarrow (j, i) \in E\}, aS = \{a(i, j) | (i, j) \in E\}$ is a syndrome, caused by an image of malfunctions F . Then the condition $\forall a(i, j), a(i, j) \in S \{a(i, j) = 0 \wedge a(i, j) = 1 \rightarrow i \in F\}$ is fulfilled.

Suppose the contrary: $i \in \bar{F}$. Then it follows from conditions 1 and 2 that $j \in \bar{F}$. But since $a(i, j) \neq a(j, i)$, then $(i \cup j) \cap F \neq \emptyset$. Consequently, $i \in F$ does not depend on whether it is $j \in F$ satisfied or $j \in \bar{F}$, as required to prove.

Corollary 2. Suppose $G^* = (V^*, E^*)$ is the connectivity component of a graph G_0 , which is given a value S for $G = (V, E)$, and suppose $i, j \in V$ such that $i \in V^*, (i, j) \in E$. If the condition of Assertion 2 is satisfied for i and j in G , then $G^* \subseteq F$.

The kernel is isolated as a result of a sequential analysis of the elements of the syndrome S , performed when the graph G is traversed. The rules for selecting the next vertex are the same for all vertices of the graph and are given by the following algorithm.

Algorithm 2.

Stage 1. $G^* = (V^*, E^*)$, $G^* \subset G$ - the generated connectivity component and $k \in V^*$. The set of vertices V_k of the graph G adjacent to k is subdivided into disjoint sets of direct V_{kn} and reverse V_{ko} testing directions (analysis of the values of the marks of arcs $a(i, j)$ emanating from k). If $j \in V_k$ does not enter into any of the previously formed connectivity components and the value $a(k, j)$ has not yet been checked, then $j \in V_{kn}$. If $j \in V_k$ and the transition to k is performed from j , then $j \in V_{ko}$. Introduce a mark k for the selection of vertices entering the

connectivity component: if the vertex belongs to some connectivity component, then $K(j)=0$, otherwise $K(j)=1$. Also introduce marks for the separation of arcs of the connectivity component $G^$: if $(i, j) \in E^$, then $M(i, j)=1$, otherwise $M(i, j)=0$. Define on the set V_{kn} an order relation that corresponds to an increase in the indices of marks g_i of arcs emanating from k and incident to the vertices of V_{kn} . Introduce the service Boolean variables A, B, C , the values of which will be used in Algorithm 3: $A \leftarrow 0; B \leftarrow 0; C \leftarrow 0$; form for $k \in V_{kn}$ and V_{ko} .

Stage 2. If $V_{kn} \neq \emptyset$, then go to stage 3, otherwise - go to stage 6.

Stage 3. Suppose j is another element V_{kn} . If $a(k, j)=0$, then go to stage 4, otherwise to stage 5.

Stage 4. Exclude j from $V_{kn}; K(j) \leftarrow 0; M(k, j) \leftarrow 1$; go to the vertex $j: k \leftarrow j$, form V_{ko} : if $[(V_{ko} = \emptyset \wedge j \in V_k \wedge M(j, k)=1)]$, then $j \in V_{ko}$; form V_{kn} : $\forall i \in V_k - V_{ko} \{K(i)=1 \rightarrow i \in V_{kn}\}$; $A \leftarrow 1$; go to stage 9.

Stage 5. Here $a(k, j)=1$. Delete j from V_{kn} ; go to stage 2.

Stage 6. Here $V_{kn} = \emptyset$. If $V_{ko} \neq \emptyset$, go to stage 7; otherwise, go to stage 8.

Stage 7. Testing is referred by a singleton set V_{ko} (vertex j); delete j from $V_{ko}; B \leftarrow 1$, go to stage 9.

Stage 8. Here $V_{kn} = V_{ko} = \emptyset$. Formation of $G^$ is completed; $C \leftarrow 1$.

Stage 9. The end of the algorithm.

Assertion 3. When using algorithm 2, the generated connectivity component $G^=(V^, E^)$ is a tree covering the set of vertices $V^$. The root is the vertex with which the formation of $G^$ is started. Suppose $k \in V^$ is the vertex from which the analysis of marks $a(k, j); j \in V_k$ begins. Then the following assertions hold:

1. for any $G^$, a singular oriented simple goal C exists, starting from the root vertex and entering into k , such as $\forall j \in V^ (V_{jn} = \emptyset \rightarrow j \in C)$; the reverse statement is not true;

2. for every $j \in C$: if there exists $(j, m) \in E^$ such that $(j, m) \notin C$, then there exists $(m, j) \in E^$;

3. suppose that $j \in V^$ satisfies the conditions of §3.2: exclude from $G^$ the $(j, m)(m, j)$ arcs, denote the $G(m, j)=[V^ (m, j), E^ (m, j)]$ subgraph of the graph $G^$, for which $m \in V^ (m, j)$. Then $\forall k \in V^ (m, j) \{ (k, s) \in E^ (m, j) \rightarrow (s, k) \in E^ (m, j) \}$.

Corollary 3. Suppose $G^ (m, j)$ is a subgraph of a graph $G^$ that satisfies the conditions of §3 of Assertion 3. Then $\forall k \in V^ (m, j) \{x(k)=x(j)\}$.

Assertion 4. Suppose C is an arbitrary simple chain defined on the structure of the connectivity component $G^$. Suppose i and j are the vertices entering into C , while j is accessible from i , i.e. $i < j$. Then, $\forall i, j \in C \{i < j \rightarrow x(i) \geq x(j)\}$, i.e. in C the vertices with marks $x(i)=0$ can not precede the vertices with marks $x(j)=1$.

The proof follows directly from conditions 1 and 2.

Corollary 4. Suppose $L(C)$ is the number of vertices in chain C . If $L(C) = (t^* + 1) + k, k \geq 0$, then C contains no more than t^* vertices with marks t^* preceding the vertices with marks $x(i) = 0$.

The proof follows from the condition of the multiplicity of faults. Suppose $x \in \{0, 1, 2, 3\}$. The values 0 and 1 of the x mark are defined as finite; the $x = 3$ value is the initial value when executing the kernel allocation algorithms; the vertex gets the value $x(i) = 2$, if, based on the results of the module check, the final value of the mark can not be determined.

The connectivity component G^* is completed if one of the following conditions is true:

Condition 5. Fulfilled $\forall i \in V^* \{ (V_{in} = \emptyset) \wedge (V_{io} = \emptyset) \}$. This condition corresponds $C=1$ in the algorithm and 2. If $|V^*| < t^* + 1$, then the value x for the vertices V^* can not be determined until the CCS kernel is allocated. For such vertices $x(j) = 2$.

Condition 6. Fulfilled $\exists i, j \in V^* \{ a(i, j) = 0 \wedge a(j, i) = 1 \}$. In this case, in accordance with Corollary 2, G^* contains the vertices of two connectivity components of the graph $G_0 : G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$. Here $\forall i \in V_1 \{ x(i) = 1 \}; \forall i \in V_2 \{ x(i) = 2 \}$, as for any component satisfying the condition $|V^*| < (t^* + 1)$.

Condition 7. On passing to the vertex j in the course of direct viewing $|V^*| = t^* + 1$ is received. In this case, we have $|V^*| = t^* + 1$ for the last vertex included in V^* . In accordance with Corollary 2 and Assertion 4, it is possible that $\exists i, j \in V^* \{ a(j, i) = 1 \}$. In this case, G^* decomposes into two connectivity components: G_1^* , for vertices i of which $x(i) = 1$, and G_0^* , for vertices of which $x(i) = 0$. All vertices G_0^* form the diagnostic core of the graph.

Next, suppose that for some connectivity component G^* , formed during the allocation of the kernel, $\forall i \in G^* \{ x(i) = 2 \}$. Taking into account the property of the graph G_0 , the value of the marks x of all vertices G^* is determined by the singular value $a(i, j)$ for such adjacent vertices i and j , that $i \in G^*, j \notin G^*, x(j) = 0$.

We now describe the kernel allocation algorithm using algorithms 1 and 2. In addition to the entered marks, a variable R will be used in it, the value of which determines the order of the connectivity component being formed: $R \in \{0, 1, 2, \dots, t^* + 1\}$.

Algorithm 3.

Stage 1. The initial values of the marks G and variables are determined by conditions

$$\begin{aligned} &\forall i \in V \{ P(i) = 0, T(i) = 1, V_{in} = \emptyset, K(i) = 1, x(i) = 3 \}; \\ &\forall (i, j) \in E \{ a(i, j) \in S, M(i, j) = 0 \}; \exists s \in \{ H(s) = 1 \}; \forall i \in (v - S) \{ H(i) = 0 \}. \end{aligned}$$

The initial vertex s is chosen arbitrarily. Suppose k is the vertex of the graph considered in the course of the algorithm. Then $k \leftarrow s; R \leftarrow 0$.

Stage 2. Run Algorithm 2 for k . If, $A = 1$ then go to stage 3, if $B = 1$, then go to stage 4; if $C = 1$, then go to stage 6.

Stage 3. $R \leftarrow R + 1$, if $R = t^* + 1$, then go to stage 9, otherwise go to stage 2. Here the order of G^* increases, because $j \in V_{kn}$ is included in G^* . The transition to stage 9 takes place when the first element of the kernel is defined.

Stage 4. If $a(k, j)$, then go to stage 8, otherwise go to stage 5. Fulfillment of the condition means the completion of the formation of G^* by the condition of approval 3: $G = G_1 \cup G_2$ and $j \in G_1, k \in G_2$. The component G^* is marked with notations M .

Stage 5. Move to the vertex $j: k \leftarrow j$; go to stage 2.

Stage 6. Here $G^* = G_2$; $H(k) = 1$. For all $i \in V_2^*$ perform $x(i) \leftarrow 2$.

Stage 7. Go to the vertex i of the component G^* , for which $H(i) = 1; k \leftarrow i; H(k) \leftarrow 0$; execute Algorithm 1 (stages 2, 3) until a vertex k is found, for which $K(k) = 1; K(k) \leftarrow 0; H(k) \leftarrow 1; R \leftarrow 0$; go to stage 2. As a result of the described sequence of actions, the mark H is transferred to a vertex that does not belong to one of the previously formed connectivity components.

Stage 8. For all $i \in V_1^*$ execute $x(i) \leftarrow 1$; for all $i \in V_2^*$ perform $x(i) \leftarrow 2$; go to stage 7.

Stage 9. $x(k) \leftarrow 0; K(k) \leftarrow 0$. Diagnostics begins with determining the final values of the marks x for the vertices of G^* . They are determined as a result of an analysis of the values of the marks a of arcs opposite to the arcs of a simple oriented chain C , which is starting from vertices s with a mark $H(s) = 1$ and entering the vertex k (see Corollary 4). We regard the component G^* as a collection of subtrees $L(C)$, copies of which are vertices of the chain C . Each of these trees satisfies the conditions of section 3 of Assertion 3, and Corollary 3 holds for each of them.

Stage 10. For all the vertices i from G^* , included in the sub-tree with root in k , execute $x(i) \leftarrow 0$.

Stage 11. If $V_{ko} = \emptyset$, go to stage 15. The condition is fulfilled when the root vertex G^* is reached.

Stage 12. One-element set $V_{ko} = \{j\}$ is to be tested. If $a(k, j) = 1$, then go to stage 14, otherwise go to stage 13. Fulfillment of the condition means that in accordance with Corollary 2 $j \in V_1^*$.

Stage 13. $k \leftarrow j; x(k) \leftarrow 0$ go to stage 10.

Stage 14. $k \leftarrow j; x(k) \leftarrow 1$ for all vertices $i \in V_1^*$ execute $x(i) \leftarrow 1$.

Stage 15. The analysis of G^* is complete. All $i \in V_0^*$ are involved in the diagnosis. Diagnosis consists in determining the belonging to F of the elements, not included in G^* . The exceptions are the vertices for which Assertion 2 is satisfied. For diagnostics, it is necessary to perform an analysis k of the elements S , where $K \leq N - |V^*|$. The inequality is valid if there are vertices for which Assertion 2 is satisfied, and also in connection with the fact that the determination of the state of all elements from G_2^* , which are formed when the kernel is allocated, is performed by the singular value $a(i, j)$ of the arc weight (i, j) , if $i \notin G_2^*, j \in G_2^*, i \in F$ (Corollary 2).

Result and discussion

It is easy to see that Algorithm 3 allocates the kernel of CCS in a finite number of stages. It follows from the above description of Algorithms 1-3 that they allow a decentralized implementation: changing the value of the vertex and arc marks, as well as the rules for traversing the graph are determined only by the values of the marks of adjacent elements.

To obtain estimates of the effectiveness of the heuristic Algorithm 3, the method of simulation-statistical modeling is used. The structure of the diagnostic graph $G = (V, E)$ of the system and the power r of the fault sample, having values from 1 to t^* , are set. Using r as a parameter is allowing to obtain the potential characteristics of Algorithm 3. For each $r \in \{1, 2, \dots, t^*\}$ the number of experiments B is performed, in each of which an image of faults $F_r, |F_r| = r$, the syndrome generated by it, and the vertex with a mark C are arbitrarily chosen.

Events that consist that $i \in F_r$ or i have a mark H take place with probability $1/N$ and do not depend on the value r and composition F_r . The values $a(i, j)$ for the graph G are determined for the chosen F_r , with the condition that when $i \in F_r$, then $a(i, j)$ takes the value 0 and 1 with probability $p(0)$ and $p(1)$, respectively.

Algorithm 3 is divided into three stages:

1. The allocation of the kernel - from the initialization of the algorithm to the selection of the first vertex with a mark $x = 0$;
2. Determining the value of the vertex marks for the connectivity component of the order $t^* + 1$;
3. Determining the marks of the remaining vertices of the graph.

During the simulation, the data are summarized to determine the integral potential characteristics of the algorithm's efficiency, as well as to assess the practicability of implementing its individual elements (practical completeness of the algorithm). The latter is due to the fact that under the conditions of practical application, some elements of Algorithm 3 can be performed rather rarely because of the low probability of the occurrence of events causing their execution.

To do this, integral characteristics of the algorithm are introduced.

1. Vector coefficient $K_k = \{K_{kr}\}, r \in \{1, 2, \dots, t^*\}$ of the relative overhead expenses for the allocation of the CCS kernel, the coordinates of which are the values $K_{kr} = [M_r(T_k) - t^*] / t^*$. Here the multiplicity of faults t^* coincides with the minimum number of checks of values $a(i, j)$ (tests) for the allocation of the kernel; $M_r(T_k)$ - the average number of tests required to perform the first mark $x = 0$, when $|F_r| = r$.

2. Vector coefficient $K_e = \{K_{er}\}, r \in \{1, 2, \dots, t^*\}$ of the relative expenses of determining the state of CCS, the coordinates of which are the values $K_{er} = M_r(T_e) / |E|$, where $M_r(T_e)$ is the average number of tests required to determine the state of CCS, when $|F_r| = r$.

For FAIS graphs $|E| = 2vN$ (here $v = 2$). Obviously, the smaller the values K_{er} are, the more efficient the algorithm.

To evaluate the conditions for the practical completeness of the algorithm, vector coefficients are used whose coordinates are the values of the characteristics of the following events, processed by Algorithm 3: completion of the formation of the connectivity component in stage 1 by the formation G_2^* or formation G_1^* and G_2^* ; in stage 2, by formation G_0^* and G_1^* ; using Algorithm 1. The completion of the formation of connectivity components is characterized by the following indicators.

1. Vector coefficient $K_m = \{K_{mr}\}, r \in \{1, 2, \dots, t^*\}$ of the relative coverage of the image of malfunctions with the power r . The coordinates K_n are the values $K_{mr} = M_r(A_1) / r$, where $M_r(A_1)$ is the average number of vertices i , such that $i \in F_r$ received marks $x(i) = 1$ or $x(i) = 2$ in either stage 1 or 2 of Algorithm 3, $M_r(A_1) = \sum_{i=1}^3 M_{ri}(A_1); M_{r1}(A_1), M_{r2}(A_1)$ and

$M_{r3}(A_1)$ the average number of vertices from F_r , which are included in the components of the species G_1 and G_2 in stages 1,2,1 respectively.

2. Vector coefficient $K_{m2} = \{K_{m2r}\}, r \in \{1, 2, \dots, t^*\}$ of covering the image of malfunctions in stage 2. The coordinates K_{m2} are the values $M_{r2}(A_1)$.

3. Vector coefficient $K_{cm} = \{K_{c2}\}, r \in \{1, 2, \dots, t^*\}$ of the possibility of completing stage 2 by forming G_0 and G_1 . The components of the vector coefficient are the probabilities of occurrence of the specified event.

So, FAIS graphs representing CCS of N modules are investigated, $13 \leq N \leq 90$. On fig. 1 and fig. 2 the characteristics of a set of graphs are given, the order of which corresponds to the values $N = 13, 20, 25, 30, 40, 50, 60, 70, 80, 90$; multiplicity of faults for them $t_{13}^* = t_{20}^* = 4$; $t_{25}^* = t_{30}^* = t_{40}^* = t_{50}^* = 12$; $t_{60}^* = t_{70}^* = t_{80}^* = 16$; $t_{90}^* = 20$. Defining relations (except those which are setting commutativity) for the group description of these graphs have the form $(g_0^{13} = I, g_1 = g_0^5)$; $(g_0^{20} = I, g_1 = g_0^8)$; $(g_0^{25} = I, g_1 = g_0^7)$; $(g_0^{30} = I, g_1 = g_0^6)$; $(g_0^{40} = I, g_1 = g_0^5)$; $(g_0^{50} = I, g_1 = g_0^6)$; $(g_0^{60} = I, g_1 = g_0^{10})$; $(g_0^{70} = I, g_1 = g_0^{22})$; $(g_0^{80} = I, g_1 = g_0^{12})$. Here I is the singular element of the group.

In fig.1 and fig. 2, the coordinates of the vector coefficients are shown as functions of r for different values N . The investigated functions are monotonically increasing from r and monotonically decreasing from N .

From fig. 1 and fig. 2, where the functions K_k and K_e are respectively shown, it is clear that the efficiency of the algorithm increases with the number of modules in CCS. The number of tests required for the diagnosis of CCS does not exceed the value $0,4|E|$.

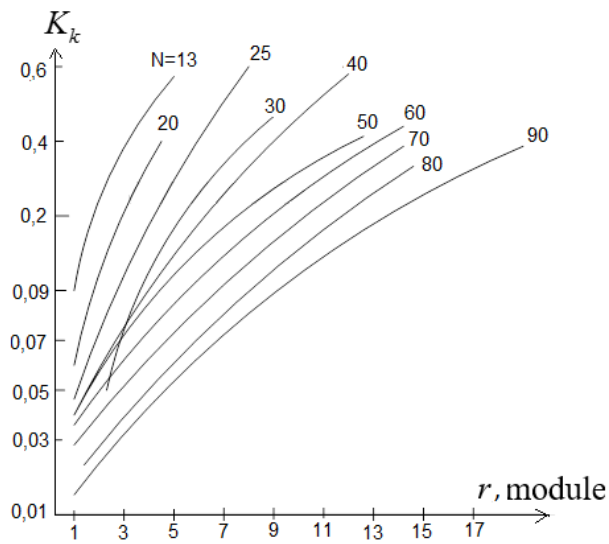


Fig. 1. Characteristics of a set of graphs from the function K_k

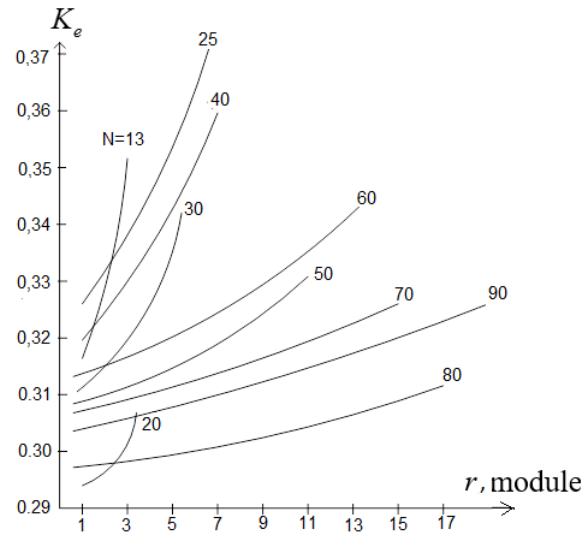


Fig. 2. Characteristics of a set of graphs from the function K_e

Fig. 2 shows the essential dependence of the costs of diagnostics on the relationship t^* / N .

The simulation results show that no less than $0,9r$ faulty CCS modules are determined at the stage 3 of the algorithm being investigated. The contribution to the value of the coordinates of the vector coefficient K_m is determined by the ratio

$M_{1r}(A_1):M_{2r}(A_1):M_{3r}(A_1)=10^{-3}:1:10^{-1}$, i.e. the main contribution to the value of coordinates K_n is made by the completion of stage 2 by the formation of G_0^* and G_1^* .

Studies have shown that K_{m2} is a nonlinearly increasing function of r . The nonlinearity depends on the probability that for stage 2 $|V_1^*| > 1$ (at $r = t^*/2$ this probability for the investigated structures is not lower than (0.15)). The dependence of K_{c2r} on r is close to a linear function $K_N r$. The coefficient K_N corresponds to the value obtained by modeling the value of the first coordinate K_{02} .

A typical sequence of execution of Algorithm 3 can be represented as follows. In most cases, the allocation of the connectivity component that makes up the kernel is performed on the first attempt. There is a possibility of one or two faulty modules present in this component. One of them is the root module of the subsystem. The structure of the component making up the kernel is in most cases a simple chain, which ensures the maximum number of kernel modules involved in determining the state of CCS. Usually, in stage 1, one or two connectivity components are formed $G_2^*; 1 \geq |V_2^*| \geq 2$.

The formation of the connectivity component in stage 1 is rarely completed by the formation of G_1^* and G_2^* . If such an event takes place, then $|V_1^*| \leq 3$. Other values for the examined graphs were not observed.

Conclusions

Thus, the conditions for automating the determination of the state of serviceability of durable modular CCS are investigated, which are t-diagnosed with repair. The way to determine their state is the modification of the known method of promotion. For CCS with a software-configurable structure, the concept of a diagnostic kernel is concretized, a heuristic decentralized kernel allocation algorithm is described. The efficiency of the proposed self-diagnostic algorithm is shown by the imitation-statistical modeling method. It has been analytically established that, without prejudice to the practical use of it, reverse testing for the connectivity components in stage 1 of the mark H transfer algorithm and the means associated with the formation of the structure G_2^* can be excluded from it.

References

1. Артамонов, Г.Т. Топология сетей ЭВМ и многопроцессорных систем / Г.Т. Артамонов, В.Д. Тюрин. — М.: Радио и связь, 1991. — 248 с.
2. Mariño, P.P. Optimization of Computer Networks: Modeling and Algorithms: A Hands-On Approach 2016. — Pp.1-375. DOI: 10.1002/9781119114840
3. Danilin I.S, Guseev L.I, Zagorodny Y.I. Quality assurance of REA by methods of diagnostics and forecasting. Moskva: Izd. Standards, 1983. — 224 p. [in Russian]
4. Wolf, M. The Physics of Computing, 2016, 1-264
5. Harari F. Theory of graphs. Mir: Moskva, 1973. — 300 p. [in Russian]
6. Koh, K.M., Dong, F., Ng, K.L., Tay, E.G. Graph Theory: Undergraduate Mathematics, 2015. — Pp. 1-479. DOI: 10.1142/9426
7. Gulyaev V.A. Organization of diagnostic systems for computers. Science. Dumka: Kyiv, 1979. — 116 p. [in Ukrainian]
8. Ligeza, A. Towards knowledge compilation for automated diagnosis: A qualitative, model-based approach with constraint programming. Advanced and Intelligent Computations in Diagnosis and Control, 2015. — Pp. 355-367. DOI: 10.1007/978-3-319-23180-8_26
9. Henley E.J., Kumamoto H. Reliability of technical systems and risk assessment. Mechanical Engineering: Moskva, 1984. — 528 p. [in Russian]

10. Verma, A.K., Ajit, S., Karanki, D.R. Reliability and Safety Engineering: Second Edition, 2015. — Pp. 1-571. DOI: 10.1007/978-1-4471-6269-8
11. Todinov, M. Reliability and Risk Models: Setting Reliability Requirements: Second Edition, 2015. — Pp. 1-419. DOI: 10.1002/9781118873199

САМОДІАГНОСТИКА КОМПЛЕКСНИХ СИСТЕМ З ПРОГРАМНО-КОНФІГУРОВАНОЮ СТРУКТУРОЮ

I.B. Коробійчук¹, Р.В. Гришук², В.О. Хорошко³, Ю.Є. Хохлячова³

¹Інститут автоматичного управління та робототехніки, Варшавський технологічний університет, пл. Політехніки, 1, Варшава, 00-661, Польща; e-mail: igor@mchtr.pw.edu.pl

²Житомирський військовий інститут ім. С. Корольова, просп. Миру, 22, корп. ЖВІ, Житомир, 10004, Україна; e-mail: dr.hry@i.ua

³Національний авіаційний університет, просп. Космонавта Комарова, 1, Київ, 03058, Україна; e-mail: professor_va@ukr.net, hohlachova@gmail.com

За допомогою методу імітаційно-статистичного моделювання встановлено працездатність і отримані оцінки ефективності запропонованого алгоритму самодіагностики складних обчислювальних систем з програмно-конфігурованою структурою. Структура складних обчислювальних систем є діаграмою Келі деякої кінцевої абелевих групи дуги в діаграмі Келі мають позначки утворюють групи. Описані графи названі КАІС-графами (графи для надання кінцевих абелевих ізотропних і симетричних структур). Через обмежену кількість міжмодульних зв'язків складних обчислювальних систем для визначення її стану необхідно використовувати робочі зв'язки між модулями. Отже, діагностичний граф G для складних обчислювальних систем є КАІС-граф. Властивість симетричності КАІС-графа означає, що сусідні модулі складних обчислювальних систем є взаємотестуємими. Вірне визначення стану складних обчислювальних систем можливо, якщо воно здійснюється свідомо справними засобами, що є складовими ядра складних обчислювальних систем. Визначимо діагностичне ядро як сукупність засобів, що мають більш високу надійність, ніж система, яка перевіряється з його допомогою. Надійність ядра забезпечується засобами, які не належать системі, що ним перевіряється. Одним з методів автоматизації визначення стану сучасних складних обчислювальних систем є метод розкрутки. На кожному кроці розкрутки справність одних вузлів визначається справністю інших, яка встановлена на попередніх кроках. Процес розкрутки завжди починається з ядра системи. Функціональні характеристики модулів складних обчислювальних систем такі, що будь-який з них можна використовувати в якості ядра. Якщо $t < N$, то завдання визначення стану системи можна уточнити: за результатами взаємної перевірки виявити хоча б один справний модуль. Виявлені модулі використовуються в якості ядра складних обчислювальних систем. Спосіб визначення стану справності модульних живучих складних обчислювальних систем є модифікація відомого методу розкрутки. Для складних обчислювальних систем з програмно-конфігурується структурою конкретизується поняття діагностичного ядра, описаний евристичний децентралізований алгоритм виділення ядра.

Ключові слова: складні обчислювальні системи, діагностична модель, діагностичний граф, алгоритм, витрати на діагностику

**САМОДИАГНОСТИКА КОМПЛЕКСНЫХ СИСТЕМ
С ПРОГРАММНО-КОНФИГУРИРОВАННОЙ СТРУКТУРОЙ**И.В. Коробийчук¹, Р.В. Гришук², В.А. Хорошко³, Ю.Е. Хохлачева³¹Институт автоматического управления и робототехники, Варшавский технологический университет, пл. Политехники, 1, Варшава, 00-661, Польша; e-mail: igor@mchtr.pw.edu.pl²Житомирский военный институт им. С. Королева, просп. Мира, 22, корп. ЖВИ, Житомир, 10004, Украина; e-mail: dr.hry@i.ua³Национальный авиационный университет, просп. Космонавта Комарова, 1, Киев, 03058, Украина; e-mail: professor_va@ukr.net, hohlachova@gmail.com

С помощью метода имитационно-статистического моделирования установлена работоспособность и получены оценки эффективности предложенного алгоритма самодиагностики сложных вычислительных систем с программно-конфигурируемой структурой. Структура сложных вычислительных систем является диаграммой Кэли некоторой конечной абелевой группы дуги в диаграмме Кэли имеют отметки образующих группы. Описанные графы названы КАИС-графами (графы для предоставления конечных абелевых изотропных и симметричных структур). Из-за ограниченного числа межмодульных связей сложных вычислительных систем для определения ее состояния необходимо использовать рабочие связи между модулями. Следовательно, диагностический граф G для сложных вычислительных систем есть КАИС-граф. Свойство симметричности КАИС-графа означает, что соседние модули сложных вычислительных систем взаимотестируемы. Правильное определение состояния сложных вычислительных систем возможно, если оно осуществляется заведомо исправными средствами, составляющими ядро сложных вычислительных систем. Определим диагностическое ядро как совокупность средств, имеющих более высокую надежность, чем проверяемая с его помощью система. Надежность ядра обеспечивается средствами, которые не принадлежат проверяемой им системе. Одним из методов автоматизации определения состояния современных сложных вычислительных систем является метод раскрутки. На каждом шаге раскрутки исправность одних узлов определяется исправностью остальных, которая установлена на предыдущих шагах. Процесс раскрутки всегда начиналась с ядра системы. Функциональные характеристики модулей сложных вычислительных систем таковы, что любой из них можно использовать в качестве ядра. Если $t < N$, то задачу определения состояния системы можно уточнить: по результатам взаимной проверки выявить хотя бы один заведомо исправный модуль. Выявленные модули используются в качестве ядра сложных вычислительных систем. Способом определения состояния исправности модульных живучих сложных вычислительных систем является модификация известного метода раскрутки. Для сложных вычислительных систем с программно-конфигурируемой структурой конкретизируется понятие диагностического ядра, описан эвристический децентрализованный алгоритм выделения ядра.

Ключевые слова: сложные вычислительные системы, диагностическая модель, диагностический граф, алгоритм, затраты на диагностику

СИНТЕЗ И МОДЕЛИРОВАНИЕ КОМБИНИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ С ИЗМЕРЕНИЕМ ВОЗМУЩЕНИЯ ПО МОДЕЛИ ОБЪЕКТА

С.А. Бобриков, Е.Д. Пичугин, А.Г. Кисель

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: bobrikov1932@gmail.com

Проведен синтез системы управления с использованием двух принципов управления: по отклонению и по возмущающему воздействию. Измерение возмущающего воздействия осуществляется косвенно по модели объекта, в которую входит заданная часть системы. Заданная часть включает в себя усилитель мощности – звено первого порядка, и двигатель – звено второго порядка. Выходной сигнал системы управления сравнивается с сигналом на выходе модели. Разность этих сигналов через компенсирующее устройство подается на вход усилителя мощности. В качестве показателей процесса приняты: максимальное перерегулирование в переходной характеристике и время переходного процесса. Схема управляющего устройства и расчет его параметров выполнены с учетом максимальной допустимой величины перегрузки электропривода по моменту вращения при минимальном времени переходного процесса. При расчете управляющего устройства приняты условия, обеспечивающие минимум среднеквадратичного интегрального критерия оптимальности. Показано, что введение в систему компенсирующего устройства уменьшает степень влияния на выходную величину системы управления возмущающего воздействия, приложенного к объекту. Определены структурная схема и параметры компенсирующего устройства, приведены условия устойчивости контура компенсации. Разработана структурная схема системы управления и метод расчета его параметров в аналоговом и в цифровом вариантах. Рассмотрен пример расчета системы и схемы моделирования в системе MATLAB-Simulink при выполнении всех управляющих элементов системы в аналоговой и в цифровой формах.

Ключевые слова: регулятор, система управления, управление по отклонению, управление по возмущающему воздействию, передаточные функции, моделирование, переходная характеристика, показатели качества управления, объект управления, исполнительный механизм, усилитель, обратная связь

Введение

Комбинированные системы управления, в которых используются одновременно два принципа построения системы – по отклонению и по возмущающему воздействию, позволяют существенно снизить зависимость ошибки управления от того возмущающего воздействия, по которому выполнен канал воздействия на управляющее устройство. Для выполнения такого канала необходимо измерить возмущающее воздействие, что во многих случаях выполнить невозможно. В работах [1,2] рассмотрен метод оценки величины возмущающего воздействия со стороны внешней среды путем сравнения сигналов на выходе системы управления с сигналом, полученным на выходе модели системы. При этом в модель системы включены все элементы системы: заданная часть и управляющее устройство. Включение в модель управляющего устройства существенно усложняет модель. При необходимости изменять настройку управляющего устройства нужно соответственно изменять и настройку модели. В данной работе рассмотрен метод построения комбинированной системы управления с

использованием для измерения возмущений модель, в которую включены только объект управления с усилителем мощности.

Цель работы

Целью работы является синтез и моделирование системы управления, с использованием двух принципов управления: по отклонению и по возмущающему воздействию. При этом оценка величины воздействия возмущений на объект управления осуществляется путем сравнения сигналов на выходе объекта и на выходе модели. В модель включены объект и усилитель мощности. Система управления обеспечивает заданные показатели качества в пределах заданного диапазона изменения параметров объекта. В качестве показателей принято минимальное перерегулирование при заданной верхней границе времени переходного процесса.

Основная часть

Обобщенная структурная схема разрабатываемой системы показана на рис. 1, где приняты следующие обозначения: $K_{yy}(p)$ – передаточная функция управляющего устройства; $K_{ym}(p)$ – передаточная функция усилителя мощности; $K_{oy}(p)$ – передаточная функция объекта управления; $K_{ym}^1(p)$ – передаточная функция модели усилителя мощности; $K_{oy}^1(p)$ – передаточная функция модели объекта управления; $K_{ky}(p)$ – передаточная функция компенсирующего звена.

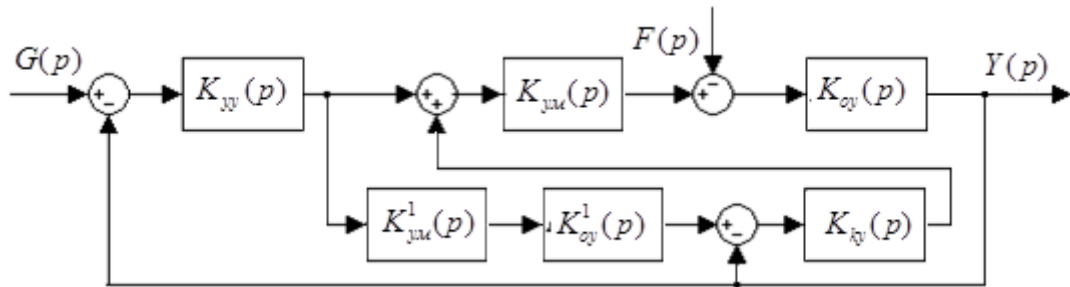


Рис. 1. Структурная схема комбинированной системы управления

Полагаем, что заданная часть системы (усилитель мощности и объект управления) описываются следующими передаточными функциями:

$$K_{ym}(p) = K_{ym}^1(p) = \frac{K_{ym}}{T_{ym}p + 1}, \quad K_{oy}(p) = K_{oy}^1(p) = \frac{K_{oy}}{(T_{oy}p + 1)p}.$$

Определим передаточную функцию, связывающую возмущающее воздействие, приложенное к объекту, с выходной величиной, для чего воспользуемся формулой Мейсона [6]:

$$W_{fy}(p) = \frac{y(p)}{F(p)} = \frac{W_{np}(p)\Delta_{np}(p)}{\Delta(p)}. \quad (1)$$

где $W_{np}(p)$ – передаточная функция прямого пути от точки приложения возмущения до выходной величины; $\Delta(p) = 1 - \sum_i W_{конт.i}(p) + \sum_{i,j} W_{конт.i}(p)W_{конт.j}(p) - \dots, W_{конт.i,j}(p)$ – передаточные функции замкнутых контуров.

В рассматриваемой системе (рис. 1) передаточные функции замкнутых контуров равны:

$$\begin{aligned} W_{конт.1}(p) &= -K_{yy}(p)K_{ym}(p)K_{oy}(p); \quad W_{конт.2}(p) = -K_{ky}(p)K_{ym}(p)K_{oy}(p); \\ W_{конт.3}(p) &= -K_{yy}(p)K_{ym}^1(p)K_{oy}^1(p)K_{ky}(p)K_{ym}(p)K_{oy}(p). \end{aligned} \quad (2)$$

Учитывая, что в формуле Мейсона (1) из произведения контуров исключаются (приравняются нулю) те пары, в которых есть повторение каких-либо одинаковых элементов, а также то, что $\Delta_{np}(p) = \Delta(p)$ за вычетом тех элементов, которые есть в прямом пути, получим передаточную функцию (2), подставив передаточные функции звеньев системы:

$$W_{fy}(p) = \frac{K_{oy}(p)}{\Delta(p)}. \quad (3)$$

Знаменатель данной передаточной функции равен:

$$\begin{aligned} \Delta(p) &= 1 + K_{yy}(p)K_{ym}(p)K_{oy}(p) + K_{ky}(p)K_{ym}(p)K_{oy}(p) + \\ &+ K_{yy}(p)K_{ym}^1(p)K_{oy}^1(p)K_{ky}(p)K_{ym}(p)K_{oy}(p). \end{aligned}$$

Передаточная функция компенсирующего звена $K_{ky}(p)$ входит в $\Delta(p)$, т.е. расположена в знаменателе передаточной функции (3). Очевидно, чем больше будет величина $K_{ky}(p)$, тем в меньшей степени будет влиять возмущающее воздействие $f(t)$ на выходную величину системы $y(t)$. Компенсирующее звено входит в замкнутый контур, тип звена и величины его параметров влияют на динамические свойства контура и всей системы.

Для определения типа звена $K_{ky}(p)$ и его параметров рассмотрим замкнутый контур $W_{конт.2}(p)$:

$$W_{конт.2}(p) = -K_{ky}(p)K_{ym}(p)K_{oy}(p).$$

Характеристическое уравнение этого контура имеет вид:

$$1 + K_{ky}(p)K_{ym}(p)K_{oy}(p) = 0.$$

Подставив передаточные функции усилителя мощности и объекта получим:

$$1 + \frac{K_{ky}(p)K_{ym}K_{oy}}{(T_{ym}p + 1)(T_{oy}p + 1)p} = 0. \quad (4)$$

Принимаем, что передаточная функция компенсирующего звена имеет следующий вид:

$$K_{ky}(p) = \frac{K_{ky}(T_{ym}p + 1)(T_{oy}p + 1)}{(T_d p + 1)(T_d p + 1)}. \quad (5)$$

Постоянные времени T_d в знаменателе (5) необходимы для физической реализуемости звена. Их величина должна быть выбрана на порядок меньше наименьшей величины постоянных времени в заданной части системы. Подставив (5) в (4) получим:

$$1 + \frac{K_{ky}K_{ym}K_{oy}}{(T_d p + 1)(T_d p + 1)p} = 0.$$

Сделав ряд преобразований получим:

$$T_d^2 p^3 + 2T_d p^2 + p + K_{ky}K_{ym}K_{oy} = 0.$$

В соответствии с критерием устойчивости Гурвица, для устойчивости этого контура необходимо выполнение следующего неравенства:

$$T_d^2 K_{ky}K_{ym}K_{oy} < 2T_d.$$

Откуда следует:

$$K_{ky} < \frac{2}{T_d K_{ym}K_{oy}} = K_{kykr}. \quad (6)$$

Очевидно, что если компенсирующее звено имеет передаточную функцию (5), то для уменьшения влияния возмущающего воздействия на выходную величину нужно увеличивать коэффициент усиления K_{ky} , но при этом величина этого коэффициента должна быть меньше его критического значения (6).

Для разработки управляющего устройства воспользуемся методом, рассмотренным в [3,4]. В соответствии с [4] принимаем условие – передаточная функция контура $W_{конт.1}(p)$ равна:

$$W_{конт.1}(p) = K_{yy}(p)K_{ym}(p)K_{oy}(p) = \frac{K_c(T_y p + 1)}{p^2}. \quad (7)$$

Как показано в [4], если передаточная функция разомкнутой системы имеет вид (7), то произведение $K_c T_y$ в относительных единицах равно ускорению выходной величины в момент подачи на вход системы ступенчатого сигнала. В момент включения ускорение выходной величины системы имеет наибольшее значение и произведение $K_c T_y$ численно равно перегрузке электропривода по моменту вращения λ . Из этого следует: $K_c T_y = \lambda$.

Из равенства (7) следует:

$$K_{yy}(p) = \frac{K_c(T_y p + 1)}{p^2 K_{ym}(p)K_{oy}(p)} = \frac{K_c(T_y p + 1)(T_{ym} p + 1)(T_{oy} p + 1)}{K_{ym}K_{oy} p}.$$

Окончательно принимаем передаточную функцию управляющего устройства следующего вида:

$$K_{yy}(p) = \frac{K_y(T_y p + 1)(T_{ym} p + 1)(T_{oy} p + 1)}{(T_d p + 1)^2 p}, \quad K_y = \frac{K_c}{K_{ym} K_{oy}}. \quad (8)$$

В формуле (8) дополнительные постоянные времени T_d введены для выполнения условия физической реализуемости устройства управления. Величина их должна быть на порядок меньше наименьшей постоянной времени в заданной части системы. Параметры T_y и K_c определяются по заданным показателям качества системы: максимальное перерегулирование в переходной характеристике и время переходного процесса [4], а также по заданной величине максимальной перегрузки по моменту вращения λ .

Последовательность расчёта системы рассмотрим на примере. Пусть передаточные функции заданной части системы равны:

$$K_{ym}(p) = \frac{0,5}{0,1p + 1}; \quad K_{oy}(p) = \frac{0,2}{(0,5p + 1)p}.$$

Принимаем условия:

1. Максимально допустимая перегрузка привода по моменту вращения равна $\lambda = 2,5$.

2. Максимальная величина перерегулирования $\sigma_{\max} \leq 5\%$.

Из графика, приведенного на рис. 2 [4] для заданной величины $\sigma_{\max} = 5\%$ определяем $K_c T_y^2 : K_c T_y^2 = 15$. $K_c T_y = \lambda = 2,5$. Определяем параметры управляющего

устройства: $T_y = \frac{K_c T_y^2}{K_c T_y} = \frac{15}{2,5} = 6$; $K_c = \frac{2,5}{6} = 0,4$. Коэффициент усиления управляющего

устройства равен: $K_y = \frac{K_c}{K_{ym} K_{oy}} = \frac{0,4}{0,5 \times 0,2} = 4$. Определим критическое значение

коэффициента усиления компенсирующего устройства (6):

$$K_{kyp} = \frac{2}{T_d K_{ym} K_{oy}} = \frac{2}{0,01 \times 0,5 \times 0,2} = 2000. \text{ Принимаем } K_{ky} = 1000.$$

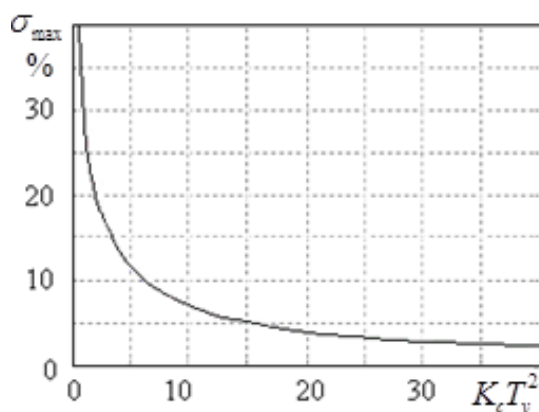


Рис. 2. Зависимость максимального перерегулирования в переходной характеристике от $K T^2$

Данная система промоделирована в системе MATLAB-Simulink [7] при выполнении всех элементов управления (управляющее устройство, модель заданной части системы и компенсирующее устройство) на аналоговых элементах (рис. 3) и в цифровом исполнении (рис. 4).

Для преобразования аналоговых передаточных функций управляющих элементов системы в цифровые использована подстановка в аналоговые передаточные функции выражения [7,8]

$$p = \frac{2(z-1)}{T_0(z+1)}, \quad (9)$$

где T_0 – шаг квантования непрерывных сигналов в дискретные. Для обеспечения адекватности дискретной системы с исходной непрерывной $T_0 \leq 0,5T_{\min}$, $T_{\min}$ – минимальная постоянная времени в непрерывной передаточной функции.

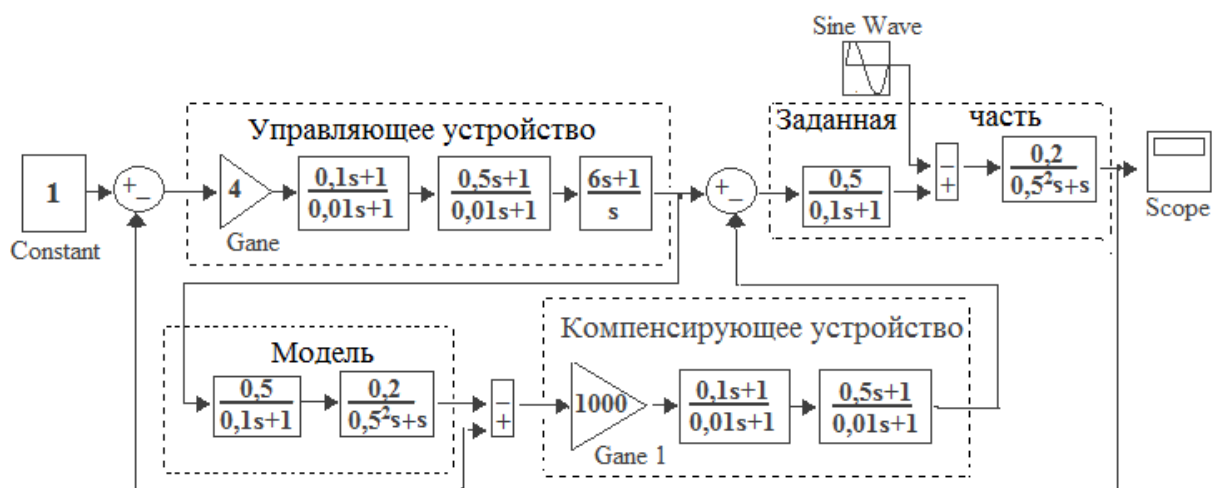


Рис. 3. Схема модели системы с аналоговыми элементами управления

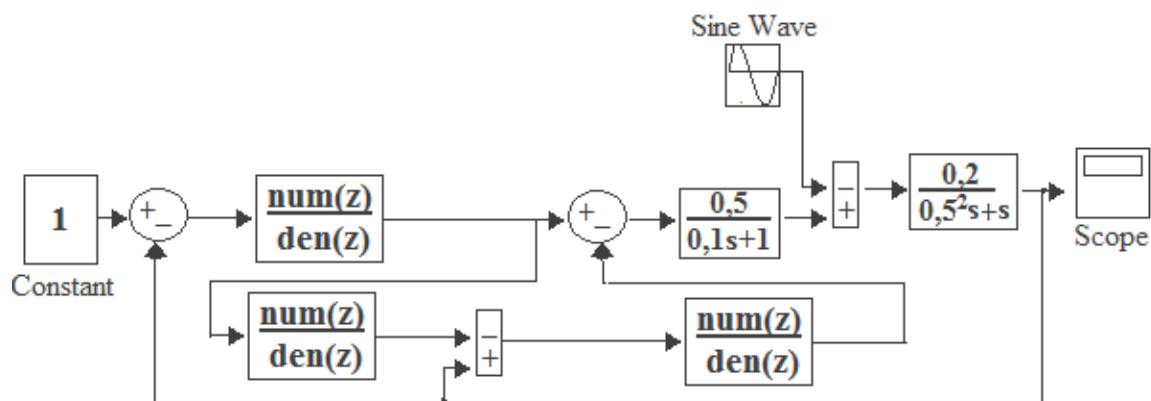


Рис. 4. Схема модели системы с цифровыми элементами управления

Определение дискретных передаточных функций элементов управления.

1. Управляющее устройство.

Аналоговая передаточная функция равна:

$$K_{yy}(p) = \frac{4(0,1p+1)(0,5p+1)(6p+1)}{(0,01p+1)^2 p}.$$

Сделав подстановку (9), получим дискретную передаточную функцию управляющего устройства:

$$K_{yy}(z) = \frac{s_3 z^3 + s_2 z^2 + s_1 z + s_0}{g_3 z^3 + g_2 z^2 + g_1 z + g_0}, \quad (10)$$

где $s_3 = 9,8933205$; $s_2 = 29,0906785$; $s_1 = 28,506681$; $s_0 = 9,3093195$; $g_3 = 0,00125$; $g_2 = -0,00275$; $g_1 = 0,00195$; $g_0 = -4,5e-0,4$. $T_0 = 0,005$ с.

2. Модель заданной части системы.

Аналоговая передаточная функция равна:

$$K_M(p) = K_{ym}(p)K_{oy}(p) = \frac{0,1}{(0,1p + 1)(0,5p + 1)p}.$$

Дискретная передаточная функция имеет вид (10), её коэффициенты равны: $s_3 = 1,25e-8$; $s_2 = 3,75e-8$; $s_1 = 3,75e-8$; $s_0 = 1,25e-8$; $g_3 = 0,41205$; $g_2 = -1,21195$; $g_1 = 1,18795$; $g_0 = -0,38805$. $T_0 = 0,005$ с.

3. Компенсирующее устройство.

Аналоговая передаточная функция равна:

$$K_{ky}(p) = \frac{1000(0,1p + 1)(0,5p + 1)}{(0,01p + 1)(0,01p + 1)}.$$

Дискретная передаточная функция имеет вид:

$$K_{ky}(z) = \frac{s_2 z^2 + s_1 z + s_0}{g_2 z^2 + g_1 z + g_0},$$

где $s_2 = 206,025$; $s_1 = 399,95$; $s_0 = 194,025$; $g_2 = 6,25e-4$; $g_1 = -7,5e-4$; $g_0 = 2,25e-4$. $T_0 = 0,005$ с.

Результаты моделирования приведены на рис. 5. Кривая *a* – переходная характеристика при условии, что к объекту приложено гармоническое возмущающее воздействие, компенсирующее устройство включено; кривая *b* – компенсирующее устройство отключено. Результаты моделирования по схеме рис. 3 и по схеме рис. 4 практически полностью совпадают.

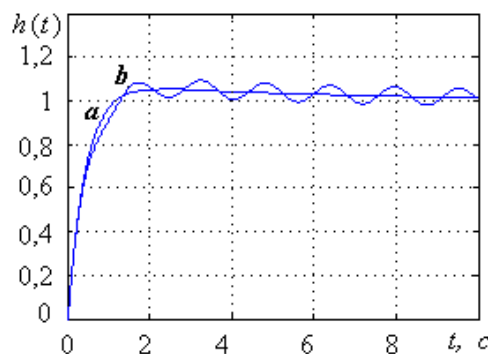


Рис. 5. Результаты моделирования: *a* – компенсирующее устройство включено; *b* – компенсирующее устройство отключено

Выводы

Разработана комбинированная система управления, в которой используется принцип управления по отклонению и принцип управления по возмущающему воздействию. Рассмотрен случай, когда возмущающее воздействие приложено к объекту управления. Для измерения возмущающего воздействия использована модель, включающая объект управления и усилитель мощности. Проведен расчет системы с определением передаточных функций управляющего устройства, модели и компенсирующего устройства. Разработанный метод расчета позволяет рассчитать систему по заданным показателям качества – максимальное перерегулирование и время переходного процесса при условии высокой степени компенсации возмущающего воздействия, приложенного к объекту управления. Результаты проведенного моделирования подтверждают эффективность разработанного метода.

Список литературы

1. Бобриков, С.А. Компенсация возмущений с использованием модели системы автоматического управления для измерения возмущений / С.А. Бобриков, Е.Д. Пичугин // Электротехнические и компьютерные системы. — К.: Техніка, 2011. — С.15-18.
2. Бобриков, С.А. Компенсация волновых возмущений в системе автоматического управления курсом судна / С.А. Бобриков, Е.Д. Пичугин // Электротехнические и компьютерные системы. — К.: Техніка, 2012. — № 05 (81). — С. 119-124.
3. Бобриков, С.А. Цифровой регулятор в системе управления с астатизмом второго порядка / С.А. Бобриков, Е.Д. Пичугин // Электротехнические и компьютерные системы. — К.: Техніка, 2013. — № 12 (88). — С. 55-60.
4. Бобриков, С.А. Оптимальная настройка цифрового регулятора для системы управления с астатизмом второго порядка / С.А. Бобриков, Е.Д. Пичугин, Б.Б. Бабийчук // Электротехнические и компьютерные системы. — К.: Техніка, 2015. — №17(93).—С.80-86.
5. Бобриков, С.А. Преобразование непрерывной передаточной функции управляющего в дискретную / С.А. Бобриков, Е.Д. Пичугин // Электротехнические и системы. — К.: Техніка, 2013. — № 10 (86). — С. 68-73
6. Бесекерский, В.А. Теория систем автоматического регулирования / В.А. Бесекерский, Е.П. Попов. — М.: Наука, 1972. — С. 695-719.
7. Краснопрошина, А.А. Современный анализ систем управления с применением MATLAB, Simulink, ControlSistem / А.А. Краснопрошина, Н.Б. Репникова, А. Ильченко. — К.: Корнійчук, 1999. — 141с

СИНТЕЗ І МОДЕЛЮВАННЯ КОМБІНОВАНОЇ СИСТЕМИ УПРАВЛІННЯ З ВИМІРЮВАННЯМ ЗБУРЕННЯ ПО МОДЕЛІ ОБ'ЄКТА

С.А. Бобриков, Е.Д. Пичугин, А.Г. Кисель

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

Проведено синтез системи управління з використанням двох принципів управління: по відхиленню і по впливі, що обурює. Вимірювання впливу, що обурює здійснюється побічно за моделлю об'єкта, в яку входить задана частина системи. Задана частина включає в себе підсилювач потужності – ланка першого порядку, і двигун – ланка другого порядку. Вихідний сигнал системи управління порівнюється з сигналом на виході моделі. Різниця цих сигналів через компенсуючий пристрій подається на вхід підсилювача потужності. Як показники процесу прийняті: максимальне перегулювання в перехідній характеристиці і час перехідного процесу. Схема керуючого пристрою і розрахунок його параметрів виконані з урахуванням максимальної допустимої величини перевантаження електроприводу по моменту обертання при мінімальному часу перехідного процесу. При розрахунку керуючого пристрою прийняті умови, що забезпечують мінімум середньоквадратичного інтегрального критерію оптимальності. Показано, що введення в систему компенсуючого пристрою зменшує ступінь впливу на вихідну величину системи управління обурюваного впливу, прикладеного до об'єкту. Визначено структурну схему та параметри компенсуючого пристрою, наведені умови стійкості контуру компенсації. Розроблено структурну схему системи управління і метод розрахунку його параметрів в аналоговому і в цифровому варіантах. Розглянуто приклад розрахунку системи і схеми моделювання в системі MATLAB-Simulink при виконанні всіх керуючих елементів системи в аналоговій і в цифровій формах.

Ключові слова: регулятор, система управління, управління по відхиленню, управління по впливі, що обурює, передавальні функції, моделювання, перехідна характеристика, показники якості управління, об'єкт управління, виконавчий механізм, підсилювач, зворотний зв'язок

SYNTHESIS AND SIMULATION OF COMBINED CONTROL SYSTEMS WITH MEASUREMENT OF PERTURBATION BY MODEL OF THE OBJECT

S.A. Bobrykov, E.D. Pichugin, A.G. Kisel

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

The control system is synthesized using two control principles: deviation and perturbation. Measurement of the disturbing effect is carried out indirectly by the model of the object into which the given part of the system enters. The predetermined portion includes a power amplifier, a first-order unit, and an engine - second-order link. The output signal of the control system is compared with the signal at the output of the model. The difference of these signals through the compensating device is fed to the input of the power amplifier. As indicators of the process, the maximum overshoot in the transient response and the transient time are adopted. The circuit of the control device and the calculation of its parameters are made taking into account the maximum permissible value of the electric drive overload at the moment of rotation with the minimum time of the transient process. When calculating the control device, conditions are adopted that ensure a minimum of the root-mean-square integral optimality criterion. It is shown that the introduction of a compensating device into the system. It is shown that the introduction of a compensating device into the system reduces the degree of influence on the output value of the control system of the disturbing effect applied to the object. The structural scheme and parameters of the compensating device are determined, the stability conditions of the compensation circuit are given. A structural diagram of the control system and a method for calculating its parameters in the analog and digital versions are developed. An example of calculation of the system and modeling circuit in the MATLAB-Simulink system is considered when all control elements of the system are executed in analog and digital forms.

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

ПРОГНОЗУВАННЯ ТЕХНІЧНОГО СТАНУ ОДНОТИПНИХ ПРОГРАМНО-АПАРАТНИХ ЗАСОБІВ

В.В. Кузавков, П.В. Хусаїнов

Військовий інститут телекомунікацій та інформації імені Героїв Крут,
вул. Московська, 45/1, Київ, 01011, Україна; e-mail: nevse@ukr.net

Розглянуто підходи, засновані на фізичних передумовах до прогнозування технічного стану (визначення ресурсу) радіоелектронних об'єктів, які потрапляють під визначення «однотипні програмно-апаратні засоби». Прогнозування технічного стану радіоелектронного обладнання (РЕО) – важлива складова частина теорії надійності, а показники «ресурс» і «термін служби» є одними з основних понять цієї теорії. Особливе місце має задача прогнозування ресурсу (визначення часу до досягнення критичного стану) РЕО на стадії експлуатації. Дана задача пов'язана з оцінкою поточного стану та його прогнозом на майбутнє, оцінкою ймовірностей настання відмов, ризику аварійних ситуацій. На основі прогнозу встановлюється термін чергового контролю стану РЕО або призначається гранично-допустимий термін експлуатації. Процес прогнозування принципово можливий в разі наявності діагностичного параметру (ДП), який відповідає умовам вимірюваності, інваріантності до впливу завад, інформативності, а також адекватної діагностичної моделі об'єкту контролю, (яка встановлює зв'язок між простором стану технічного пристрою і простором діагностичних ознак). В статті розглядається вирішення завдань технічної діагностики для сукупності технічних засобів прийому, передачі збереження та обробки інформації під управлінням програмної складової зазначеного технічного об'єкту. Застосування фізичних передумов функціонування РЕО для оцінки ресурсу технічних засобів радіоелектроніки стало можливим з появою та розвитком теорії дефектоутворення в напівпровідникових структурах, виникненням нових методів збору діагностичної інформації на основі стохастичних процесів зміни струму в напівпровідникових структурах в залежності від часу напруження. Запропоновано діагностичну модель, яка враховує швидкі та повільні процеси у об'єкту контролю, розглянуто теоретичні та практичні питання прогнозування ресурсу РЕО.

Ключові слова: прогнозування, діагностичний параметр, фізико-хімічні процеси, радіоелектронне обладнання, діагностична модель

Вступ

Прогнозування технічного стану – процес визначення технічного стану об'єкту на майбутній період часу, що заснований на застосуванні методів екстраполяції явищ на майбутній час за відомими результатами спостережень (за відповідними явищами в попередній період).

Параметрами, які використовуються для прогнозування, можуть бути:

- експлуатаційні параметри, що вимірюються штатними приладами (застосовується функціональна діагностика) без виведення обладнання з експлуатації;
- параметри технічного стану, що вимірюються зовнішнім устаткуванням (автономними автоматизованими системами діагностування) із зупинкою обладнання, частковим або повним розбиранням.

В процесі функціонування радіоелектронного обладнання (РЕО) в умовах прийнятої планово-попереджувальної стратегії технічного обслуговування і ремонту прогноз технічного стану з суто теоретичного питання (прогноз остаточного ресурсу устаткування) переходить до практичного аспекту: чи здатне функціонувати

устаткування до наступного терміну планових регламентних робіт. Інакше кажучи, період прогнозування технічного стану (ТС) цілком визначений. Необхідно мати відповідь на питання: чи збережеться працездатний стан об'єкту контролю до моменту наступного контролю функціонування (регламентних робіт) [1,2].

Існує два основних напрямки визначення ресурсу об'єкту: напрямок, заснований на імовірносних методах оцінки, та заснований на фізичних передумовах функціонування об'єкту контролю [3-5].

Застосування імовірнісних методів оцінки ресурсу вимагає виконання умови статистичної стійкості [5]. Оцінка ресурсу унікального обладнання, існуючого в одиничному виконанні або в умовах обмеженої кількості таких зразків, є завданням індивідуального прогнозування, коли передбачається поведінка окремо взятого виробу за певний період часу. В цьому випадку не виконуються умови статистичної стійкості, використання імовірнісних методів сумнівно.

Застосування фізичних передумов функціонування РЕО для оцінки ресурсу до недавнього часу не дозволяло врахувати різноманіття реальних умов експлуатації [3]. Ситуація змінилася з появою нових досягнень в області технічної діагностики. Розвиток теорії дефектоутворення в напівпровідникових структурах, виникнення нових безконтактних методів збору інформації, реєстрації значень діагностичного параметру на основі стохастичних процесів зміни струму в напівпровідникових структурах дозволяють не лише вирішувати дві основні задачі технічної діагностики – визначення технічного стану і локалізація несправності, а й впритул підійти до вирішення третьої задачі – прогнозування технічного стану об'єктів РЕО [6,7].

Результати, отримані в ході проведення прискорених випробувань типових радіoeлектронних компонентів (РЕК) в рамках розвитку теорії дефектоутворення у напівпровідникових структурах, дозволили з високою вірогідністю підтвердити адекватність математичних моделей РЕК, ефективність і придатність діагностичного параметра на основі стохастичних процесів зміни струму для прогнозування технічного стану сучасних радіoeлектронних компонентів та програмно-апаратних засобів на їх основі [8,9].

Мета роботи

В статті розглядаються особливості вирішення завдань технічної діагностики для об'єктів, які підпадають під визначення «однотипних програмно-апаратних засобів», а саме сукупність технічних засобів прийому, передачі, збереження та обробки даних під управлінням (керівництвом) програмної складової (сукупність технічних засобів РЕО, які є практичною реалізацією моделі OSI).

Метою роботи є доведення узагальненої схеми діагностичної моделі одного з видів радіoeлектронного устаткування (озброєння) – однотипних програмно-апаратних засобів та підходів до визначення їх ресурсу (прогнозування), заснованих на фізичних передумовах функціонування таких об'єктів; представлення варіантів практичного визначення ресурсу технічних засобів РЕО в залежності від обсягу наявної інформації.

Основна частина

Відомо, що однією з задач, які вирішуються технічною діагностикою на рівні з визначенням технічного стану та пошуком несправностей, є прогнозування технічного стану об'єкту контролю. Отримані дані застосовуються при експлуатації з метою попередження аварійних станів або при виході з ладу для скорочення часу відновлення. Враховуючи особливості запропонованого об'єкту контролю (кількісну розмірність, територіальне рознесення, різноманіття технічних засобів), прийняття рішення на

відновлення працездатного стану в реальному часі неможливо без застосування автоматизованих систем та заздалегідь підготовленого плану відновлювальних робіт. Тому в автоматизованій системі діагностування застосовуються елементи системи підтримки прийняття рішень. Структурна схема, що представлена на рис. 1, пояснює процес діагностування визначеного класу устаткування (зазначеного об'єкту контролю).

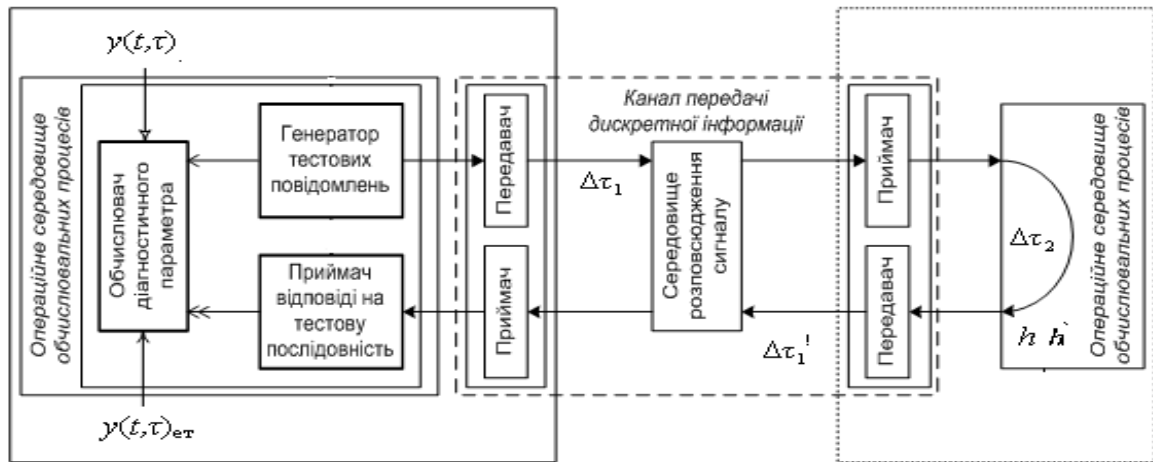


Рис. 1. Узагальнена схема проходження тестових послідовностей у системі однотипних програмно-апаратних засобів

На рис. 1 позначено напрямки проходження спеціально підготовлених тестових повідомлень та основні складові енергетично-часового діагностичного параметру, а саме: $y(t, \tau)$, $y(t, \tau)_{\text{ет}}$ – діагностичний параметр та еталонне значення діагностичного параметру (ДП), які залежать від конструктивних параметрів: $\dot{h}$ – апаратної складової об'єкту контролю, амплітудної та фазочастотної характеристики тракту формування (АЦП, ЦАП перетворень) та передачі тестових повідомлень; t – час напрацювання об'єкту контролю; τ – тривалості перевірних тестових послідовностей; $\Delta\tau_{\Sigma} = \Delta\tau_1 + \Delta\tau_2 + \Delta\dot{\tau}_1$ – сумарне приращення часу; $\Delta\tau_1 \Delta\dot{\tau}_1$ – часове приращення, пов'язане з функціонуванням апаратної частини об'єкту контролю; $\Delta\tau_2$ – приращення часу, яке характеризує затримки, обумовлені дисципліною обслуговування (обробки) тестових повідомлень у термінах теорії масового обслуговування, вплив параметрів налаштування операційного середовища h .

Слід відзначити, що складова $\Delta\tau_2$ також відображує в собі параметри апаратної частини $\dot{h}$ (обсяг пам'яті, частота процесору, частота опитування пристроїв вводу-виводу і т. ін.), оскільки обчислювальні процеси виконуються відповідною складовою апаратної частини.

Нехай основні функціональні властивості об'єкту контролю характеризуються оператором L , який пов'язує вхідні і вихідні сигнали $U_{\text{вх}}(t)$ і $U_{\text{вих}}(t)$, конструктивні параметри $h, \dot{h}$, а також враховує залежність вихідного сигналу $U_{\text{вих}}(t)$ від фактору збудження $\Delta U(t, \tau)$, який, в свою чергу, породжений спеціально підготовленим вхідним перевірним тестом та має ознаки тривалих (t) та швидких (τ) процесів.

Показник функціонування об'єкту контролю – діагностичний параметр $y(t, \tau)$ (зміна технічного стану РЕО контролюється за стохастичними змінами струму, який протікає в шині живлення об'єкту контролю) [6] залежить не тільки від конструктивних параметрів h та перевірних тестів тривалістю τ , а і від часу функціонування об'єкту

контролю t та пов'язаними з ним фізико-хімічними процесами в напівпровідникових структурах та компонентах об'єкту контролю.

Узагальнена схема діагностичної моделі представлена на рис .2.

Визначений тип об'єкту контролю (діагностування) складається з взаємопов'язаних частин: апаратної (конструктивні параметри $\dot{h}$) та програмної, яка визначає алгоритм функціонування апаратної частини (конструктивні параметри h). Тому запропоновано діагностичний параметр, який складається з двох складових: перша – енергетична на основі стохастичних процесів зміни струму, друга – часова для відображення часу (зміни часу) виконання елементарних функцій при опрацюванні вхідної тестової послідовності.

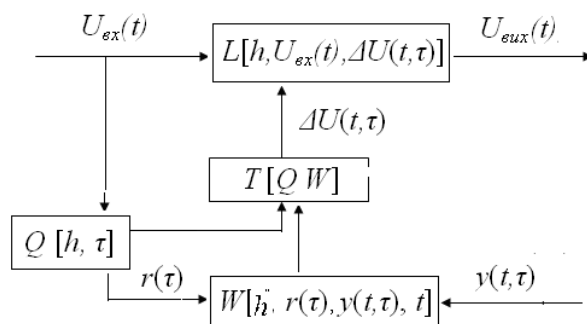


Рис. 2. Узагальнена схема діагностичної моделі

Оператор Q пов'язує між собою конструктивні параметри h (склад програмних модулів або елементарних функцій) та вхідні перевірні тести (з тривалістю τ).

Параметр $r(\tau)$ відображає вплив програмної складової на апаратну складову об'єкту контролю.

Оператор W пов'язує між собою конструктивні параметри $\dot{h}$ (склад апаратної частини), вплив керуючої програмної складової $r(\tau)$, та енергетичну складову діагностичного параметру $y(t, \tau)$.

Оператор T введено для мультиплексування (поєднання) та відображення внеску обох конструктивних параметрів об'єкту контролю $\dot{h}, h$ (програмного та апаратного) у фактор збудження $\Delta U(t, \tau)$ (поєднання операторів операторами Q та W).

Зміна струму, енергетичної складової ДП в результаті старіння (за часом) відбувається значно повільніше, в порівнянні з флуктуаціями основних експлуатаційних (функціональних) показників. Динаміка зміни діагностичного параметру розглядається протягом усього життєвого циклу РЕО.

Отже, представлена модель враховує два види процесів, які відбуваються в тракці проходження тестових повідомлень: швидкі τ – флуктуація експлуатаційних (функціональних) показників і повільні t – розвиток дефектів в напівпровідникових структурах. Швидкі процеси визначають технічний стан об'єкта контролю на момент діагностування (в момент часу контролю), а повільні – параметричну надійність об'єкту контролю.

Залежно від математичного апарату, який застосовується, в теорії розрізняють: експертні оцінки; аналітичні оцінки (розрахунки); імовірнісні, коли в результаті прогнозування визначається ймовірність виходу (невиходу) параметру або параметрів ТС за допустимі межі; статистична класифікація (розпізнавання образів), коли в наслідок прогнозування визначається клас об'єкту, який діагностується за критерієм працездатності [3,5].

Серед параметрів технічного стану (ПТС) розрізняють прямі (безпосередньо характеризують конкретні властивості об'єкту або його складової частини) і непрямі

(параметр ТС, пов'язаний з прямим ПТС детермінованою або стохастичною залежністю) параметри.

Прогнозування ресурсу виробу за непрямыми параметрами засноване на врахуванні наступних умов:

- відомі фізичні процеси, які призводять до ресурсних відмов, а також математичні моделі зміни прямих (структурних) і непрямих (діагностичних) параметрів;
- для кожного прямого ПТС встановлені граничні значення, досягнення яких визначає величину ресурсу за цим параметром;
- в процесі спостереження за зміною технічного стану виробу є можливість фіксації параметрів, які відображають індивідуальні особливості об'єкту контролю;
- існує інформація про функціональні або регресійні співвідношення між прямими і непрямыми ПТС;
- залежність між математичними очікуваннями прямих і непрямих ПТС є монотонною і неперервною.

У випадку прогнозування технічного стану однотипних програмно-апаратних засобів визначення ресурсу (за непрямыми ПТС) супроводжується трьома видами похибок: похибками вимірювання непрямих параметрів; похибками, пов'язаними з випадковою природою фізичних процесів розвитку відмов; методичними похибками визначення прямих ПТС за значеннями непрямих. При цьому, залежно від обсягу наявної інформації щодо об'єкту контролю, можливі три групи типових ситуацій.

Перша група:

- відомий вид функції F , яка визначає зв'язок між прямим і непрямым параметрами, та усі коефіцієнти і дисперсії цих коефіцієнтів;
- існують результати періодичних вимірювань непрямого параметру.

Друга група:

- вид функції F відомий, коефіцієнти невідомі;
- існують результати періодичних вимірювань непрямого параметру та результати навчального експерименту, в процесі якого відбувається одночасне вимірювання прямого і непрямого ПТС.

Третя група:

- функція F монотонна і неперервна (загальний вид невідомий);
- існують результати навчального експерименту.

Дисперсія оцінки ресурсу представлена у вигляді суми трьох доданків:

- похибки вимірювань;
- похибки визначення коефіцієнтів функції F ;
- похибки визначення дисперсії випадкової зміни збільшення параметру контролю.

Застосування відомих співвідношень ускладнюється необхідністю значного обсягу попередніх досліджень для встановлення вихідних даних.

Найбільш доступним для практичного використання є метод, заснований на степеневій апроксимації зміни ПТС для прогнозування процесів погіршення технічного стану об'єкту контролю.

Математичний опис процесу зміни параметру технічного стану $Y(t)$ ґрунтується на апроксимації кожної реалізації цього процесу випадковою функцією виду:

$$Y(t) = Kt^{\alpha} + z(t),$$

де K – випадкове для групи однойменних складових частин, але незмінне значення показника швидкості зміни діагностичного параметру для кожної реалізації випадкового процесу; α – показник ступеню функції апроксимації, який характеризує

конструктивні особливості складової частини об'єкту контролю; $z(t)$ – нормальний стаціонарний випадковий процес відхилень фактичних значень параметру контролю від апроксимуючої степеневі функції кожної реалізації процесу $Y(t)$.

Статистичні характеристики випадкового процесу $z(t)$ (при $t > 0,3T_{cp}$) наступні:

$$M[z(t)] = 0;$$

$$D[z(t)] = \sigma^2;$$

$$R[z(t), z(t + \Delta t)] = R(\Delta t);$$

$$f[z(t_k)] = \frac{1}{\sqrt{2\pi}\sigma} \exp\left[-\frac{z^2(t_k)}{2\sigma^2}\right],$$

Середній ресурс складової частини об'єкту контролю обчислюють на основі інформації про зміну параметра її технічного стану Y_k і про напрацювання t_k до моменту контролю за наближеною формулою:

$$t^{cp} = t_k \left[\left(\frac{Y_n}{Y_k} \right)^{1/2} - 1 \right] K_t.$$

При $s < 0,03Y_n$ можливо не враховувати поправочний коефіцієнт K_t .

Запропонований метод забезпечує необхідну точність оцінки в тому випадку, якщо зміна параметру технічного стану до моменту контролю становить не менше половини граничного відхилення параметра Y_n та при дотриманні умови $t_p < 0,5t_k$. При виконанні наведених умов похибка прогнозування не перевищує 8-9%.

Описаний підхід (метод) може бути використано для лінійного

$$Y(t) = C_1 + C_{2t}, \quad (1)$$

квадратичного

$$Y(t) = C_1 + C_{2t} + C_{3t}, \quad (2)$$

та експонентного

$$Y(t) = \exp\{C_1 + C_{2t}\} \quad (3)$$

законів зміни діагностичного параметру. Коефіцієнти C_1, C_2, C_3 – невідомі.

Для використання методу необхідно переконатися в тому, що зміна контрольованого параметра підпорядковується одному із законів (1-3), а його дисперсія не змінюється зі збільшенням напрацювання виробу.

Показник Y_i оцінюється за вимірними значеннями контрольованого параметру

$$Y_i = F(t_i) + D_i, i = \overline{1, N},$$

де t_i – значення напрацювання в i -й час.

Кількість вимірів N обирають з умови: $N > 2m$, де m – кількість невідомих коефіцієнтів закону зміни діагностичного параметру.

Моменти вимірювань t_i обирають таким чином, щоб випадкові величини D_i були незалежними.

Теоретичним підґрунтям методу є оцінка відповідних показників за методом найменших квадратів. Можлива послідовність розрахунків наступна:

1. Здійснюються N вимірювань діагностичного параметру $Y_i, i = \overline{1, N}$ в певні моменти часу t_i .

2. Обчислюються величини: $Y_1 = \sum Y_i; Y_2 = \sum t_i Y_i; X_1 = \sum t_i; X_2 = \sum t_i^2;$
 $D = N \sum t_i^2 - (\sum t_i)^2; D_{22} = N/D; D_{11} = \sum t_i/D; D_{12} = D_{21} = -\sum t_i/D,$ де $\sum$ – сума по i від 1 до N .

3. Обчислюються крапкові оцінки коефіцієнтів закону (1-3).

4. Обчислюється оцінка середнього квадратичного відхилення діагностичного параметру: $\sigma = \sqrt{S/(N-2)},$ де $S = S(Y_i - C_1 - C_2 * t_i)^2$.

5. Обчислюються оцінки – середні квадратичні відхилення коефіцієнтів C_1 та C_2 :
 $\sigma_1 = \sigma \sqrt{D_{11}}; \sigma_2 = \sigma \sqrt{D_{22}}.$

6. Обчислюються гарантовані оцінки коефіцієнтів: $C_j = C_j \pm K \times s_j, j=1;2,$
 “+” – для випадку коли параметр зростає, “-” – для випадку коли параметр зменшується; g – довірна ймовірність; при $g = 0,9, K = 1,282;$ при $g = 0,95, K = 1,6459;$ при $g = 0,99, K = 2,326;$

7. Обчислюється очікуваний ресурс та гарантований остаточний ресурс:
 $T_{cp} = \frac{(Y_{II} - C_1)}{C_2} - t_k; T_g = \frac{(Y_{II} - C_1)}{C_2} - t_k,$ де t_k – напрацювання на момент останнього контролю.

Основні результати. Організаційно будь-який засіб РЕО в Збройних Силах України супроводжується комплектом технічної документації (в паперовому вигляді та з відповідним обліком). Такий підхід не тільки закріплює персональну відповідальність за експлуатацію технічних засобів, але й забезпечує безперервний облік напрацювання (безперервний збір та облік статистичних даних, необхідних для прогнозування). Однак в сучасних умовах все частіше постачаються технічні засоби закордонного виробництва. При цьому, як правило, відсутня технічна документація, в якій присутній облік напрацювання. Обидва типи технічних засобів повинні функціонувати в єдиній прийнятій планово-попереджувальній системі технічного обслуговування та ремонту.

Розглянемо два варіанти практичного визначення ресурсу технічних засобів РЕО:

– характерний для нових зразків техніки, отриманих безпосередньо із заводу виробника – прогнозування ресурсу при відомому напрацюванні від початку експлуатації;

– характерний для зразків, які перебували на озброєнні при невідомому напрацюванні від початку експлуатації.

Обидва варіанти передбачають наявність та функціонування автоматизованої системи діагностування з елементами системи прийняття рішень.

У роботах [8,9] наведено порівняння (умови проведення порівняння) результатів натурних випробувань з результатами аналітичних досліджень діагностичних моделей РЕК, з яких складаються сучасні зразки РЕО, для подальшого використання при вирішенні завдань технічної діагностики. Аналітична модель радіоелектронного компоненту (РЕК) (модель зміни діагностичного параметру) отримана з урахуванням фізико-хімічних процесів, які відбуваються в напівпровіднику протягом часу його експлуатації. Результатом натурних випробувань (форсованих випробувань), в основі яких лежить сукупність теоретично та експериментально обґрунтованих

закономірностей та допущень, є математичне очікування динаміки зміни діагностичного параметру. Внаслідок порівняння результатів, отриманих аналітично та експериментально, визначено ступінь їх подібності з урахуванням відносної похибки моделювання. Закономірність зміни енергетичної складової діагностичного параметру наведено на рис. 2.

В свою чергу, часова складова, запропонованого для програмно-апаратних засобів діагностичного параметру, також має певну динаміку змін, яка залежить від параметрів перевірного тесту.

Спрощені графічні залежності динаміки зміни діагностичного параметру, для наочного представлення процедури визначення ресурсу, наведені на рис. 3, використовуються наступні позначення: $I_{\text{дп}}$ – енергетична складова діагностичного параметру (струм), $t_{\text{кр}}$ – критичний час напруження.

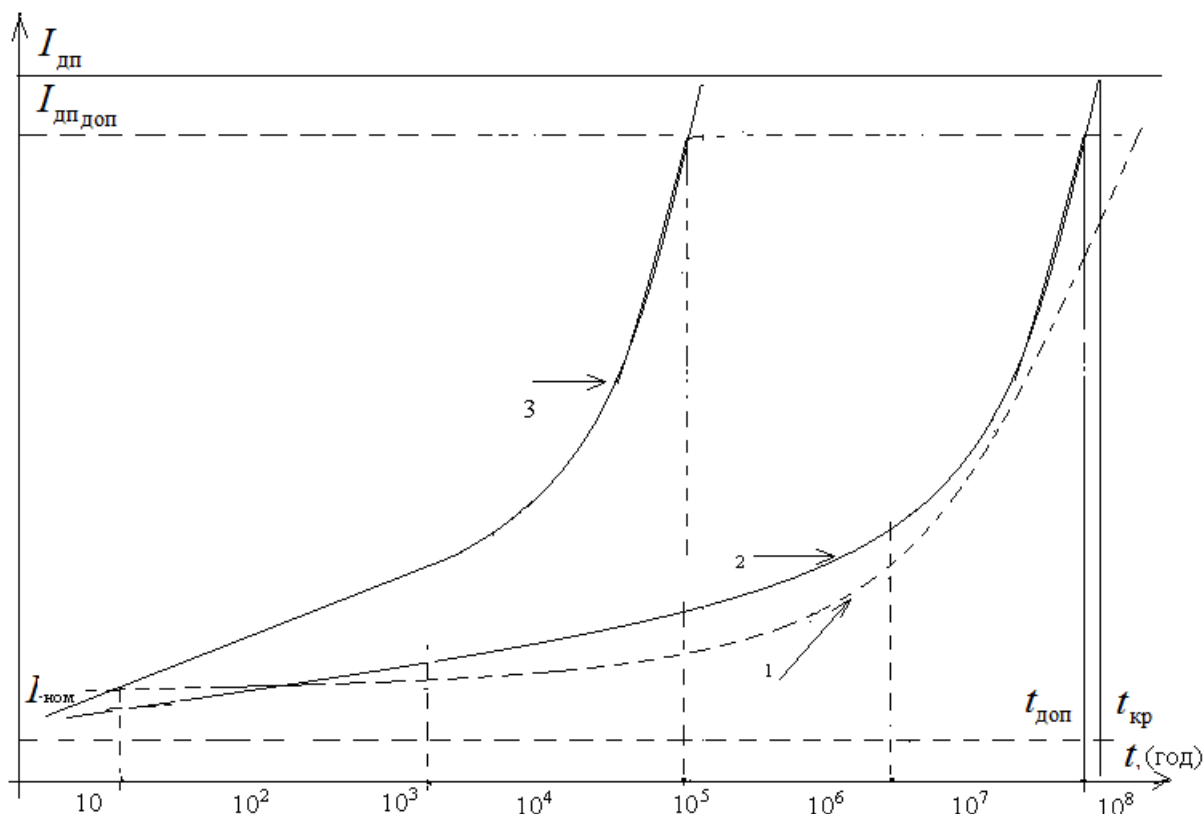


Рис. 3. Зміни діагностичного параметру простішого РЕК: 1 – експериментальна крива, 2 – аналітична крива, 3 – динаміка зміни струму у випадку складного (10^3 РЕК) об'єкту контролю

Розглянемо процедуру визначення ресурсу (часу досягнення критичного стану) зразку РЕО (P_p) на прикладі енергетичної складової діагностичного параметру. При використанні запропонованої автоматизованої системи діагностування в базі даних такої системи повинна бути низка вихідних даних (перелік необхідної інформації наведено у табл.1).

Визначення ресурсу (P_p) при відомій закономірності зміни діагностичного параметру представлено на схемі (рис. 4). В частині рис. 4 (а) використані наступні позначення: $P_{\text{вик}}$ – використаний ресурс до моменту контролю; $I_k = P_k - P_n$ – зміна значення параметра до моменту контролю (діагностування); $I_{\text{пр}} = P_{\text{пр}} - P_n$ – граничне зміна значення параметра; P_p – шуканий ресурс.

Таблиця 1.

Дані для визначення ресурсу РЕО

№	Вихідні дані	Позначення	Джерело
1	Номінальне значення діагностичного параметру	Π_n	Технічна документація
2	Граничне значення діагностичного параметру	$\Pi_{гр}$	Технічна документація
3	Показник, який характеризує закономірність змін значення діагностичного параметру	α	Технічна документація
4	Напрацювання від початку експлуатації	$P_{вик}$	Технічна документація
5	Значення діагностичного параметру (вимірюється під час контролю)	Π_k	Показання засобів вимірювання

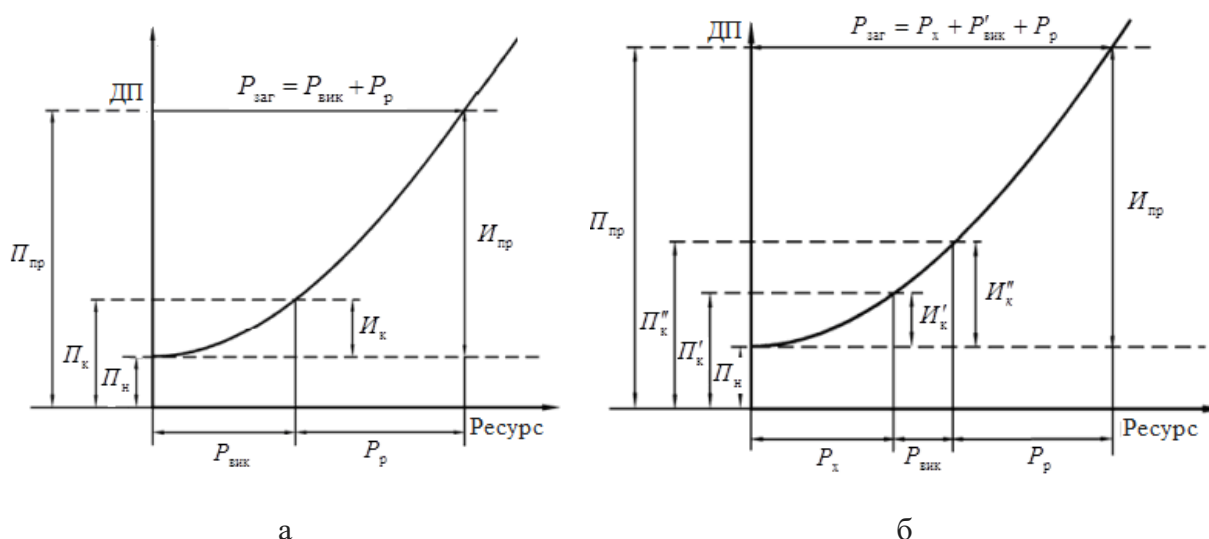


Рис. 4. Спрощена схема визначення ресурсу при: а – відомому напрацюванні об'єкту контролю від початку експлуатації; б – невідомому напрацюванні об'єкту контролю від початку експлуатації

Маючи вказані дані, P_p визначають за формулою [4]:

$$P_p = P_{вик} \left[\left(\frac{\Pi_{пр}}{\Pi_k} \right)^{\frac{1}{\alpha}} - 1 \right]. \quad (4)$$

На практиці значення α знаходиться в межах від 0,8 до 2,0 [10]. Значення $\Pi_{пр}$, Π_n , α розраховують заздалегідь і заносять в базу даних автоматизованої системи діагностування об'єкту РЕО для використання при визначенні P_p .

Таким чином, для визначення ресурсу (4) необхідно провести виміри діагностичного параметру і знати напрацювання до моменту виміру. Значення інших показників – табличні.

У другому випадку, коли відомості про напрацювання окремих складових частин РЕО від початку експлуатації або останнього капремонту відсутні, ресурс можливо визначити за значеннями параметрів, виміряних при дворазовому контролі (діагностуванні) та напрацювання між першим і другим вимірюваннями.

Схема прогнозування ресурсу при невідомому напрацюванні від початку експлуатації представлена на рис.4 (б), де використовуються наступні позначення: Π'_k – значення параметру при першій перевірці; Π''_k – значення параметру при повторній перевірці; $I'_k = \Pi'_k - \Pi_n$ – зміна значення параметру від початку експлуатації до першої перевірки; $I''_k = \Pi''_k - \Pi_n$ – зміна значення параметру від початку експлуатації до повторної перевірки; $I_{пр} = \Pi_{пр} - \Pi_n$ – гранична зміна значення параметру; P_x – використаний ресурс (величина невідома); $P'_{вик}$ – ресурс, використаний за час роботи між першою і другою перевірками.

Таким чином, для визначення P_p при невідомому напрацюванні зразку РЕО з початку експлуатації необхідно виміряти значення контрольованого параметру не менше двох разів і знати напрацювання за час роботи між цими вимірами.

В цьому випадку P_p визначають за формулою [4]:

$$P_p = P'_{вик} \left[\frac{1}{\left(\frac{I''_k}{I'_k}\right)^{\frac{1}{\alpha}} - 1} \left(\frac{I_{пр}}{I'_k}\right)^{\frac{1}{\alpha}} + 1 \right] \left[\left(\frac{I_{пр}}{I''_k}\right)^{\frac{1}{\alpha}} - 1 \right].$$

Висновки

Прогнозування технічного стану принципово можливе лише в разі наявності інформаційного діагностичного параметру та адекватної діагностичної моделі об'єкту контролю.

На сьогодні в ЗСУ функціонують зразки та системи РЕО, для яких характерна наявність програмної та апаратної складової. При цьому фактичне напрацювання таких об'єктів може бути відоме та невідоме. Для обох випадків необхідно вирішення задач технічного діагностування. Вирішення зазначеної задачі можливе при застосуванні автоматизованої системи діагностування. Визначення ресурсу об'єктів РЕО та обґрунтування часу проведення регламентних робіт дозволить скоротити число відмов РЕО в процесі експлуатації, виключити позапланову (аварійну) зупинку, заощадити кошти на відновлення, збільшити міжремонтний період напрацювання.

Напрямок подальших досліджень є :

- встановлення динаміки зміни узагальненого енергетично часового діагностичного параметру;
- визначення та обґрунтування припустимих меж цього параметру в двовірній площині;
- використання отриманої інформації для обґрунтування періодичності контролю та регламентних робіт однотипних програмно-апаратних засобів як одного з видів сучасних об'єктів РЕО.

Список літератури

1. Ключев, В.В. Технические средства диагностирования: справочник / В.В. Ключев, П.П. Пархоменко, В.Е. Абрамчук. — М.: Машиностроение, 2009. — С. 448.
2. Ершов, Д.Ю. Техническое диагностирование и методы контроля механических узлов в машиностроении. — Москва, 2013. — № 4. — С. 62-64.

3. Стрельников, В.П. Состояние и перспективы теории и практики надежности. Надежность и долговечность машин и сооружений: Международный научно-технический сборник. – Москва, 2005. — № 24. — С. 27-38.
4. Лебедев, А.Н. Вероятностные методы в инженерных задачах: справ. / А.Н. Лебедев, М.С. Куприянов, Д.Д. Недосекин, Е.А. Чернявский. – СПб.: Энергоатомиздат. 2008. – 333 с.
5. Хан, Г. Статистические модели в инженерных задачах / Г. Хан, С. Шапиро. – М.: Мир, 2010. — 3-е изд. — 412 с.
6. Вишнівський, В.В. Безконтактний індукційний метод діагностування радіоелектронних блоків : збірник наук. праць ВІКНУ ім. Т. Шевченка / В.В. Вишнівський, М.К. Жердев, Б.П. Креденцер, В.В. Кузавков. – Київ, 2013. — № 43. — 336 с.
7. Кузавков, В.В. Діагностична модель р-п (п-р) переходу в динамічному режимі для безконтактного індукційного методу діагностування / М.К. Жердев / збірник наук. праць ВІКНУ ім. Т. Шевченка. – Київ, 2014. — № 45. — 317 с.
8. Жердев, М.К. Узагальнення результатів форсованих випробувань радіоелектронних компонентів / М.К. Жердев, В.В. Кузавков, І.В. Пампуха / збірник наук. праць ВІКНУ ім. Т. Шевченка. – Київ, 2015. — № 49. — С. 40-47.
9. Жердев, М.К. Перевірка адекватності аналітичної моделі радіоелектронного компоненту / М.К. Жердев, В.В. Кузавков / науковий журнал Інформаційна безпека Східноукраїнський національний університет ім. В. Даля. – Луганськ, 2014. — № 3 (15). — С. 76-81.
10. Судакова, Р.С. Надежность и эффективность в технике. Экспериментальная отработка и испытания / Р.С. Судакова, О.И. Тескина. – М.: Машиностроение, 2011. — Т.6. — 408 с.

ПРОГНОЗИРОВАНИЕ ТЕХНИЧЕСКОГО СОСТОЯНИЯ ОДНОТИПНЫХ ПРОГРАМНО-АППАРАТНЫХ СРЕДСТВ

В.В. Кузавков, П.В. Хусаинов

Военный институт телекоммуникаций и информатизации имени Героев Крут,
ул. Московская, 45/1, Киев, 01011, Украина; e-mail: nevse@ukr.net

В статье рассмотрены подходы, основанные на физических предпосылках, к прогнозированию технического состояния (определение ресурса) радиоэлектронных объектов, которые попадают под определение «однотипные программно-аппаратные средства». Прогнозирование технического состояния радиоэлектронного оборудования (РЭО) – важная составная часть теории надежности, а показатели «ресурс» и «срок службы» являются одними из основных понятий этой теории. Особое место имеет задача прогнозирования ресурса (определение времени достижения критического состояния) РЭО на стадии эксплуатации. Данная задача связана с оценкой текущего состояния и его прогнозом на будущее, оценке вероятностей наступления отказов, риска аварийных ситуаций. На основе прогноза устанавливается срок очередного контроля состояния РЭО или назначается предельно допустимый срок эксплуатации. Процесс прогнозирования принципиально возможен при наличии диагностического параметра, который соответствует условиям измеримости, инвариантности к воздействию помех, информативности, а также адекватной диагностической модели объекта контроля (которая устанавливает связь между пространством состояния технического устройства и пространством диагностических признаков). В статье рассматривается решение задач технической диагностики для совокупности технических средств приема, передачи хранения и обработки информации под управлением программной составляющей указанного технического объекта. Применение физических предпосылок функционирования РЭО для оценки ресурса технических средств радиоэлектроники стало возможным с появлением и развитием теории дефектообразования в полупроводниковых структурах, возникновением новых методов сбора диагностической информации на основе стохастических процессов изменения тока в полупроводниковых структурах в зависимости от времени наработки. Предложена диагностическая модель, которая учитывает быстрые и медленные процессы в объекте контроля, рассмотрены теоретические и практические вопросы прогнозирования ресурса РЭО.

Ключевые слова: прогнозирование, диагностический параметр, физико-химические процессы, радиоэлектронное оборудование

FORECASTING THE TECHNICAL STATE OF THE SAME TYPE SOFTWARE AND HARDWARE EQUIPMENT

V.V. Kuzavkov, P.V. Khusainov

Military Institute of Telecommunication and Information Technologies named after Heroes Krut,
45/1, Moscovska Str., Kiev, 01011, Ukraine; e-mail: nevse@ukr.net

In the article, the approaches based on physical conditions are precondition for the prediction of the technical condition (determination of the resource) of radio-electronic objects that fall under the definition of "the same type of software and hardware". Technical station prediction of the radio electronic equipment (REE) is an important part of the reliability theory, and the resource and service performance are part of the theory basic understanding. A special role is played by the task of forecasting the REE resource (determining the time to reach the critical state) at the operational stage. The given task connected with an estimation of a current condition and its forecast for the future, probabilities of approach refusals estimation, emergencies risk. On the forecast basis, the period for the next monitoring REE condition is established or the maximum permissible service life is set. The forecasting process is possible in principle if there is a diagnostic parameter that corresponds to the conditions of measurability, invariance to interference, informatively, and an adequate diagnostic model of the monitoring object (which establishes a connection between the technical device state space and the space of diagnostic features). The article considered the solution of technical diagnostics tasks for a technical means set of reception, storage and processing transmission of information under the specified technical objects program component control. Using of the physical prerequisites for the REO functioning to evaluate technical means of radio electronics resource became possible with the advent and development of the defect formation in semiconductor structures theory, the emergence of new methods for collecting diagnostic information based on stochastic processes of current change in semiconductor structures, depending on the time elapsed. The diagnostic model, which takes into account the fast and slow processes in the object of control, is offered, theoretical and practical questions of REO resource forecasting are considered.

Keywords: forecasting, diagnostic parameter, physico-chemical processes, radio-electronic equipment

УДОСКОНАЛЕННЯ РЕАЛІЗАЦІЇ КРИПТОАЛГОРИТМУ ЕЛЬ-ГАМАЛЯ НА ОСНОВІ СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ

І.З. Якименко

Тернопільський національний економічний університет,
вул. Львівська, 11, Тернопіль, 46020, Україна; e-mail: iyakimenko@ukr.net

В даній роботі проведено аналіз систем захисту інформаційних потоків з використанням асиметричних криптоалгоритмів, на основі якого встановлені недоліки існуючих підходів реалізації операцій модулярного експоненціювання при шифруванні/дешифруванні, а саме – використання ключів, блоків шифрування та модуля криптоперетворення до 2048 та 4096 біт, що призводить до зменшення часових характеристик. Встановлено, що одним з перспективних підходів щодо вирішення даного класу задач є використання системи залишкових класів (СЗК), яка володіє рядом переваг в порівнянні з двійковою – здійснення операцій паралельно та зменшення розрядності операндів, які не перевищують розрядності набору обраних модулів СЗК. Вказані недоліки, які стосуються переведення з СЗК в десяткову систему числення, а саме необхідність пошуку оберненого елемента за модулем, тобто базисних чисел. В роботі зазначено, що існують набори модулів, які утворюють досконалу форму СЗК (базисні числа рівні 1) та модифіковану досконалу СЗК (базисні числа рівні ± 1), що суттєво зменшує часову складність переведення. Наведені теоретичні основи удосконалення реалізації асиметричного криптоалгоритму Ель-Гамала на основі сумісного використання СЗК та векторно-модульного алгоритму модулярного множення, що дозволило розпаралелити процес, зменшити часову складність та підвищити ефективність виконання процесу шифрування/дешифрування.

Ключові слова: криптосистема Ель-Гамала, система залишкових класів, модулярне множення, векторно-модульний метод, обчислювальна складність, обернений елемент за модулем, досконала форма системи залишкових класів, модифікована система числення системи залишкових класів, шифрування, дешифрування

Вступ

На сьогоднішній день для забезпечення високого рівня захисту інформаційних потоків використовують асиметричні криптоалгоритми RSA, Ель-Гамала [1], Рабіна [2] з параметрами – ключі, блок шифрування та модуль криптоперетворення не менше 1024 біт з перспективою їх зростання в найближчі роки до 2048 та 4096 біт, що призводить до зменшення часових характеристик. При шифруванні/дешифруванні основними операціями зазначених асиметричних алгоритмів є модулярне експоненціювання та піднесення до квадрату за модулем багаторозрядних чисел. Багатьма вченими розроблялися методи модулярного множення та експоненціювання, які мають певні функціональні обмеження, а саме використовують двійково-десяткову систему числення, яка характеризується високою обчислювальною складністю.

Найперспективнішим підходом щодо вирішення даного класу задач є використання системи залишкових класів (СЗК), яка володіє рядом переваг в порівнянні з двійковою – здійснення операцій паралельно та зменшення розрядності операндів, які не перевищують розрядності набору обраних модулів СЗК. Поряд з цим існують певні труднощі при переведенні з СЗК в десяткову систему числення, а саме необхідність пошуку оберненого елемента за модулем, тобто базисних чисел. Слід відмітити, що існують набори модулів, які утворюють досконалу форму СЗК (базисні

числа рівні 1) [3] та модифіковану досконалу СЗК (базисні числа рівні ± 1) [4], що суттєво зменшує часову складність переведення.

Метою роботи є підвищення швидкодії та зменшення складності базових операцій асиметричних криптоалгоритмів RSA, Ель-Гамала на основі сумісного застосування СЗК та алгоритму векторно-модульного множення [5].

Удосконалення реалізації алгоритму шифрування Ель-Гамала з використанням системи залишкових класів

На першому етапі відбувається генерування ключів, а саме:

1. Вибираються два простих числа p і q , та випадкове ціле число x для якого має місце нерівність: $1 < x < p$.

Обчислюється значення $y = q^x \bmod p$ на основі сумісного використання СЗК і векторно-модульного алгоритму модулярного експоненціювання, тобто згідно формули, що дозволяє розпаралелити процес на l потоків, які відповідають кількості модулів:

$$y = q^x \bmod p = \left(\sum_{i=1}^l b_i B_i q_i \right) \bmod p,$$

де $q_i = (q \bmod p_i)^x \bmod p_i$, $p = \prod_{i=1}^l p_i$, $B_i = \frac{p}{p_i}$, $b_i = B_i^{-1} \bmod p_i$, l – кількість модулів та потоків.

Пошук значення $q_i = (q \bmod p_i)^x \bmod p_i$ здійснюється на основі використання векторно-модульного методу модулярного множення з використанням представлення

$x = \sum_{j=0}^{n-1} x_j \cdot 2^j$, де $x_j = 0,1$ згідно формули обчислити q_i :

$$q_i = (q \bmod p_i)^{\sum_{j=0}^{n-1} x_j \cdot 2^j} \bmod p_i = \prod_{j=1}^{n-1} (q \bmod p_i)^{x_j \cdot 2^j} = \prod_{j=0}^{n-1} s_j \bmod p_i,$$

де $s_i = M^{2^i} \bmod p_i$, при чому $s_i = (s_{i-1})^2 \bmod p_i$. Тоді будь-який степінь x можна записати за степенями 2 і шуканий результат можна отримати, перемноживши відповідну кількість стовбців за допомогою таблиці 1.

Таблиця 1.

Вектор піднесення до степеня в базисі Радемахера–Крестенсона

x_{n-1}		x_i	...	x_1	x_0
s_{n-1}		s_i	...	s_1	s_0
$q^{2^{n-1}} \bmod p_i$	...	$q^{2^i} \bmod p_i$	...	$q^{2^1} \bmod p_i$	$q^{2^0} \bmod p_i$

Для пошуку значення q_i перемножаються ті значення s_i , для яких $x_j = 1$. Основними перевагами такого методу є здійснення операцій над числами значно менших розмірів в порівнянні з класичним підходом, що дозволяє пришвидшити алгоритм модулярного експоненціювання.

При знаходженні значення $s_i s_{i-1} \bmod p_i$ представимо $s_{i-1} = \sum_{k=0}^{n-1} w_k \cdot 2^k$, де $w_k = 0,1$, n – розрядність модуля p_i . На основі використання векторно-модульного методу будуються два вектор-рядки, в першому з яких записуються елементи:

$$h_0 = 2^0 s_i \bmod p_i, \quad h_i = 2 \cdot s_{i-1} \bmod p_i,$$

в другому w_i , як показано в таблиці 2.

Таблиця 2.

Представлення вектор-рядків модульного множення

h_{n-1}	...	h_i	...	h_1	h_0
w_{n-1}		w_i	...	w_1	w_0

Результат модулярного множення двох n -розрядних чисел знаходиться згідно формули:

$$s_i s_{i-1} \bmod p_i = \left(\sum_{i=0}^{n-1} w_i \cdot h_i \right) \bmod p_i.$$

Розроблений метод характеризується меншою часовою складністю порівняно з класичними. Отже, відкритим ключем виступає (p, q, y) , а закритим – x .

2. Шифрування. Вибирається випадкове ціле число k таке, що $1 < k < p-1$. Обчислюється значення $a = q^k \bmod p$. Для цього використовується СЗК та векторно-модульний алгоритм модулярного експоненціювання на основі формули:

$$y = q^k \bmod p = \left(\sum_{i=1}^l b_i B_i q_i \right) \bmod p,$$

де $q_i = (q \bmod p_i)^k \bmod p_i$, $p = \prod_{i=1}^l p_i$, $B_i = \frac{p}{p_i}$, $b_i = B_i^{-1} \bmod p_i$, l – кількість модулів та потоків.

Пошук значення $q_i = (q \bmod p_i)^k \bmod p_i$ здійснюється на основі використання векторно-модульного методу модулярного множення з використанням представлення $k = \sum_{j=0}^{n-1} k_j \cdot 2^j$, де $k_j = 0,1$ згідно формули обчислити q_i :

$$q_i = (q \bmod p_i)^{\sum_{j=0}^{n-1} k_j \cdot 2^j} \bmod p_i = \prod_{j=1}^{n-1} (q \bmod p_i)^{k_j \cdot 2^j} = \prod_{j=0}^{n-1} y_j \bmod p_i,$$

де $y_i = q^{2^i} \bmod p_i$, при чому $y_i = (y_{i-1})^2 \bmod p_i$. Тоді будь-який степінь k можна записати за степенями 2 і шуканий результат можна отримати, перемноживши відповідну кількість стовбців за допомогою таблиці 3:

Таблиця 3.

Вектор піднесення до степеня в базисі Радемахера–Крестенсона

k_{n-1}		k_i	$\dots$	k_1	k_0
y_{n-1}		y_i	$\dots$	y_1	y_0
$q^{2^{n-1}} \bmod p_i$	$\dots$	$q^{2^i} \bmod p_i$	$\dots$	$q^{2^1} \bmod p_i$	$q^{2^0} \bmod p_i$

Для пошуку значення q_i перемножаються ті значення y_i , для яких $k_j = 1$. При знаходженні значення $y_i y_{i-1} \bmod p_i$ представимо $y_{i-1} = \sum_{z=0}^{n-1} a_z \cdot 2^z$, де $a_z = 0,1$, n – розрядність модуля p_i . На основі використання векторно-модульного методу будуються два вектор-рядки, в першому з яких записуються елементи:

$$r_0 = 2^0 y_i \bmod p, \quad r_i = 2 \cdot y_{i-1} \bmod p,$$

в другому a_z , як показано в таблиці 4.

Таблиця 4.

Представлення вектор-рядків модульного множення

r_{n-1}	$\dots$	r_i	$\dots$	r_1	r_0
a_{n-1}		a_i	$\dots$	a_1	a_0

Результат модулярного множення двох n -розрядних чисел знаходиться згідно формули:

$$y_i y_{i-1} \bmod p_i = \left(\sum_{i=0}^{n-1} a_i \cdot r_i \right) \bmod p_i.$$

Розроблений метод характеризується меншою часовою складністю порівняно з класичними за рахунок заміни операції множення операцією додавання.

Для отримання шифр-тексту для повідомлення M знаходиться значення $b = y^k \cdot M \bmod p$.

Спочатку обчислюється значення $\alpha = y^k \bmod p$ на основі використання векторно-модульного алгоритму модулярного експоненціювання згідно формули:

$$\alpha = y^k \bmod p = \left(\sum_{i=1}^l b_i B_i y_i \right) \bmod p,$$

де $y_i = (y \bmod p_i)^k \bmod p_i$, $p = \prod_{i=1}^l p_i$, $B_i = \frac{p}{p_i}$, $b_i = B_i^{-1} \bmod p_i$, l – кількість модулів та потоків.

Пошук значення $y_i = (y \bmod p_i)^k \bmod p_i$ здійснюється на основі використання векторно-модульного методу модулярного множення з використанням представлення

$k = \sum_{j=0}^{n-1} k_j \cdot 2^j$, де $k_j = 0,1$ згідно формули обчислити y_i :

$$y_i = (y \bmod p_i)^{\sum_{j=0}^{n-1} k_j 2^j} \bmod p_i = \prod_{j=1}^{n-1} (y \bmod p_i)^{k_j 2^j} = \prod_{j=0}^{n-1} \beta_j \bmod p_i,$$

де $\beta_i = y^{2^i} \bmod p_i$, при чому $\beta_i = (\beta_{i-1})^2 \bmod p_i$. Тоді будь-який степінь k можна записати за степенями 2 і шуканий результат можна отримати, перемноживши відповідну кількість стовбців за допомогою таблиці 5.

Таблиця 5.
Вектор піднесення до степеня в базисі Радемахера–Крестенсона

k_{n-1}		k_i	...	k_1	k_0
β_{n-1}		β_i	...	β_1	β_0
$y^{2^{n-1}} \bmod p_i$	...	$y^{2^i} \bmod p_i$	...	$y^{2^1} \bmod p_i$	$y^{2^0} \bmod p_i$

Для пошуку значення y_i перемножаються ті значення β_i , для яких $k_j = 1$. Для знаходження значення $\beta_i \beta_{i-1} \bmod p_i$ представимо $\beta_{i-1} = \sum_{z=0}^{n-1} f_z \cdot 2^z$, де $f_z = 0, 1$, n – розрядність модуля p_i . На основі використання векторно-модульного методу будуються два вектор-рядки, в першому з яких записуються елементи:

$$c_0 = 2^0 \beta_i \bmod p_i, \quad c_i = 2 \cdot \beta_{i-1} \bmod p_i,$$

в другому f_z , як показано в таблиці 6.

Таблиця 6.
Представлення вектор-рядків модульного множення

c_{n-1}	...	c_i	...	c_1	c_0
f_{n-1}		f_i	...	f_1	f_0

Результат модулярного множення знаходиться згідно формули:

$$\beta_i \beta_{i-1} \bmod p_i = \left(\sum_{i=0}^{n-1} c_i \cdot f_i \right) \bmod p_i.$$

На наступному кроці обчислюються значення $b = y^k \cdot M \bmod p = \alpha \cdot M \bmod p$ на основі векторно-модульного методу модулярного множення. Для знаходження значення $\alpha \cdot M \bmod p$ представимо $M = \sum_{k=0}^{n-1} M_k \cdot 2^k$, де $\alpha_j, M_k = 0, 1$, n – розрядність модуля p . Будуються два вектор-рядки, в першому з яких записуються елементи:

$$\delta_0 = 2^0 \alpha \bmod p_i, \quad \delta_i = 2 \cdot \delta_{i-1} \bmod p_i,$$

в другому M_i , як показано в таблиці 7.

Таблиця 7.

Представлення вектор-рядків модульного множення

δ_{n-1}	...	δ_i	...	δ_1	δ_0
M_{n-1}		M_i	...	M_1	M_0

Результат модулярного множення знаходиться зі співвідношення:

$$b = \alpha \cdot M \bmod p = \left(\sum_{i=0}^{n-1} \delta_i \cdot M_i \right) \bmod p.$$

В результаті проведених обчислень, отримується пара (a, b) , яка є шифротекстом.

3. Дешифрування відбувається згідно формули $M = b \cdot (a^x)^{-1} \bmod p$. Спочатку знаходиться значення $\varepsilon = a^x \bmod p$, для цього використовується векторно-модульний метод модулярного експоненціювання:

$$\varepsilon = a^x \bmod p = \left(\sum_{i=1}^l b_i B_i a_i \right) \bmod p,$$

де $a_i = (a \bmod p_i)^k \bmod p_i$, $p = \prod_{i=1}^l p_i$, $B_i = \frac{p}{p_i}$, $b_i = B_i^{-1} \bmod p_i$, l – кількість модулів та потоків.

Пошук значення $a_i = (a \bmod p_i)^x \bmod p_i$ здійснюється на основі використання векторно-модульного методу модулярного множення, представивши $x = \sum_{j=0}^{n-1} x_j \cdot 2^j$, де $x_j = 0, 1$ і згідно формули обчислити a_i :

$$a_i = (a \bmod p_i)^{\sum_{j=0}^{n-1} x_j \cdot 2^j} \bmod p_i = \prod_{j=1}^{n-1} (a \bmod p_i)^{x_j \cdot 2^j} = \prod_{j=0}^{n-1} \phi_j \bmod p_i.$$

де $\phi_i = a^{2^i} \bmod p_i$, при чому $\phi_i = (\phi_{i-1})^2 \bmod p_i$.

Тоді будь-який степінь x можна записати за степенями 2 і шуканий результат можна отримати, перемноживши відповідну кількість стовбців за допомогою таблиці 8. Для пошуку значення a_i перемножаються ці значення ϕ_i для яких $x_j = 1$. При обчисленні $\phi_i \phi_{i-1} \bmod p_i$ представимо $\phi_{i-1} = \sum_{j=0}^{n-1} \phi_j \cdot 2^j$, де $\phi_j = 0, 1$, n – розрядність модуля p_i .

Таблиця 8.

Вектор піднесення до степеня в базисі Радемахера–Крестенсона

x_{n-1}		x_i	...	x_1	x_0
ϕ_{n-1}		ϕ_i	...	ϕ_1	ϕ_0
$a^{2^{n-1}} \bmod p_i$	...	$a^{2^i} \bmod p_i$	...	$a^{2^1} \bmod p_i$	$a^{2^0} \bmod p_i$

На основі використання векторно-модульного методу будуються два вектор-рядки, в першому з яких записуються елементи:

$$g_0 = 2^0 \phi_i \bmod p_i, \quad g_i = 2 \cdot g_{i-1} \bmod p_i,$$

в другому φ_j , як показано в таблиці 9.

Таблиця 9.

Представлення вектор-рядків модульного множення

g_{n-1}	$\dots$	g_i	$\dots$	g_1	g_0
φ_{n-1}		φ_i	$\dots$	φ_1	φ_0

Результат модулярного множення обчислюється згідно формули:

$$\phi_i \phi_{i-1} \bmod p_i = \left(\sum_{i=0}^{n-1} g_i \cdot \varphi_i \right) \bmod p_i.$$

В подальшому необхідно знайти $\eta = \varepsilon^{-1} \bmod p$ на основі методу з додаванням залишку, що дозволить зменшити часову складність в порівнянні з класичними методами, які ґрунтуються на розширеному алгоритмі Евкліда, методі повного перебору та з використанням функції Ейлера.

Спочатку обчислюється $\eta_0 = p \bmod \varepsilon \neq 0$, після чого послідовно виконується операція додавання: $\eta_1 = (\eta_0 + 1) \bmod \varepsilon$, $\eta_2 = (\eta_1 + \eta_0) \bmod \varepsilon = (2\eta_0 + 1) \bmod \varepsilon$, $\dots$, $\eta_i = (\eta_{i-1} + \eta_0) \bmod \varepsilon = (i\eta_0 + 1) \bmod \varepsilon$.

Описана процедура продовжується до тих пір, поки деяке число η_i не стане рівним нулю. Тоді обернений елемент визначається за формулою:

$$\eta = \varepsilon^{-1} \bmod p = \frac{i \cdot p + 1}{\varepsilon}.$$

Векторно-модульний метод модулярного множення дозволить знайти значення $M = b \cdot \eta \bmod p$, що i є результатом дешифрування. Запишемо $\eta = \sum_{k=0}^{n-1} \eta_k \cdot 2^k$, де $b_j, \eta_k = 0, 1$, n – розрядність модуля p . На основі використання векторно-модульного методу будуються два вектор-рядки, в першому з яких записуються елементи:

$$\lambda_0 = 2^0 b \bmod p, \quad \lambda_i = 2 \cdot \lambda_{i-1} \bmod p,$$

в другому η_i , як показано в таблиці 10.

Таблиця 10.

Представлення вектор-рядків модульного множення

λ_{n-1}	$\dots$	λ_i	$\dots$	λ_1	λ_0
η_{n-1}		η_i	$\dots$	η_1	η_0

Результат модулярного множення $M = b \cdot \phi \bmod p$ знаходиться згідно співвідношення:

$$M = b \cdot \eta \bmod p = \left(\sum_{i=0}^{n-1} \lambda_i \cdot \eta_i \right) \bmod p.$$

Отже, запропонований підхід шифрування/дешифрування асиметричної криптосистеми Ель-Гамала дозволяє розпаралелити процес та проводити обчислення над числами меншої розрядності в порівнянні з класичним підходом, що, в свою чергу, призводить до зменшення часової складності базових операцій: модулярного множення та експоненціювання, пошуку оберненого елемента за модулем.

Висновки

В роботі представлено удосконалення реалізації асиметричного алгоритму шифрування Ель-Гамала, а саме базові операції модулярного експоненціювання багаторозрядних чисел, на основі СЗК та векторно-модульного алгоритму модулярного множення, що дозволило суттєво зменшити часову складність та підвищити ефективність виконання процесу шифрування/дешифрування.

Список літератури

1. Касянчук, М.М. Модифікований метод шифрування Рабіна з використанням різних форм системи залишкових класів / М.М. Касянчук, І.З. Якименко, Л.О. Дубчак, Н.А. Рендзеньяк, Н.М. Мандебура // Вісник Хмельницького національного університету. Технічні науки, 2017. — № 1 (245). — С. 127-131.
2. Якименко, І.З. Теорія алгоритмів RSA та Ель-Гамала в розмежованій системі числення Радемахера-Крестенсона / І.З. Якименко, М.М. Касянчук, О.І. Волинський, І.Р. Пітух // Вісник Хмельницького національного університету. Технічні науки, 2011. — № 3. — С. 265-273.
3. Kasianchuk, M.M. Algorithms of findings of perfect shape modules of remaining classes system / M. Kasianchuk, I. Yakymenko I. Pazdriy, O. Zastavnyy // XIII International Conference "The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM-2015)", 23-25 February, 2015, Polyana-Svalyava (Zakarpatty), Ukraine. — Pp. 168-171.
4. Касянчук, М.М. Аналітичний пошук модулів досконалої форми системи залишкових класів та їх застосування в китайській теоремі про залишки / М.М. Касянчук, І.З. Якименко, І.Р. Паздрій, Я.М. Николайчук // Вісник Хмельницького національного університету. Технічні науки, 2015. — № 1 (221). — С. 170-176.
5. 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) – Warsaw, Poland, September, 2015. — V.1. — Pp. 161-163.

УСОВЕРШЕНСТВОВАНИЕ РЕАЛИЗАЦИИ КРИПТОАЛГОРИТМА ЭЛЬ-ГАМАЛЯ НА ОСНОВЕ СИСТЕМЫ ОСТАТКОВ

И.З. Якименко

Тернопольский национальный экономический университет,
ул. Львовская, 11, Тернополь, 46020, Украина; e-mail: iyakymenko@ukr.net

В данной работе проведен анализ систем защиты информационных потоков с использованием асимметричных криптоалгоритмов, на основе которого установлены недостатки существующих подходов реализации операций модулярного экспоненцирования при шифровании/дешифровании, а именно – использование ключей, блоков шифрования и модуля криптопреобразования до 2048 и 4096 бит, что приводит к уменьшению временных характеристик. Установлено, что одним из перспективных подходов к решению данного класса задач является использование системы остаточных классов (СОК), которая обладает рядом преимуществ по сравнению с двоичной – осуществление операций параллельно и уменьшение разрядности операндов, которые не превышают разрядности набора выбранных модулей СОК. Указанные недостатки, касающиеся перевода с СОК в десятичную систему счисления, а именно необходимость поиска обратного элемента по модулю, то есть базисных чисел. В работе отмечено, что существуют наборы модулей, которые образуют совершенную форму СОК (базисные числа равны 1) и модифицированную совершенную СОК (базисные числа равны ± 1), что существенно уменьшает временную сложность перевода. Приведенные теоретические основы совершенствования реализации асимметричного криптоалгоритма Эль-Гамала на основе совместного использования СОК и векторно-модульного алгоритма модулярного умножения, что позволило распараллелить процесс, уменьшить временную сложность и повысить эффективность выполнения процесса шифрования/дешифрования.

Ключевые слова: криптосистема Эль-Гамала, система остаточных классов, модульное умножение, векторно-модульный метод, вычислительная сложность, обратный элемент по модулю, совершенная форма системы остаточных классов, модифицированная система счисления системы остаточных классов, шифрование, дешифрование

IMPROVING THE IMPLEMENTATION OF EL-GAMAL CRYPTOALGORITHM ON THE BASIS OF THE SYSTEM OF RESIDUE CLASSES

I.Z. Yakymenko

Ternopil National Economic University,
11, Lvivska Str., Ternopil, 46020, Ukraine; e-mail: iyakymenko@ukr.net

The analysis of information flow protection systems, using asymmetric cryptalgorithms, on the basis of which the shortcomings of existing approaches of realization of the operations of modular exponentiation at encrypting/decrypting, namely - use of keys, encryption units and crypto-conversion module up to 2048 and 4096 bt, which reduces the time characteristics, was made in this work (thesis). It was established, that one of the perspective approaches concerning the solution of this class of tasks is use of the system of residue classes (SRC), which has several advantages in comparison with the binary one – conducting operations in parallel and digit capacity decrease of the operands, which do not exceed digit capacity of the selected SRC modules set. These drawbacks concern transfer from SRC to the decimal number system, namely the need to search for the reverse element by module, that is, the basis numbers. The thesis states that there are modules sets, which form the perfect SRC form (basic numbers are equal to 1) and modified perfect SRC (basic numbers are equal to ± 1), which significantly reduces the time complexity of the transfer. Theoretical foundations of improvement of implementation of asymmetric El-Gamal cryptoalgorithm on the basis of joint use of SRC and vector-modular algorithm of modular multiplication, which made it possible to parallelize the process, to reduce time complexity and to improve performance of encrypting/decrypting process were given.

Keywords: El-Gamal cryptosystem, the system of residue classes, modular multiplication, vector-modular method, computational complexity, reverse element by module, perfect form of the system of residue classes, modified system of computation of the system of residue classes, encrypting, decrypting

ОПТИМИЗАЦИЯ МЕТОДОВ ПРОГНОЗИРОВАНИЯ, ОБРАБОТКИ И АНАЛИЗА ИНФОРМАЦИИ В РАЗНОСТРУКТУРНЫХ ХРАНИЛИЩАХ ДАННЫХ

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

Одесский национальный морской университет,
ул. Мечникова, 34, Одесса, 65029, Украина; e-mail: denshibaeв@outlook.com

В статье предложен метод оптимизации обработки большого объема данных, предназначенный для диагностирования состояния оборудования сложных технических систем. Такое диагностирование позволяет повысить эффективность анализа неисправностей в технических системах с целью их скорейшего устранения. Это достигается за счет прогнозирования отказа критически уязвимых систем, способных вывести из эксплуатации транспортное средство, либо привести к последствиям, угрожающим жизни людей. Метод реализован в информационной системе, основанной на наборе алгоритмических согласованностей, направленных на идентификацию информации в высоконагруженных сетях и ее обработку в моменты передачи от сложных технических систем к центральному хранилищу данных. Функционирование информационной системы основывается на применении гибридных алгоритмов поиска и сортировки данных, концепции Data Mining, а также алгоритмов для работы с большими объемами данных. Методы отбора и распределения данных выполняются на уровне контроля показаний датчиков технической системы и распределяются до момента записи в хранилище данных. Это позволяет идентифицировать информацию, необходимую для построения прогноза отказа критически уязвимых технических систем. С целью увеличения скорости обработки данных, применяется язык разработки C/C++, который позволяет взаимодействовать информационной системе с датчиками контроля показаниями. В качестве хранилища данных используются реляционная и нереляционная базы данных, позволяющие сохранять большие массивы информации и обеспечивать постоянный доступ к данным. Разработанная информационная система может быть использована в транспортных средствах с используемой системой контроля показаний в реальном времени.

Ключевые слова: анализ данных, большие данные, компьютерные системы, базы данных, модульное программное обеспечение, Big Data, Data Mining, коллекции данных, гибридные хранилища данных

Введение

Надежное функционирование современных, например, судовых сложных технических систем (СТС) [1-4] часто основывается на использовании удаленных программных решений по прогнозированию их работоспособности [5,6].

Для решения подобных задач используются клиент-серверные архитектуры, на основе сервера баз данных (БД), применяемых для хранения полученных данных, а также серверные анализаторы данных. Использование такой архитектуры позволяет выявлять неисправности в работе технической системы на ранних этапах ее выхода из строя, а также уменьшить вероятность отказа технической системы при несвоевременном ее обслуживании. Работоспособность клиент-серверного хранилища данных зависит от модели и структуры хранения данных. Использование реляционной модели относится к классической нотации для разработки клиент-серверных

приложений, ориентированных на структурное хранение данных. К основным преимуществам реляционных БД следует отнести:

- наличие языка манипулирования и описания данных (sql);
- разработанную систему оптимизации запросов, способную выполнять декомпозицию запросов, обеспечивая параллельное выполнение таких работ на кластерных архитектурах;
- использование механизма контроля, включающего атомарность, согласованность, долговечность и т.д.;
- присутствие общесистемных ресурсов, обеспечивающих работу реляционной архитектуры повсеместно.

Работа реляционной архитектуры использует единую структуру передачи транзакционного запроса от пользователя с дальнейшей его обработкой системой управления базами данных (СУБД), а также модели хранения данных, применяемых в различных условиях. Главными составляющими, обеспечивающими дальнейшую работу пользователей с данными, при помощи которых выполняется проверка на права доступа, организацию, структуру и прочее, являются базы метаданных. Физическое расположение данных также обеспечивает база метаданных, формирующая схему распределения и контроля изменений в хранилище данных.

В связи с усложнением задач диагностирования состояния СТС, связанных с генерацией большего объема данных для оценки текущего состояния объектов диагностирования, использование классических реляционных хранилищ привело к существенному повышению требований к кластерным архитектурам. В результате возросли сложности задач, решаемых реляционными БД. Существующие проблемы в подобных системах стали проявляться более значимо, что привело к усугублению недостатков использования подобной архитектуры. Одной из весомых проблем стала потеря соответствия данных. Ее проявление выражается в том, что реляционные БД не позволяют хранить агрегаты в явном виде, что существенным образом влияет на распознавание таблиц при их постоянном росте. В связи с этим усложняется связывание таблиц при выполнении запроса и, как следствие, осложняется формирование агрегата. Второй весомой проблемой является масштабирование данных. Это связано с использованием дорогостоящих аппаратно-программных комплексов, необходимых для работы параллельных систем БД и дальнейшей поддержкой отказоустойчивости. Чем сложнее формируются запросы в БД, тем больше падает производительность системы, связанная с межмашинным обменом данными в кластерной архитектуре.

Немаловажной составляющей, связанной с использованием реляционной архитектуры БД, является сложность модификации или реорганизации соответствующих таблиц при необходимости. Это достаточно весомый недостаток архитектуры, так как он не позволяет в кратчайшие сроки исправить ошибку, которая могла быть совершена на начальных этапах. Полное изменение всей схемы данных, а также модификация таблиц – это существенная проблема, которая может возникнуть.

Одним из решений проблемы реляционных БД является альтернативная технология, позволяющая хранить данные нереляционными методами, получившая название «NoSQL». Согласно [7], существует две причины, при которых использование нереляционной архитектуры является актуальным:

- эффективность разработки приложений (использование БД в качестве основного хранилища данных является стандартным решением, однако много времени уходит на отображение данных из структур, хранящихся в БД; использование нереляционной архитектуры может обеспечить уменьшение объемов кода, упростить последующую отладку приложения, а также обеспечить общее взаимодействие БД и программного решения);
- работа с большими объемами данных (использование реляционных архитектур является достаточно дорогостоящим и сложным решением в случаях, когда объемы

хранимых данных велики, что связано с архитектурными особенностями реляционных БД, которые изначально планировались для стационарного использования, а позже были доработаны до серверных реалий, однако использование кластерных серверов является сложным техническим условием, при котором реляционная архитектура не эффективное решение, как от него требуют разработчики) [8].

Нереляционные БД изначально созданы для использования на кластерных решениях. От этого повышается эффективность их использования, общее масштабирование, а также возможность работы с большими объемами удаленной информации. В связи с этим требуется разработать единое решение, направленное на повышение эффективности использования методов диагностирования СТС, а также обеспечить возможность удаленного прогнозирования их технического состояния.

С ростом использования технологических решений, основанных на архитектуре «Big Data», возникли противоречия, связанные с необходимостью хранения больших объемов неструктурированных данных с целью дальнейшего их структурирования методами разработки схемы БД. В результате развитие реляционных архитектур приостановлено из-за сложности добавления новых решений, а также изменившейся логики работы таких систем. Сегодня не используются прямые запросы в БД. Произошли глобальные изменения в пользовательских интерфейсах и моделях их использования, растет популярность веб-архитектур, требующих более сложные и гибкие решения в области хранения и работы с данными.

Целевой задачей Data Mining является осуществления поисковых операций, применяемых к законам поведения и общего функционирования исследуемой системы, состоящей из числовых данных. Обязательное условие, возникающее при использовании методологий Data Mining, заключается в трактовке полученных закономерностей, сформированных в результате определения практической полезности данных. В связи с этим возникает необходимость в разработке метода оптимизации большого объема данных, позволяющего распределять показания состояния СТС. Метод должен основываться на использовании разнотипных хранилищ данных, а также работать в высоконагруженной сети [9].

Целью работы является разработка метода оптимизации обработки большого объема данных, получаемых вследствие диагностирования СТС, позволяющего обеспечить сбор и обработку больших объемов информации в высоконагруженных сетях с учетом реального времени.

Основная часть

Разрабатываемый метод основан на использовании набора алгоритмических согласованностей. Они направлены на идентификацию информации в высоконагруженных сетях и ее обработку в моменты передачи от СТС к центральному хранилищу данных. Такие решения образуют единый комплекс, являющийся информационной системой, способной функционировать как дополнительная составляющая для оценки и прогнозирования состояния СТС.

Одним из требований к информационной системе, ориентированной на анализ данных, является своевременное обеспечение аналитической информацией, необходимой для принятия решения. Все собранные данные требуют дополнительной операции обработки – очистки. При использовании очистки может происходить процесс удаления выбросов (нехарактерных и ошибочных значений), обработка отсутствующих значений параметров, выполнение численного преобразования и т.д. На рис. 1 представлен алгоритм, реализующий разработанный метод анализа большого объема данных. Использование подобного решения позволяет собирать аналитические данные и выполнять предварительную их оценку за счет использования алгоритмов интеллектуального анализа данных. Разработанное решение применяется для контроля

состояния СТС. Для предотвращения трудностей, возникающих вследствие непрерывных изменений данных и проблемы контроля за СТС со стороны аналитика, используется технология Data Mining, направленная на сбор данных с рабочего окружения технической системы, с возможностью динамического масштабирования. В целях повышения эффективности системы анализа, применены алгоритмы самостоятельного обучения, обеспечивающие системе автономность от внешнего воздействия.

Использование алгоритмов, способных обучаться в процессе своей работы, активно применяют при решении задач классификации с обучением. Классификация с обучением подразумевает следующие действия:

- подготовка данных (имеющийся набор объектов с известными метками классов разбивается на две части: обучающую выборку и тестовую выборку);
- обучение модели (параметры модели классификации подбираются на основе обучающей выборки таким образом, чтобы добиться наилучшего соответствия между предсказанными и фактическими метками классов);
- тестирование модели (полученная в результате обучения модель проверяется на достоверность, для чего вычисляется процент недостоверных результатов классификации объектов из тестовой выборки).

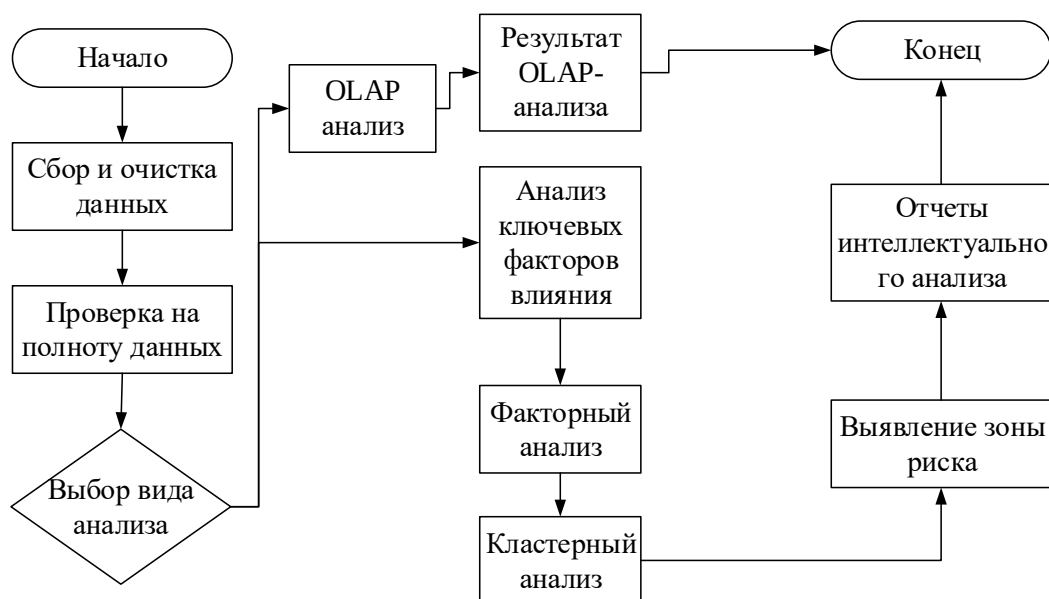


Рис. 1. Алгоритм, реализующий разработанный метод анализа данных в высоконагруженных сетях СТС

Целевой составляющей разработанной программной системы является извлечение структурированной информации из разно-структурированного хранилища данных. Такая задача является актуальной из-за повышения уменьшения работоспособности СТС при их эксплуатации в различных условиях, а также изменения конструктивной сложности таких систем. На практике применяются хранилища показаний работоспособности технической системы, имеющей строго структурированную структуру. Это обусловлено проблемой оперирования только структурированной информацией, которую используют такие методы анализа, как OLAP или Data Mining. Наиболее остро проблема извлечения информации возникает при работе с неструктурированными данными, имеющими текстовую форму, содержащими большие объемы информации и имеющие полезную форму.

Поисковый процесс включает в себя стадию поиска информационных ресурсов, являющихся релевантными задаче, с последующим извлечением из них исходных

коллекций данных. При этом ресурсы, принимающие участие в поиске, могут содержать в себе как структурированные, так и слабоструктурированные наборы данных. На следующем этапе данные пропускаются через средства анализа. Немаловажным является использование механизмов, способствующих увеличению скорости аналитической обработки. На рис. 2 представлены этапы, входящие в основу извлечения сущностей, которые формируются в разнотипных коллекциях данных и используются для дальнейшего анализа получаемой информации, необходимой для решения задачи классификации информации. В кластерных решениях, применяемых для обработки большого объема данных, использование коллекций является неотъемлемой составляющей при работе алгоритмов Hadoop.

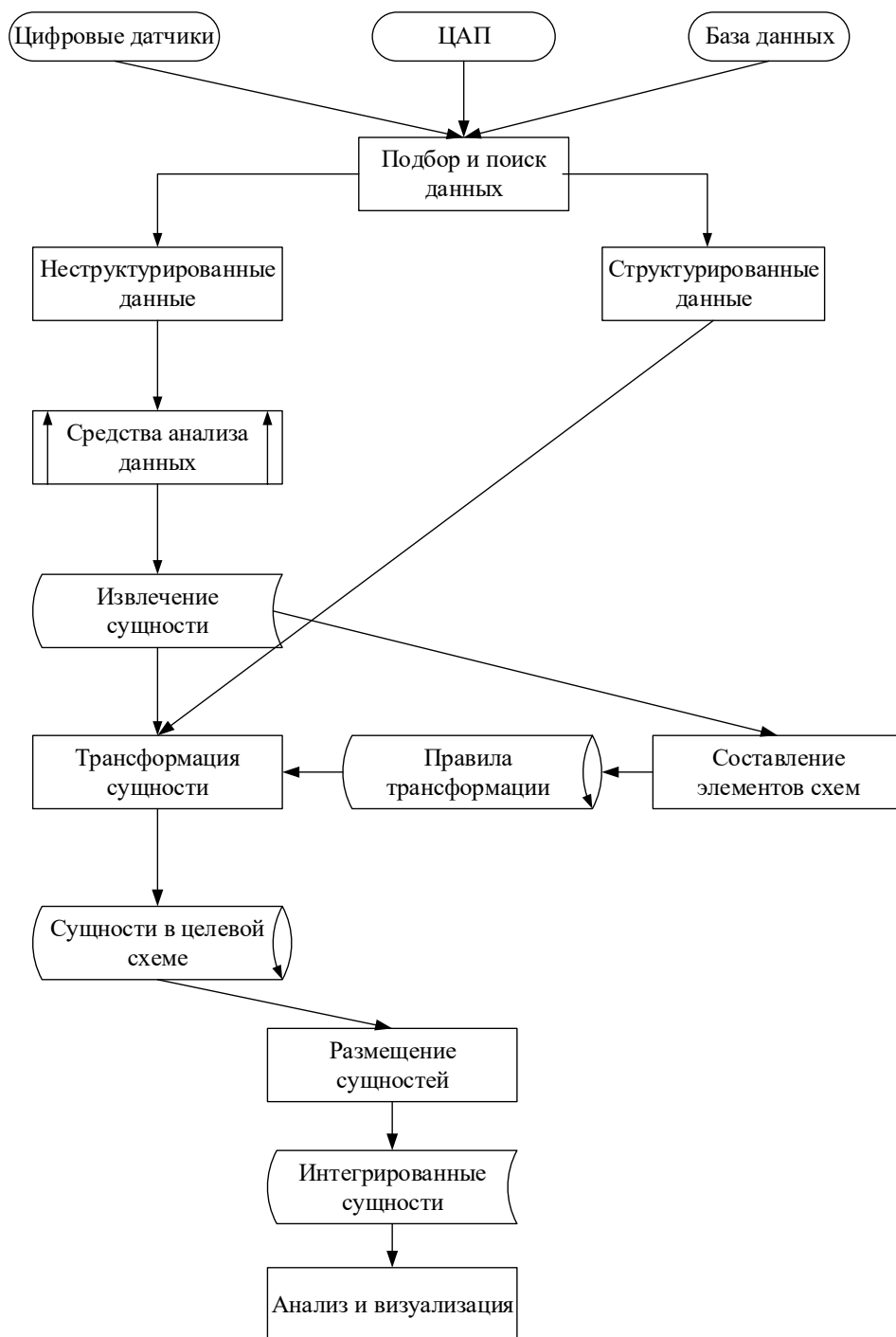


Рис. 2. Схема внутреннего анализа сущностей данных

По окончании процесса анализа, наступает процесс интеграции собранных коллекций, онтологий и извлеченных сущностей в общую интегрированную коллекцию. Первым этапом работы такой схемы является использования сопоставления элементов исходных схем и целевой схемы, в которой применяются различные методы автоматизации. Все эти правила применяются для трансформации данных, использующих более тонкие методы интеграции. Одним из таких методов является метод расширения сущностей, позволяющий установить сходство сущностей между собой. По окончании использования методов расширения наступает процесс слияния данных, содержащий информацию об одной сущности реального состояния СТС, сформированной из различных источников данных.

Процесс аналитической обработки, используемый для работы репрезентативной выборки, формируется из двух частей: построение модели и использование построенной модели для новых наборов данных. Процесс, строящий модель, является достаточно ресурсоемкой задачей, которая может изменяться в зависимости от применяемого алгоритма и включает в себя кеширование, сканирование, расчет множества вспомогательных параметров и т.д.

Использование уже готовых моделей к новым данным требует намного меньше ресурсов в связи с упрощенной работой с вычислением простых функций. Из этого следует, что использование небольших множеств данных может давать существенный результат при вычислении разноструктурных наборов данных и влиять на временные интервалы, выделяемые на расчет и анализ информации в базах данных. В качестве практического метода, используемого для построения и получения результатов от репрезентативных выборок, применяют сэмплинг. Его главной особенностью является сохранение скорости аналитической обработки данных без потери качества результирующего анализа.

Выводы

В результате анализа современных методов обработки разноструктурированной информации в высоконагруженных сетях разработан метод оптимизации обработки большого объема данных, решающий проблему диагностирования состояния оборудования в СТС. Основой метода является информационная система, способная извлекать и анализировать потоки информации в высоконагруженных сетях передачи данных и использовать полученную информацию для дальнейшего прогнозирования состояния СТС.

Работоспособность информационной системы основывается на применении гибридных алгоритмов поиска и сортировки данных, концепции Data Mining, а также математических алгоритмов для работы с большими объемами данных.

Список литературы

1. Вычужанин, В.В. Повышение эффективности эксплуатации судовой системы комфортного кондиционирования воздуха при переменных нагрузках. Монография / В.В. Вычужанин. — Одесса: ОНМУ, 2009. — 206 с.
2. Вычужанин, В.В. Математические модели нестационарных режимов воздухообработки в центральной СКВ / В.В. Вычужанин // Вісник Одеського національного морського університету, збірник наукових праць, 2007. — № 23. — С.172-185.
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. — Том 1, № 2 (67). — С. 18-22.

4. 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. Kononov // Восточно-Европейский журнал передовых технологий, 2016. — 6 (9). — Pp. 4-11.
5. Вычужанин, В.В. Информационное обеспечение мониторинга и диагностирования технического состояния судовых энергоустановок / В.В.Вычужанин // Вісник одеського національного морського університету, збірник наукових праць, 2012. — № 35. — С. 111-124.
6. Шibaева, Н.О. Информационное обеспечение дистанционной оценки рисков сложных технических систем / Н.О. Шibaева, В.В. Вычужанин // Информатика и математические методы в моделировании, 2016. — Том 6, № 2. — С. 133-141.
7. Кудрявцев, К.Я. Методы повышения скорости поиска информации в базах данных / К.Я. Кудрявцев, А.Е. Коротков // LAP Lambert Academic Publishing, 2012. — 84 с.
8. Samet, H. The Quadtree and Related Hierarchical Data Structures / H. Samet. // ACM Comput. Surv, 1984. — Pp. 187-260.
9. Arasu, A. Efficient exact set-similarity joins / A. Arasu, V. Ganti, R. Kaushik // Proceedings of the 32nd international conference on Very large data bases. VLDB '06. VLDB Endowment, 2006. — Pp. 918-929.

ОПТИМІЗАЦІЯ МЕТОДІВ ПРОГНОЗУВАННЯ, ОБРОБКИ ТА АНАЛІЗУ ІНФОРМАЦІЇ В РІЗНОСТРУКТУРНИХ СХОВИЩАХ ДАНИХ

Д.С. Шibaев, В.В. Вычужанин, Н.О. Шibaева, Н.Д. Рудниченко

Одеський національний морський університет,
вул. Мечнікова, 34, Одеса, 65029, Україна; e-mail: denshibaev@outlook.com

У статті запропоновано метод оптимізації обробки великого обсягу даних, призначений для діагностування стану устаткування складних технічних систем. Таке діагностування дозволяє підвищити ефективність аналізу несправностей в технічних системах з метою їх якнайшвидшого усунення. Це досягається за рахунок прогнозування відмови критично уразливих систем, здатних вивести з експлуатації транспортний засіб, або призвести до наслідків, що загрожують життю людей. Метод реалізований в інформаційній системі, заснованій на наборі алгоритмічних узгодженостей, спрямованих на ідентифікацію інформації в високонавантажених мережах та її обробку в моменти передачі від складних технічних систем до центрального сховища даних. Функціонування інформаційної системи ґрунтується на застосуванні гібридних алгоритмів пошуку та сортування даних, концепції Data Mining, а також алгоритмів для роботи з великими обсягами даних. Методи відбору і розподілу даних виконуються на рівні контролю показань датчиків технічної системи і розподіляються до моменту запису в сховище даних. Це дозволяє ідентифікувати інформацію, необхідну для побудови прогнозу відмови критично вразливих технічних систем. З метою збільшення швидкості обробки даних, застосовується мова розробки C/C++, яка дозволяє взаємодіяти інформаційній системі з датчиками контролю показників. В якості сховища даних використовуються реляційне та нереляційне сховище даних, що дозволяє зберігати великі масиви інформації і забезпечувати постійний доступ до даних. Розроблена інформаційна система може бути використана в транспортних засобах з системою контролю показників в реальному часі.

Ключові слова: аналіз даних, великі дані, комп'ютерні системи, бази даних, модульне програмне забезпечення, Big Data, Data Mining, колекції даних, гібридні сховища даних

OPTIMIZATION OF PREDICTION METHODS, PROCESSING AND ANALYSIS OF INFORMATION IN DIFFERENT STRUCTURE DATA

D.S. Shibaiev, V.V. Vychuzhanin, N.O. Shibaieva, N.D. Rudnichenko

Odesa National Maritime University,
34, Mechnikova Str., Odesa, 65029, Ukraine; e-mail: denshibaev@outlook.com

In article the method of optimization of processing of a large volume of the data intended for diagnostics of a condition of the equipment of difficult technical systems is offered. Such diagnostics allows to increase the efficiency of the analysis of faults in technical systems with a view to their early elimination. This is achieved by predicting the failure of critically vulnerable systems capable of decommissioning the vehicle, or lead to consequences that threaten people's lives. The method is implemented in an information system based on a set of algorithmic consistency aimed at identifying information in high-load networks and its processing at the time of transmission from complex technical systems to the Central data warehouse. The functioning of the information system is based on the use of hybrid algorithms for searching and sorting data, the concept of Data Mining, as well as algorithms for working with large amounts of data. The methods of data selection and distribution are carried out at the level of sensor readings control of the technical system and distributed until recording in the data warehouse. This allows to identify the information necessary for the prediction of failure of critically vulnerable technical systems. In order to increase the speed of data processing, the C\C++ development language is used, which allows the information system to interact with the reading control sensors. As a data warehouse uses the relational and not relational database, allowing to save large amounts of data and provide constant access to data. The developed information system can be used in vehicles with the system used to monitor the readings in real time.

Keywords: data analysis, big data, computer systems, databases, modular software, Big Data, Data Mining, data collections, hybrid data stores

ПОДДЕРЖКА ПРИНЯТИЯ РЕШЕНИЙ О РЕАЛИЗАЦИИ ПРИЛОЖЕНИЙ В ГИБРИДНОЙ ОБЛАЧНОЙ ИНФРАСТРУКТУРЕ

Л.А. Волощук, О.И. Розновец, Д.Д. Волощук

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

Облачные технологии и платформы активно развиваются и становятся все более востребованными. Наибольшую популярность последнее время завоевывают гибридные облака и мультиоблачные услуги, в которых реализуется распределенное размещение ИТ-инфраструктуры предприятия частично на облачных платформах, частично на территории заказчика. Для принятия решения о возможности частичной миграции ИТ-инфраструктуры в облако возникает задача выбора правильного сочетания частных и облачных решений в единой архитектуре приложений и, собственно, ИТ-среде предприятия в целом. Современный подход к проектированию ИТ-приложений и комплексов предполагает реализацию модульной, многозвенной архитектуры, в которой каждый модуль системы обладает определенной функциональностью, набором собственных методов и свойств и предполагает соблюдение определенных технических требований к своей реализации и реализации связей с другими компонентами архитектуры. Технические требования могут быть определены соответствующими критериями и их значимостью при различных способах и платформах размещения подсистем. Интегрированная оценка технической возможности работы в гибридном облаке подсистем приложения ИТ-среды предприятия может быть получена путем проведения многокритериального анализа и выбора лучшего решения. В статье рассмотрены вопросы построения гибридной облачной инфраструктуры ИТ-среды предприятия, оценки технической возможности и эффективности проведения частичной миграции в публичное облако приложений и их подсистем. Предложена методика оценки эффективности миграции, основанная на структурно-функциональной декомпозиции архитектуры приложения, анализе технической возможности миграции подсистем приложения в соответствии с выбранной совокупностью критериев и, собственно, оценке эффективности миграции. Оценка эффективности проводится с применением метода анализа иерархий. Применение методики позволяет формализовать и упростить процесс принятия решения о целесообразности и эффективности построения гибридной облачной инфраструктуры приложения.

Ключевие слова: гибридные облачные платформы, миграция приложения в облако, оценка эффективности миграции в облако

Введение

Особое место в современных направлениях развития информационных технологий занимают облачные технологии и платформы. Облачная парадигма формирует обширный рынок: появилось большое число крупных провайдеров облачных сервисов, включая Amazon, Google, Microsoft, Salesforce и Yahoo. Ведущие производители СУБД IBM и Oracle обеспечивают поддержку облаков в своих продуктах, что не может не привлечь интерес широкого круга исследователей к решению задач миграции корпоративных приложений в облачную инфраструктуру.

С понятием облачных вычислений связывают такие сервис-предоставляющие технологии, как:

- инфраструктура как сервис («Infrastructure as a Service» или «IaaS»);
- платформа как сервис («Platform as a Service», «PaaS»);
- программное обеспечение как сервис («Software as a Service» или «SaaS»).

Эти технологии при совместном использовании позволяют пользователям облачных вычислений воспользоваться вычислительными мощностями и хранилищами данных, которые посредством определенных технологий виртуализации и высокого уровня абстракции предоставляются им как услуги.

Помимо различных способов предоставления сервисов различают несколько вариантов развёртывания облачных систем:

- частное облако (private cloud) – используется для предоставления сервисов внутри одной компании, которая является одновременно и заказчиком, и поставщиком услуг. Это вариант реализации «облачной концепции», когда компания создает ее для себя самой, в рамках организации;
- публичное облако (public cloud) – используется облачными провайдерами для предоставления сервисов внешним заказчикам;
- смешанное облако (hybrid cloud) – совместное использование двух вышеперечисленных моделей развёртывания.

Одна из ключевых идей облачных технологий заключается как раз в том, чтобы с технологической точки зрения разницы между внутренними и внешними облаками не было и заказчик мог гибко перемещать свои задания между собственной и арендуемой ИТ-инфраструктурой, не задумываясь, где конкретно они выполняются.

Наиболее востребованными в последнее время стали облачные сервисы IaaS и SaaS, однако, главный тренд 2017 года – популярность гибридных облаков и мультиоблачных услуг [3]. Гибридные облака предполагают размещение инфраструктуры частично на территории заказчика, частично в публичном облаке. Мультиоблачные услуги предоставляют заказчику возможность разделить свою информационную систему и передать ее на поддержку облачным провайдерам в разных инфраструктурах, которые затем будут синхронизированы. Последние исследования Gartner показали, что 70 процентов предприятий будут внедрять стратегию с несколькими облаками к 2019 году [4].

Таким образом, гибридная облачная инфраструктура видится в качестве ключевой стратегии в будущем, а компании, которые смогут реализовать лучшее сочетание публичного и частного облаков в своей ИТ-среде, получат долгосрочные преимущества [1,2].

На этапе принятия решения о возможной частичной миграции в облако возникает сложная задача – найти и выбрать правильное сочетание частных и общедоступных облачных решений в единой ИТ-среде предприятия, в том числе модернизируемом или создаваемом приложении, для эффективного удовлетворения потребностей бизнеса. Решение этой задачи требует тщательного анализа архитектуры перемещаемого приложения на основании совокупности технических атрибутов, критериев их оценки и, собственно, методологии и модели принятия окончательного решения.

Цель работы – разработка методики принятия решения о частичной миграции в публичное облако подсистем приложений ИТ-среды предприятия на основании оценки технической эффективности перехода на облачную платформу.

Основная часть

Решение об использовании «облачных» вычислений должно приниматься с учетом состояния собственной информационной системы предприятия. Можно выделить три основных состояния информационной системы:

- на предприятии приняты все необходимые меры по модернизации информационной системы, которая отвечает всем требованиям к ее эффективности;
- информационная система неэффективна или проводится реинжиниринг бизнес-процессов;
- информационная система находится на стадии создания, например, на новом предприятии.

В первом случае с экономической точки зрения переход в «облака» не является оправданным, в такой ситуации может быть целесообразным перенос в «облака» новых сервисов, которые будут появляться, а также разработка концепции перехода к облачным сервисам в будущем.

Во втором и особенно третьем случае перенос информационного обслуживания в «облака» может оказаться наиболее приемлемым шагом построения эффективных информационных сервисов предприятия. Для новых предприятий выбор в пользу облачного обслуживания может дать максимально возможный экономический и технологический эффекты.

Использование публичных облачных платформ в течение последнего десятилетия показало, что чрезмерная зависимость от публичного облака приводит к проблемам:

- понижения производительности;
- увеличения стоимости или снижения контроля;
- в некоторых случаях дорогостоящим миграциям назад из публичного облака.

Стало очевидным, что публичное облако лучше для более традиционных бизнес-приложений и основные направления использования публичного облака это [12]:

- хранение данных, в том числе хранение файлов и базы данных;
- резервное копирование данных;
- аварийное восстановление;
- облачная аналитика;
- программное обеспечение как услуга (SaaS);
- управление взаимоотношениями с клиентами (CRM);
- использование «облака» как инструмента совместной работы;
- организация удаленной работы.

Частичный перенос ИТ-инфраструктуры компании в публичное облако может быть обоснован также следующими причинами:

- необходимостью обеспечить отказоустойчивость критичных сервисов;
- необходимостью освобождения локальных ресурсов путем переноса второстепенных сервисов в облако;
- необходимостью масштабирования ресурсов;
- реализацией плавного перехода к полной миграции;
- переносом требовательных к производительности узлов инфраструктуры с целью освобождения от дополнительных затрат на оборудование сети компании;
- возможностью использования облачных сервисов и служб.

С другой стороны, приложения с интенсивными данными и чувствительными к задержкам требованиями будут работать лучше в локальной физической ИТ-среде предприятия.

Таким образом, очевиден факт необходимости правильного сочетания общедоступного и частного в гибридной облачной инфраструктуре, при которой будет:

- оптимизирована производительность;
- соблюдены условия безопасности;
- обеспечен быстрый, удобный доступ к ИТ-сервисам в рамках общедоступного облака;
- доступны безопасные, совместимые службы в частном облаке;
- сохранен легкий доступ к устаревшим приложениям в традиционной ИТ-инфраструктуре;

– соблюдено целесообразное соответствие стоимости/качества предоставляемых услуг.

Общепринятая схема миграции в публичное облако освещена достаточно широко и предполагает следующую последовательность этапов [5,6]:

1. Выполнение инвентаризации существующего ИТ-окружения и определение модели облака.
2. Поиск, оценка и выбор облачного провайдера с последующим тестированием возможностей облачной площадки и выполнением тестовой миграции.
3. Составление плана или дорожной карты миграции, которые позволяют контролировать все выполняемые шаги на пути «переезда» в облако.
4. Процесс миграции.
5. Выполнение проверки и тестирования перенесенных сервисов.

Приведенная схема миграции, являясь достаточно общей, не отражает глубинных особенностей принятия решений при оценке пригодности для миграции в облако отдельных подсистем приложений, технической сложности ее проведения. Анализ, оценка и построение гибридной облачной архитектуры приложения должны быть проведены уже на этапе 1.

Именно на первом этапе необходимо оценить текущую картину имеющейся инфраструктуры и отдельных приложений. Необходимо выполнить определение всех компонентов – какие из них являются важными, какие вспомогательными, как компоненты взаимодействуют друг с другом. Оценить с помощью интегральной модели оценки, системы критериев и их значимости, возможность и целесообразность миграции в публичное облако отобранных приложений, подсистем или их компонентов. Наличие такой документации облегчит процесс миграции и упростит задачу тестирования всех перенесенных в облако систем.

Для принятия решения на первом этапе вышеприведенной схемы миграции в облако о возможности частичной миграции подсистем приложений с точки зрения технической возможности и целесообразности может быть предложена методика, содержащая следующую последовательность шагов:

Шаг 1. Инвентаризация ИТ-окружения, в ходе которой нужно категоризировать каждое приложение и подсистему один за другим на основании атрибутов.

Шаг 2. Рассмотреть и отобрать из выделенных приложений и подсистем кандидатов на перенос в публичное облако с точки зрения экономической целесообразности и безопасности.

Шаг 3. Составить функционально-структурную детализацию архитектуры для каждого выделенного приложения, а также карту связей основных его модулей и подсистем.

Шаг 4. Для каждого приложения и подсистемы, миграция которого целесообразна, провести аудит технической возможности миграции с применением совокупности технических критериев, соответствующей данному типу модуля.

Шаг 5. Провести оценку эффективности миграции в публичное облако, основываясь на выбранной модели принятия решения.

Рассмотрим шаги предложенной методики подробнее.

Инвентаризация ИТ-окружения на шаге 1 является частным процессом, индивидуальным для каждого предприятия, в ходе которого определяется перечень и аппаратно-системные требования отдельных программных систем и комплексов, обслуживающих бизнес-процессы предприятия.

Экономическая целесообразность использования облачной инфраструктуры на шаге 2 сегодня в большинстве случаев является очевидной, а стоимостная политика предоставления облачных услуг, как и гарантии безопасности данных, формируется непосредственно облачным провайдером. Решения, принимаемые на этом этапе можно определить как подход «сверху-вниз» [7], который позволяет понять, где приложения

принесут пользу бизнесу. Подход «сверху-вниз» следует парадигме трансформации бизнеса с целью реализации максимального потенциала, поэтому основывается на оценке финансовой выгоды с учетом сезонных скачков активности пользователей, необходимых уровней масштабируемости, отказоустойчивости и, конечно, аспектов безопасности каждого приложения.

Особый интерес для исследования и разработки гибридной облачной платформы приложения с технической точки зрения представляет шаг 3. Проведение на этом шаге структурно-функциональной декомпозиции приложения можно определить, как подход «снизу-вверх» [7], который фокусируется на технических требованиях отдельных модулей и подсистем переносимого в облако приложения и позволяет получить гибридную облачную архитектуру приложения.

Архитектура приложения влияет на способ миграции приложения в облачную среду, а иногда на саму возможность миграции. Большинство корпоративных приложений строятся с использованием нескольких уровней, чтобы разделить основные функции и модули системы [8]. Классический подход предусматривает создание приложения с тремя следующими базовыми уровнями:

- уровень управления данными, который состоит из компонентов реляционных и других баз данных;
- уровень бизнес-логики, который использует платформу приложений или контейнеры, такие как Java EE или Microsoft .NET;
- уровень представления, отвечающий за взаимодействие с пользовательскими интерфейсами и другими внешними системами, включая управление состоянием и данными для представления этим внешним системам.

Приложения, для создания которых применяется многоуровневый подход к организации архитектуры, имеют четко определенные интерфейсы между этими уровнями. В некоторых случаях особенности использования приложений делают возможным миграцию отдельных уровней или модулей программы. Например, статическое содержание веб-приложения можно перенести в инфраструктуру сети доставки информации, что позволит быстрее загружать компоненты сайта.

В другой ситуации, ограничение пропускной способности глобальной сети может помешать разделению уровней, что приведет к решению о миграции в «облако» всех уровней приложения.

Уровни приложения также могут иметь различные требования по безопасности и зонированию. Например, для защиты некоторых данных программы может потребоваться применение брандмауэра.

Общий вид архитектуры приложения [8], компоненты которого сгруппированы по функциональным областям структуры системы, где система представляет набор компонентов, выполняющих определенную функцию или набор функций, представлен на рис. 1.

Представленный вид архитектуры описывает функции, слои и уровни, которые могут присутствовать в приложении. Эффективное разделение функциональности достигается за счет применения многослойного архитектурного стиля, который позволяет отделить логику представления от бизнес-логики и логики доступа к данным. Многослойная архитектура представляет систему как единое целое, обеспечивая при этом достаточно деталей для понимания ролей и ответственностей отдельных слоев и отношений между ними. Функциональность каждого слоя объединена общей ролью или ответственностью. Слои слабо связаны, но между ними осуществляется явный обмен данными. Правильное разделение приложения на слои помогает поддерживать строгое разделение функциональности, что в свою очередь обеспечивает гибкость, удобство и простоту проведения оценки технической возможности миграции в облако. Например, чтобы понять, как масштабируется всё приложение, необходимо рассмотреть как каждый отдельный слой в архитектуре поддерживает

масштабирование, при этом под масштабированием понимаем возможность обслуживания пользователей со стороны приложения при существенном приросте их количества.

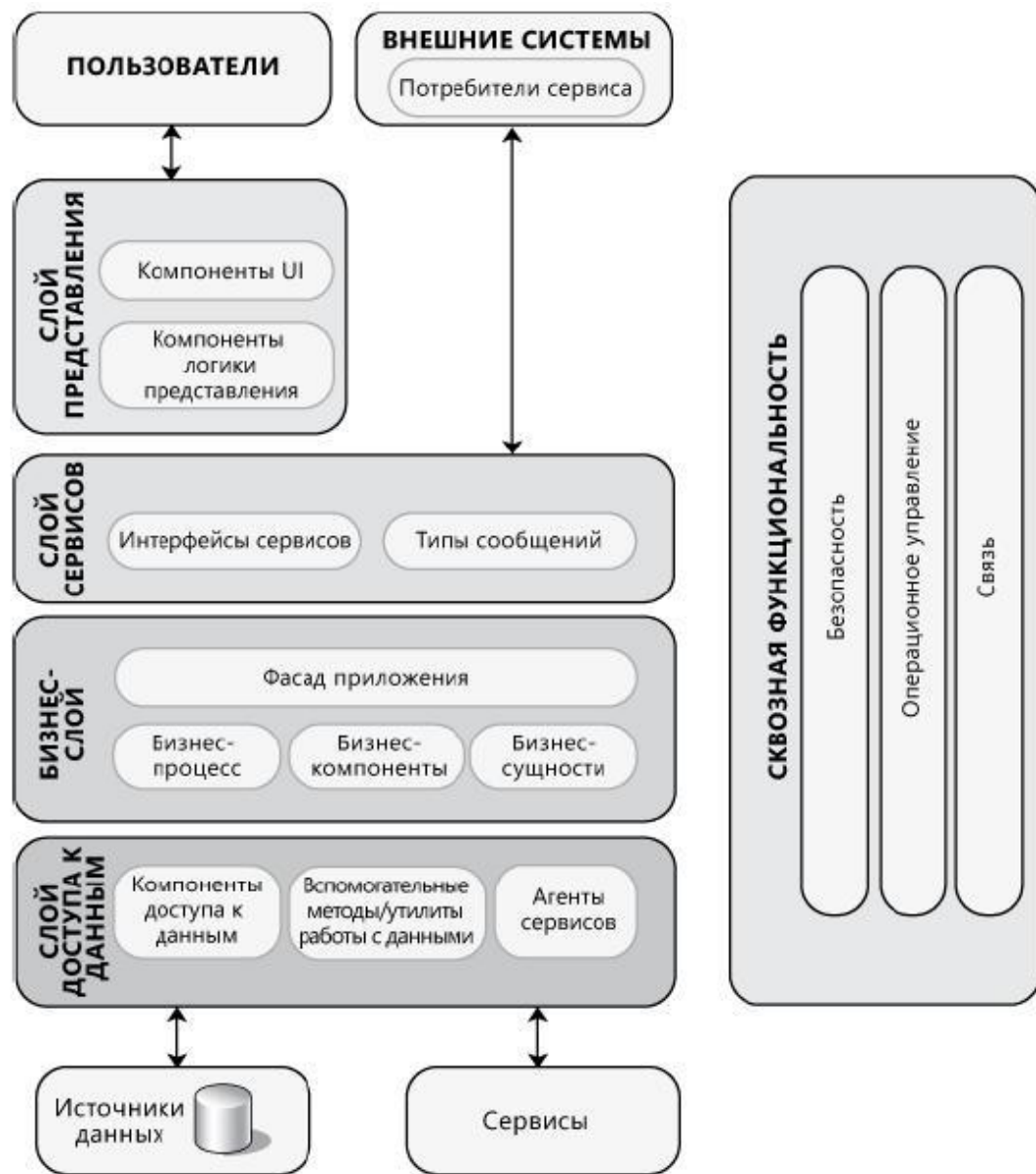


Рис. 1. Общий вид архитектуры приложения (слои, компоненты, сервисы)

Таким образом, структурно-функциональная декомпозиция архитектуры приложения позволяет определить необходимые функциональные возможности и технические требования каждой из входящих в него подсистем, целесообразность частичной миграции их на облачную платформу и оценку ее эффективности.

На шаге 4 для количественного и качественного анализа технической возможности миграции на облачную платформу необходимо составить экспертную совокупность значимых критериев и подкритериев оценки различных аспектов работоспособности выделенных подсистем приложения.

Такой подход известен и изложен в статье [9]. Оценку возможности миграции в публичное облако неделимого приложения предлагается в статье проводить в трех измерениях – «бизнес ценность», «степень риска», «техническая возможность».

Каждое из этих измерений имеет несколько критериев, которые, в свою очередь, могут иметь несколько уровней подкритериев.

Что касается оценки технической возможности миграции приложения, авторами предлагается проводить ее в соответствии с четырьмя критериями: «простота интеграции», «простота миграции», «технологический стек», «дизайн приложения».

Учитывая большое количество архитектурных вариантов приложений и их многозвенность, значительное разнообразие облачных сервисов и служб у разных облачных провайдеров, расхождение в технологических требованиях доступа к ним, предложенная совокупность критериев не является достаточной и обоснованной.

Для выбора совокупности технических критериев миграции в «облако» необходимо рассмотреть и проанализировать технические характеристики и параметры, которые в значительной степени влияют на работу приложения, соответствуют функциональной направленности его подсистем, а также выявить базовые характеристики облачных сред, которые осуществляют наибольшее влияние на возможность работы приложения и его подсистем в данной среде.

В результате проведенного исследования и анализа «облачных» сред, а также рекомендаций сервис-провайдеров были отобраны такие критерии, как «Хранение данных», «Требования к доступу».

Критерий «Хранение данных» включает подкритерии:

- продолжительность хранения данных;
- доступ к данным;
- централизация данных;
- масштабируемость;
- формат хранения данных.

Критерий «Требования к доступу» оценивает параметры доступа следующими подкритериями:

- высокая доступность;
- степень пульсации трафика;
- протокол;
- объем передаваемых данных.

Рассмотрим критерий «Хранение данных» и его подкритерии более подробно. Этот критерий необходим для оценки требований к подсистемам хранения данных приложения. Поскольку в приложении могут использоваться различные способы хранения данных, такие как реляционные базы данных, большие двоичные объекты, текстовые файлы и другие, то важную роль могут играть требования к продолжительности хранения данных, так как это будет сказываться на темпах роста объема общей совокупности данных, необходимости резервного копирования.

Также нужно учитывать такой параметр, как доступ к данным, под которым будем понимать нагрузку на базу данных, количество транзакций в секунду, причем при принятии решения о миграции необходимо знать каким может быть пиковая нагрузка и сможет ли облачная среда обеспечить корректную работу базы данных при этих показателях.

Подкритерием «централизация данных» оценивается требование централизованного хранения данных или же данные могут храниться распределенно.

Подкритерий «масштабируемость» оценивает возможность масштабирования базы данных по мере ее разрастания. Часто многие приложения ориентированы на специфические форматы хранения данных, что также может сказываться на условиях переноса программы в облачную среду.

Критерием «Требование к доступу» оценивается критичность технических параметров доступа к приложению.

Подкритерий «высокая доступность» определяет требование к степени доступности к приложению – 24 часа в сутки и 7 дней в неделю или же допускается,

что приложение может быть в какие-то моменты времени недоступно, например, по техническим причинам.

Подкритерием «степень пульсации трафика» оцениваются нагрузки на сеть с целью определения возможности обеспечения облачным провайдером необходимой пропускной способности, в том числе в моменты пиковых нагрузок.

Кроме этого в приложениях нередко используются специфические протоколы, которые не всегда могут поддерживаться облачными провайдерами. Также необходимо учитывать тот факт, что различные сервис-провайдеры используют различные протоколы доступа к своим сервисам.

Объем переданных данных всегда играет важную роль в оценке технической возможности миграции приложения в облако, хотя тарифицируются только выходные с ЦОД данные, в случае, когда необходимо обеспечить потоковую передачу больших объемов данных с ЦОД, оплата выходных данных становится заметным фактором роста расходов.

Предложенная совокупность критериев оценки технической возможности миграции в «облако» может в каждом конкретном случае дополняться другими критериями и подкритериями в соответствии с предпочтениями ИТ-экспертов и предоставляемыми условиями выбранных облачных провайдера.

Получение интегрированной оценки пригодности (технической возможности) работы в «облаке» подсистемы приложения (или отдельного приложения ИТ-среды предприятия) предполагает проведение многокритериального анализа и выбора лучшего решения. Для решения этой задачи на шаге 5 предложенного подхода предлагается использовать метод анализа иерархий (МАИ) [10,11].

Процесс использования МАИ для оценки пригодности для работы в облаке подсистем приложения может быть представлен следующей последовательностью действий:

- определение иерархии критериев оценки технической возможности;
- определение приоритетов критериев и подкритериев;
- оценка подсистемы приложения по набору критериев;
- вычисление общей МАИ-оценки для каждой подсистемы.

Определение иерархии возможных технических критериев приведено на рис.2.

Верхний уровень – глобальная цель – оценка пригодности подсистем приложения для работы в «облаке». На уровне 2 иерархии – базовые критерии «Хранение данных» и «Требования к доступу». Далее подкритерии уровня 3. Для критерия «Хранение данных» подуровень 3 включает подкритерии: продолжительность хранения данных, доступ к данным, централизация данных, масштабируемость, формат хранения данных. Для критерия «Требования к доступу» на подуровне 3 рассматриваются подкритерии: высокая доступность, степень пульсации трафика, требования к протоколу, объем передаваемых данных.

Альтернативами выступают рассматриваемые подсистемы – кандидаты для переноса в публичное облако.

После формирования иерархии критериев оценки и их подкритериев определяется относительная важность самих критериев оценки. Для этого устанавливаются веса критериев на основе экспертной оценки, осуществляемой ИТ-экспертами, и осуществляется парное сравнение критериев друг с другом по их важности – вкладу в глобальную цель. На основании суждений эксперта строятся матрицы попарных сравнений на каждом уровне по отношению к каждому критерию вышестоящего уровня, вычисляются локальные приоритеты для критериев, локальные и глобальные приоритеты для каждого подкритерия.

На следующем этапе производится оценка альтернатив анализируемых подсистем, при этом они сравниваются между собой попарно по одному из критериев,

затем по другому, до тех пор, пока не будут использованы все критерии и для каждой подсистемы приложения рассчитывается относительный балл.

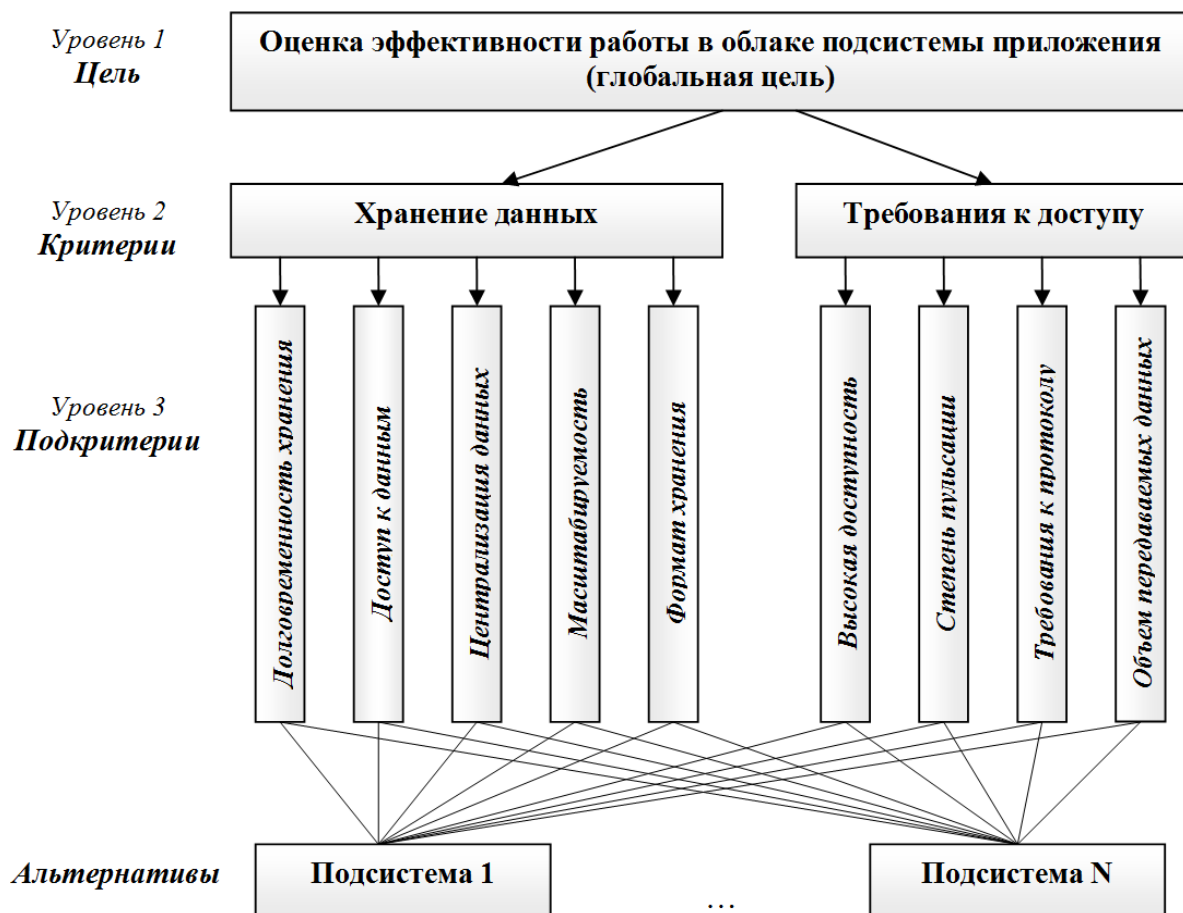


Рис. 2. Схематическое представление иерархии «цель–критерии оценки–альтернативы» МАИ для оценки технической возможности работы в облаке подсистем приложения.

Вычисление общей МАИ-оценки для каждой альтернативы – подсистемы приложения, рассчитывается, как сумма произведения его относительного приоритета по каждому критерию и относительного приоритета соответствующего критерия по формуле (1):

$$S_x = \sum_{i=1}^M \sum_{j=1}^{N_i} P_i p_{ij} s_{ijx}, \quad (1)$$

где S_x – МАИ-балл для x -й подсистемы приложения; M – число групп критериев; N_i – число элементов в i -ой группе критериев; P_i – значение приоритета i -ой группы критериев; p_{ij} – значение приоритета j -го критерия, принадлежащего i -ой группе критериев; s_{ijx} – балл сравнения x -й подсистемы приложения по j -му критерию в i -ой группе критериев.

Сравнение итоговых МАИ-оценок для каждой рассматриваемой подсистемы – кандидата для миграции в облако позволяет получить целостное представление о технической эффективности реализации гибридной облачной платформы и поможет принять обоснованное решение при модернизации ИТ-среды предприятия.

Выводы

Принимая во внимание, что популярность в корпоративной среде набирают гибридные облака, анализ технических атрибутов приложения и его подсистем приобретают особое значение. Критерии оценки технической возможности и целесообразности миграции играют важную роль в процессе проектирования гибридной облачной архитектуры приложения, подлежащего частичной миграции на облачную платформу. Вместе с тем, модели принятия решений о целесообразности перехода на облачную платформу, методы построения гибридных облачных архитектур приложений, системы показателей технических аспектов работы типовых подсистем разработаны недостаточно и носят индивидуальный частный характер в каждом конкретном случае миграции в «облако».

Предложенная методика оценки эффективности миграции подсистем приложения в «облако», предлагаемая в статье, основана на структурно-функциональной декомпозиции архитектуры приложения, анализе технической возможности миграции подсистем приложения в соответствии с выбранной экспертной совокупностью критериев и, собственно, оценкой эффективности миграции путем проведения многокритериального анализа с использованием метода анализа иерархий для выбора лучшего решения.

Применение методики оценки эффективности частичной миграции подсистем приложения в «облако» позволит формализовать и упростить процесс принятия решения о целесообразности и эффективности построения гибридной облачной инфраструктуры как для ИТ-среды предприятия, так и для отдельных его приложений.

Список литературы

1. Doebel, P. Hybrid IT: avoiding 'cloud cliff' by finding the right mix. Why Hewlett Packard Enterprise is banking on a shift towards hybrid IT adoption. Mode of access: <http://www.businesstimes.com.sg/hub/empowering-enterprise/hybrid-it-avoiding-cloud-cliff-by-finding-the-right-mix> (Date: 17.01.2018).
2. Малахов, В.Є. Сервіс-орієнтований інформаційний ресурс кафедри ВНЗ в гібридній хмарній інфраструктурі / В.Є. Малахов, Л.А. Волощук // Інформатика та математичні методи в моделюванні, 2017. — Т.7, №3. — С. 240-249.
3. Облачные сервисы 2017. [Электронный ресурс] // Режим доступа: <http://www.cnews.ru/reviews/cloud2017> (Дата обращения: 31.10.2017).
4. Gartner Says Worldwide Public Cloud Services Market to Grow 18 Percent in 2017. Mode of access: <https://www.gartner.com/newsroom/id/3616417> (Date: 22.02.2017).
5. Юдина, Е. Миграция в облако. [Электронный ресурс] // Режим доступа: <http://iaas-blog.it-grad.ru/tendencii/migraciya-v-oblako/> (Дата обращения: 08.11.2017).
6. Как компании перенести свою инфраструктуру в облако и избежать ошибок. [Электронный ресурс] // Режим доступа: <https://habrahabr.ru/company/it-grad/blog/337834/> (Дата обращения: 18.09.2017).
7. Kassner, E. How to get moving in your migration to the cloud. Mode of access: <https://azure.microsoft.com/ru-ru/blog/how-to-get-moving-in-your-migration-to-the-cloud/> (Date: 07.06.2016).
8. J.D. Meier, David Hill, Alex Homer, Jason Taylor, Prashant Bansode, Lonnie Wall, Rob Boucher Jr., Akshay Bogawat. Руководство Microsoft по проектированию архитектуры приложений. — 2009.
9. Бриджеш, Деб. Оценка пригодности корпоративных приложений для миграции в облако [Электронный ресурс] // Режим доступа: <https://www.ibm.com/developerworks/ru/library/cl-assessport/> (Дата обращения: 02.03.2017).
10. Саати, Т.Л. Принятие решений. Метод анализа иерархий / пер. с англ. Р.Г. Вачнадзе. — М.: Радио и связь, 1993. — 278 с.
11. Саати, Т.Л. Принятие решений при зависимостях и обратных связях: Аналитические сети: пер. с англ. — М.: Издательство ЛКИ, 2008. — 360 с.

12. Hybrid cloud (гибридные облака) [Електронний ресурс] // Режим доступа: http://www.tadviser.ru/index.php/Статья:Hybrid_cloud_%28гибридные_облака%29 (Дата обращения: 02.06.2017).

ПІДТРИМКА ПРИЙНЯТТЯ РІШЕНЬ ПРО РЕАЛІЗАЦІЮ ДОДАТКІВ В ГІБРИДНІЙ ХМАРНІЙ ІНФРАСТРУКТУРІ

Л.А. Волощук, О.І. Розновець, Д.Д. Волощук

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

Хмарні технології і платформи активно розвиваються і стають все більш затребуваними. Найбільшу популярність останнім часом завойовують гібридні хмари і мультіхмарні послуги, в яких реалізується розподілене розміщення ІТ-інфраструктури підприємства частково на хмарних платформах, частково на території замовника. Для прийняття рішення про можливість часткової міграції ІТ-інфраструктури в хмару виникає завдання вибору правильного поєднання приватних і хмарних рішень в єдиній архітектурі додатків і, власне, ІТ-середовищі підприємства в цілому. Сучасний підхід до проектування ІТ-програм та комплексів передбачає реалізацію модульної, багатоланкової архітектури, в якій кожен модуль системи має певну функціональність, набір власних методів і властивостей та передбачає дотримання певних технічних вимог до своєї реалізації і реалізації зв'язків з іншими компонентами архітектури. Технічні вимоги можуть бути визначені відповідними критеріями і їх значимістю при різних способах і платформах розміщення підсистем. Інтегрована оцінка технічної можливості роботи в гібридній хмарі підсистем додатку ІТ-середовища підприємства може бути отримана шляхом проведення багатокритеріального аналізу і вибору кращого рішення. У статті розглянуті питання побудови гібридної хмарної інфраструктури ІТ-середовища підприємства, оцінки технічної можливості та ефективності проведення часткової міграції в публічну хмару додатків і їх підсистем. Запропоновано методику оцінки ефективності міграції, яка заснована на структурно-функціональній декомпозиції архітектури додатку, аналізі технічної можливості міграції підсистем додатка відповідно до обраної сукупності критеріїв і, власне, оцінці ефективності міграції. Оцінка ефективності проводиться із застосуванням методу аналізу ієрархій. Застосування методики дозволяє формалізувати і спростити процес прийняття рішення про доцільність та ефективність побудови гібридної хмарної інфраструктури додатків.

Ключові слова: гібридні хмарні платформи, міграція додатка в хмару, оцінка ефективності міграції в хмару

SUPPORT FOR THE DECISION MAKING ON IMPLEMENTATION OF APPLICATIONS IN THE HYBRID CLOUD INFRASTRUCTURE

L.A. Voloshchuk, O.I. Roznovets, D.D. Voloshchuk

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

Cloud technologies and platforms are actively developing and are becoming more and more in demand. The most popular recently acquired hybrid clouds and multi-cloud services, in which the distributed deployment of the company's IT-infrastructure is implemented partly on cloud platforms, partly on the customer's premises. To decide on the possibility of a partial migration of IT-infrastructure to the cloud, the challenge arises of choosing the right combination of private and cloud solutions in a single application architecture and the IT-environment of the enterprise as a whole. A modern approach to the design of IT-applications and complexes involves the implementation of a modular, multi-tiered architecture in which each module of the system has a certain functionality, a set of its own methods and properties, and involves meeting certain technical requirements for its implementation and links to other components of the architecture. The technical requirements can be determined by the relevant criteria and their significance in different ways and platforms for allocating subsystems. Getting an integrated assessment of the technical capability of working in a hybrid cloud of subsystems of an enterprise IT-environment application can be obtained by conducting multi-criteria analysis and choosing the best solution. The article discusses the construction of a hybrid cloud infrastructure of the enterprise IT-environment, assesses the technical feasibility and efficiency of conducting partial migration to the public cloud of applications and their subsystems. A methodology for estimating the efficiency of migration based on the structural and functional decomposition of the application architecture, analysis of the technical feasibility of migration of application subsystems is proposed in accordance with the selected set of criteria and the actual estimation of migration efficiency. Efficiency evaluation is carried out using the hierarchy analysis method. The application of the methodology allows to formalize and simplify the process of making a decision about the appropriateness and efficiency of building a hybrid cloud application infrastructure.

Keywords: hybrid cloud platforms, application migration to the cloud, evaluation of the efficiency of migration to the cloud

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

Том 8, номер 1, 2018. Одеса – 98 с., іл.

ИНФОРМАТИКА И МАТЕМАТИЧЕСКИЕ МЕТОДЫ В МОДЕЛИРОВАНИИ

Том 8, номер 1, 2018. Одесса – 98 с., ил.

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Volume 8, No. 1, 2018. Odesa – 98 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 №6 від 27.02.2018)

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, 2018