МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеський національний політехнічний університет

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Том 10, № 3-4

Volume 10, No. 3-4

Одеса – 2020
Odesa – 2020

Журнал внесений до переліку наукових фахових видань України (технічні науки) згідно наказу Міністерства освіти і науки України № 463 від 25.04.2013 р. Перереєстровано на категорію «Б» за фахами 121, 122, 125, 151 згідно наказу МОН України № 1473 від 26.11.2020 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: *А.А. Кобозєва*

Заступник головного редактора:
С.А. Положаєнко

Відповідальний редактор:
О.А. Стопакевич

Редакційна колегія:
І.І. Бобок, Д. Джухар, А.А. Кобозєва, В.Ф. Ложечніков, В.В. Любченко, В.Д. Павленко, В.В. Палагін, С.А. Положаєнко, О.В. Рибальський, А.В. Соколов, В.О. Сперанський, О.А. Стопакевич, О.О. Фомін

Published 4 times a year

Founded by Odessa National Polytechnic University in 2011

Certificate of State Registration KB № 17610 - 6460P of 04.04.2011

Editor-in-chief: *A. Kobozeva*

Associate editor:
S. Polozhaenko

Executive editor:
O. Stopakevych

Editorial Board:
I. Bobok, J. Juhar, A. Kobozeva, V. Lozhechnikov, V. Liubchenko, V. Pavlenko, V. Palahin, S. Polozhaenko, O. Rybalsky, A. Sokolov, B. Speransky, O. Stopakevych, O. Fomin

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, 2020

ЗМІСТ/CONTENTS

ФОРМУВАННЯ ДІАГНОСТИЧНИХ МОДЕЛЕЙ ОБ'ЄКТІВ З НЕПЕРЕРВНИМИ ХАРАКТЕРИСТИКАМИ НА ОСНОВІ КОРЕЛЯЦІЙНОЇ ФІЛЬТРАЦІЇ В УМОВАХ ДІЇ ЗАВАД О.О. Фомін, О.Д. Рубан	125	FORMATION OF DIAGNOSTIC MODELS OF CONTINUOUS OBJECTS BASED ON CORRELATION FILTRATION UNDER CONDITIONS OF INTERFERENCE Fomin O., Ruban O.
РОЗРОБКА МЕТОДУ ПЕРЕДАЧІ СЕКРЕТНИХ ПОВІДОМЛЕНЬ НА БАЗІ ХЕШУВАННЯ ЦИФРОВИХ АУДІОФАЙЛІВ В.В. Зоріло, О.Ю. Лебедєва, В.В. Конофольський	136	DEVELOPMENT OF A METHOD FOR TRANSMITTING SECRET MESSAGES BASED ON HASHING OF DIGITAL AUDIO FILES Zorilo V., Lebedeva O., Konofolskyi V.
АВТОМАТИЗОВАНА СИСТЕМА УПРАВЛІННЯ ПОТУЖНІСТЮ КОМБІНОВАНОЇ ТЕПЛОФІКАЦІЙНОЇ УСТАНОВКИ КОТЕДЖНОГО БУДИНКУ Т.М. Клябіна, К.В. Беглов	142	CONTROL SYSTEM FOR POWER COMBINED HEATING INSTALLATION OF COTTAGE HOUSE Klyabina T., Beglov K.
МОДЕЛЮВАННЯ ПРОЦЕСУ УТВОРЕННЯ ШКІДЛИВИХ ВИКИДІВ У ВИХІДНИХ ГАЗАХ СУДНОВИХ ПАРОВИХ КОТЛІВ В.С. Михайленко, В.А. Щербінін, В.В. Лещенко, Р.Ю. Харченко, Н.В. Ложечнікова	154	MODELING THE PROCESS OF HAZARDOUS EMISSIONS FORMATION IN THE EXHAUST GASES OF SHIP'S STEAM BOILERS Mikhailenko V., Shcherbinin V., Leshchenko V., Kharchenk R., Lozhechnikova N.
МЕТОДИ ТА ЗАСОБИ ВИЯВЛЕННЯ НЕАКТУАЛЬНОЇ ТА НЕДОСТОВІРНОЇ ІНФОРМАЦІЇ НА WEB-РЕСУРСАХ А.М. Мельник	167	METHODS AND TOOLS OF DETECTING CURRENT AND RELIABLE INFORMATION ON WEB-RESOURCES Melnyk A.
ВИЯВЛЕННЯ КІБЕРАТАК В ІНФОРМАЦІЙНИХ МЕРЕЖАХ І.Р. Опірський, Ю.М. Ткач, В.О. Хорошко	177	CYBER ATTACKS DETECTION IN INFORMATION NETWORKS Opirsky I., Tkach Y., Khoroshko V.

ЗАСТОСУВАННЯ НЕЧІТКОГО РЕГУЛЯТОРА ДЛЯ РЕГУЛЮВАННЯ РІВНЯ ВОДИ В БАРАБАНІ ПАРОВОГО КОТЛА Е-50
А.С. Рура, О.С. Тарахтій
190
DEVELOPMENT OF A FUZZY CONTROLLER OF THE WATER LEVEL IN THE DRUM STEAM BOILER E-50
Rura A., Tarakhtiy O.

РОЗРОБКА СИСТЕМИ БЕЗПЕКИ КЛІЄНТ-СЕРВЕРНОГО ЗАСТОСУНКУ НА БАЗІ ОПЕРАЦІЙНОЇ СИСТЕМИ ANDROID
А.Ю. Судаков, А.В. Соколов
197
DEVELOPMENT OF CLIENT-SERVER APPLICATION SECURITY SYSTEM BASED ON ANDROID OPERATING SYSTEM
Sudakov A., Sokolov A.

СИНТЕЗ РЕГУЛЯТОРА В ДИСКРЕТНОМУ ЧАСІ З ЗАДАНИМ ЧАСОМ ВСТАНОВЛЕННЯ ПЕРЕХІДНОГО ПРОЦЕСУ
А.О. Стопакевич, О.А. Стопакевич
208
DISCRETE TIME CONTROLLER SYNTHESIS WITH THE DESIRED SYSTEM TRANSIENT TIME
Stopakevych A., Stopakevych O.

ВИКОРИСТАННЯ ТЕОРІЇ ІГОР ПРИ АНАЛІЗІ ГІБРІДНИХ ВІЙН
В.О. Хорошко, М.М. Браіловський
222
THE USE OF GAME THEORY FOR THE ANALYSIS OF HYBRID WAR
Horoshko V., Brailovskyi M.

КОНЦЕПЦІЯ КІБЕРБЕЗПЕКИ ТА МОДЕЛЮВАННЯ ПРОЦЕСІВ ОПТИМАЛЬНОГО УПРАВЛІННЯ СИСТЕМОЮ КІБЕРЗАХИСТУ ДЕРЖАВИ
В.О. Хорошко, Ю.Є. Хохлачова, І.В. Кібальчич
230
THE CONCEPT OF CYBER SECURITY AND SIMULATION OF PROCESSES OF OPTIMAL CONTROL OF THE STATE CYBER PROTECTION SYSTEM
Khoroshko V., Khokhlachova Y., Kibalchich I.

DOI 10.15276/imms.v10.no 3-4.125
UDC 004.942

Informatics and Mathematical Methods in Simulation
Vol. 10 (2020), No. 3-4, pp. 125-135

FORMATION OF DIAGNOSTIC MODELS OF CONTINUOUS OBJECTS BASED ON CORRELATION FILTRATION UNDER CONDITIONS OF INTERFERENCE

O.O. Fomin, O.D. Ruban

Odessa National Polytechnic University,
Shevchenko Ave. 1, Odessa, 65044; Ukraine; fomin@opu.ua

The paper solves the problem of constructing diagnostic models for nonlinear dynamics objects with continuous characteristics. The problems of using existing methods of diagnostics of the mentioned objects, including those under conditions of a priori uncertainty, are considered. Interference is caused by the operation of the object in a wide range of external conditions and the presence of a large number of disturbing influences and interferences of the environment. The aim is to improve the reliability and speed of diagnosis of continuous objects under the influence of interference. The aim is achieved by developing a method of model diagnosis based on correlation methods of filtering features. The most significant results: A hybrid method of forming diagnostic models of continuous objects by sequential application of attribute filtering using correlation methods for constructing a diagnostic space and constructing a diagnostic model by rotating method using a total enumeration of diagnostic attributes and method of maximum likelihood is proposed. The step-by-step algorithm of formation of diagnostic models using the proposed method is given. The significance of the results: the application of the proposed method can simultaneously provide high reliability of diagnosis of objects under the influence of noise through the use of continuous information models and to ensure efficiency of the diagnostic procedure due to correlation filtering of attributes. The proposed method is tested on the example of diagnostics of a nonlinear dynamic object with continuous characteristics - a valve-jet engine. Diagnostic models based on the combination of correlation characteristics are constructed. A family of diagnostic models of a valve-jet motor under conditions of disturbing influences and ambient noise is proposed.

Keywords: continuous objects, diagnostic models, model reduction, correlation filtration.

Introduction

With the increasing complexity of modern control objects and their operating conditions in various branches of industry, medicine, economy, the role of automated technical diagnostics systems (ATDS) in tasks of timely and reliable determination of the technical condition of diagnostic objects (DO) on assessment of product quality, minimization of costs during maintenance, etc., is increasing.

These processes lead to the active development of technical diagnostics (TD) tools and methods. In this case, of great interest are the tasks of indirect control and diagnostics of complex objects of the surrounding world with continuous characteristics and unknown structure, which can be considered as a "black box".

Such objects are often accompanied by a priori uncertainty, among the causes of which are considered operation in a wide range of external conditions, presence of a large number of disturbing influences and environmental interferences.

The use of existing ATDS is limited by the action of contradiction between the reliability of diagnostics and the efficiency of ATDS tuning when using diagnostic models of large dimensions. Due to large dimensionality and volumes of accumulated primary diagnostic information high reliability of diagnostics is provided, but it leads to increase of computational complexity and decrease of ATDS tuning efficiency. A decrease in the dimensionality and volume of primary identification information allows increasing the speed

of ATDS tuning, but leads to a decrease in the reliability of diagnosis.

Resolution of this contradiction is a promising and urgent scientific and technical task, which can be solved by building diagnostic models with significantly smaller size of diagnostic information (reduction of information models) and ensuring high reliability of diagnosis.

The purpose of the work is to increase reliability and speed of diagnostics of continuous objects under conditions of a priori uncertainty through the development of model diagnostic method based on correlation filtering methods of informative attributes.

Literature review

By 2010, typical practical diagnostic space selection tasks were limited to dimensions of a few dozen attributes, typically no more than 40 [1]. The situation has changed considerably over the past decade. The global volume of data has more than doubled every two years [2]. At the same time, large amounts of data are opening up new opportunities.

The main reasons for this growth are advances in technology and significant advances in Data Science and Big Data [3–5]. New technologies have reduced the cost of creating, collecting, classifying and managing information in dozens of times.

The concepts of the Digital Universe and big data have become one of the driving forces for fundamental changes in social life, technology, science and economics. Such advances stimulate the development of applications with the DO feature vector dimensionality of hundreds or even thousands of units.

An example of a new challenge in the field of modern industrial technology at Industry-4 level is improving the process of the technological process components diagnosis, in particular the electric motors [3, 6] that drive the actuators.

The dimensionality of such task increases, if we take into account that during the years of work the monitoring and control systems the considerable volumes of technical information are accumulated.

With a sharp increase in the dimensionality of tasks, often data accompanied by many redundant variables and a small number of training examples, there is a need to reconsider the effectiveness of traditional methods of forming diagnostic models of DO.

An effective way to solve such problems is the reduction of the primary feature space, a widely used data preprocessing technique in data mining [1, 7, 8].

There are many potential benefits of this approach: easier data visualization and understanding, reduced measurement and storage requirements, shorter training times for the diagnostic system and the diagnostic process, and improved overall performance of the machine learning algorithm.

Main part

The construction of a continuous DO model consists in selecting the type of test influences $x(t)$, measuring the response $y(t)$ and determining the models $w(t_1, t_2, \ldots, t_n)$ on their basis.

The disadvantage of such a model is considered to be the large volume of primary identification information, which leads to a decrease in ATDS tuning speed.

Reducing the amount of primary identification information by using more compact models allows increasing ATDS tuning speed, but leads to a decrease in the reliability of diagnostics.

Thus, there is a contradiction between the reliability of TD and the tuning speed of ATDS when using continuous DO model.

This contradiction can be resolved by developing a new method of secondary identification – construction of diagnostic feature space x with significantly smaller diagnostic information size.

Traditional approaches of feature selection for machine learning can be divided into three categories [1, 7, 9]: feature filtering [1, 7, 10] wrapper methods [1, 9, 11, 12] and feature embedding [1, 7].

When solving practical problems, the application of any method often leads to the desired results. This is primarily due to the a priori ambiguity of the DO. The reasons for priori ambiguity are the complexity of the object (continuous dynamic objects of various physical natures, including those with unambiguous continuous nonlinear characteristics) and insufficient study of the processes occurring in it, as well as the presence of a large number of disturbing influences and environmental interferences are considered.

Currently, many authors are also using hybrid methods consisting of a combination of these approaches, the results of which are also promising. Recently, this is one of the widely used approaches used to form diagnostic models. A hybrid approach combines several methods to take advantage of each to produce satisfactory results. This approach usually provides high diagnostic reliability with low computational complexity.

A hybrid approach to feature selection based on the sequential application of filtering and wrapping methods is a good practice. The first stage involves selecting the most valuable subset of features by filtering – a global feature search. At this stage, the number of considered features is up to several dozen. At the second stage, the optimum (in terms of reliability of diagnosis) subset of features is selected by the wrapping method – local search for the features. The proposed hybrid approach is very scalable for datasets consisting of a large number of features.

Creating a diagnostic feature space based on filtering methods. This paper proposes a hybrid method for constructing diagnostic models based on correlation filtering of features.

A simple method of describing the continuous properties of a DO in the form of a vector of features x is the parameterisation of continuous models of the DO $f(t)$. In this case, the function $f(t)$ is represented by vector $x= (x_1,\ldots, x_n)$. The diagnostic features can be obtained by a prior transformation T_j: $C[a, b] \rightarrow R^n$, $(j = 1,\ldots, n)$: $x_j= T_j(f(\tau_1,\ldots, \tau_k))$; where $C[a, b]$ is the space of real continuous functions $f(t)$ given on the interval $[a, b]$; a, b– are some real numbers. Orthogonal decompositions and integral transformations of continuous models into vectors of coefficients of basis functions can be used as operator T_j.

In practice it is accepted to use the discretisation operator as T_j:

$$x_j = f(t_j), \tag{1}$$

$t_j = j\Delta t$, where Δt – is a sampling step.

Modern data logging subsystems within ATDS are capable of taking thousands of measurements per second. This ensures completeness of the primary diagnostic data. At the same time, the measurement results are accompanied by a lot of redundant data. Moreover, it is evident that the value of different sections of measured DO output for the diagnostic procedure is different.

It has been shown in [10, 13, 14] that the most valuable parts of the DO responses are usually the parts that carry the highest signal energy. Given the above, the use of signal sampling to form the diagnostic feature space is a poorly effective technique.

When dealing with continuous characteristics of the DO to form the space of diagnostic features, correlation methods of filtering the models samples can be particularly effective [14, 15].The formation of diagnostic models based on feature filtering consists in ranking these features using statistical methods to evaluate the relationship between each

input variable and the target variable [10, 14, 16]. These methods provide fast and efficient results especially when processing large amounts of data.

The type of response variable usually indicates the type of modeling task. For example, a numerical output variable indicates a predictive modeling problem with regression and a categorical output variable indicates a predictive modeling problem with classification.

There are several types of correlation methods for estimating the diagnostic value of features, depending on the type of data for both input and output variables: numeric or categorical data.

When dealing with continuous characteristics of the DO to form the space of diagnostic features, correlation methods of filtering the samples of information models can be particularly effective [14, 15, 17].

The case of numerical input and categorical output is considered in the task of diagnosing continuous DO. In this case, Fisher's F-criterion is used to estimate the relationship between inter- and intra-group variability:

$$I = \frac{\sum_{i=1}^{n_j}\left(x_{i,j} - M^2\right)/P - 1}{\sum_{i=1}^{n_j}\left(x_{i,j} - M_j^{\,2}\right)/L - J}, \quad (2)$$

where M is the mathematical expectation of the signs, L is the full sample size, P is the number of classes.

For comparison, the results of this method are compared with the results of the method for calculating the diagnostic value I of the primary signs of OD, determined by the information method [10] according to the expression:

$$H(x) = -\sum_{i=1}^{n} p_i \log_2 p_i, \quad (3)$$

The evaluation of the reliability of diagnosis in the work is based on solving the problem of classification of examination sample by the method of maximum likelihood. The reliability of various combinations of features is indicated by the probability of correct recognition P [17]:

$$P = \sum_{i=1}^{m} L_i \left(\sum_{i=1}^{m} N_i\right)^{-1}, \quad (4)$$

where L_i– the number of objects of the i-th class, mistakenly assigned to another class k (k_i) N_i– the number of objects of the i-th class in the examination sample; i = 1, 2, ..., m; m– the number of classes of DO state.

The maximum likelihood method allows constructing the best solution when the distribution of features in the training sample is normal. To improve the quality of classification in the case of non-normal distribution of a random variable, it is proposed to perform transformations aimed at removing the relationship between the variance and the mathematical expectation. Thus, the variance becomes constant with respect to the mean. Such stabilization is proposed to be carried out by applying power transformations, in particular by logarithm the values of a random variable:

$$x_j^0 = \log_a(x_j + b), \quad (5)$$

where a–base of the logarithm's –stabilizing coefficient.

This paper proposes a method for constructing a diagnostic features space based on continuous information models, followed by their discretisation and filtering of features using an assessment of their correlation.

Hybrid method for constructing the diagnostic feature space of continuous objects. The proposed method of constructing the diagnostic feature space based on continuous models of nonlinear dynamic DO is reduced to the identification of the information model of the object in the form of multidimensional weight functions (MWF) by the "input-output" experimental data [18, 19]. The space of attributes is built on the basis of discrete samples of the obtained continuous models. Diagnostic models are built in the obtained space by filtering of attributes based on assessment of their correlation.

The stages of the method of the diagnostic features space constructing based on integral dynamic models are shown in Table 1. The development of this method consists in adding step 3 (power transformations of training sample data for distribution of features in classes different from normal for stabilization of variance of random variables) and steps 4 and 5 to the well-known procedure of model-based diagnostics for preliminary features evaluation.

Creating a diagnostic model of a valve-jet engine

Table 1.

Stages of the method of the diagnostic feature space constructing based on integral dynamic models

Stage		Description
No	**Title**	
1.	DO identification	*Purpose*: DO model generation. *Input*: test input signal $x(t)$ *Model*: continuous function (functional series) *Output*: DO continuous model
2.	Continuous model sampling	*Purpose*: discrete DO model generation *Input*: DO continuous model $w(t_1, t_2, \ldots, t_n)$ *Model*: sampling operator (1) *Output*: features vector $\mathbf{x}$
3.	Stabilization of model sampling variance	*Purpose*: stabilization of variance of vector $\mathbf{x}$ *Input*: features vector $\mathbf{x}$ *Model*: power transformations, logarithmic transformations *Output*: features vector $\mathbf{x}^0$
4.	Features evaluation	*Purpose*: get the value of each feature in vector $\mathbf{x}^0$ *Input*: features vector$\mathbf{x}^0$ *Model*: Fisher's F-criterion (2) *Output*: features vector$\mathbf{x}^1$, ranked by value I
5.	Features filtering	*Purpose*: get a space of diagnostic features *Input*: vector of ranked features $\mathbf{x}^1$ *Model*: $\mathbf{x}^2 = (x_1, \ldots, x_p)' \in \mathbf{x}$, $p<n$ *Output*: diagnostic features vector $\mathbf{x}^2 = (x_1, \ldots, x_p)'$ with maximum values I
6.	Evaluation of the noise immunity of the diagnostic model	*Purpose*: get an interference-free diagnostic feature space *Input*: diagnostic features vector $\mathbf{x}^2 = (x_1, \ldots, x_p)'$ with maximum values I *Model*: probability of correct recognition P(4) *Output*: value of probability of correctly recognizing P

Approbation of diagnostic futures space building method of continuous models is made on an example of valve-jet engine – object with non-linear dynamic characteristics.

In the process of long-term operation the rotor of valve-jet engine has friction in the air and with the time the air gap δbetween rotor and stator in engine increases (fig.1), and consequently, its power performances decrease. Therefore, it is necessary to periodically monitor the value δ [20] during the operation of the engine. Direct measurements are unacceptable, as they are lab our-intensive and require the removal of the engine from operation to be monitored.

The task of valve-jet engine diagnosis is to build a diagnostic model of the drive using indirect measurements of the air gap between the rotor and stator of the engine.

The task of valve-jet engine diagnosis is complicated by the following significant factors:

– the motor is a dynamic object with non-linear characteristics;

– the motor works under conditions of a priori uncertainty: in a wide range of external conditions, in the presence of a large number of disturbing influences and environmental noise;

– under operating conditions it is necessary to provide reliable and efficient diagnostics of the motor condition.

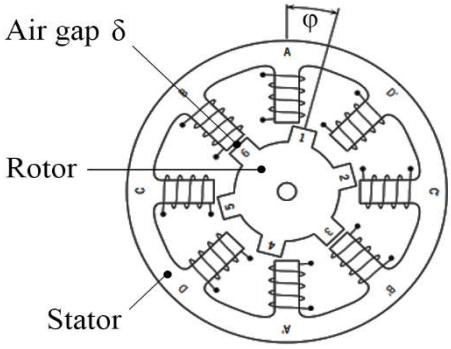

Fig.1. Air gap δ between the rotor and stator of the valve-jet engine.

For evaluation of air gap between rotor and stator of valve-jet engine in [20] it is suggested to use data of side measurements "input-output" on the basis of which the model in the form of multidimensional weight functions $w_k(\tau_1,\ldots, \tau_k)$ is constructed. The structural scheme of the input-output experiment organization in the valve-jet engine diagnostics task is shown in Fig. 2. The input signal $x(t)$ (input voltage U_φ) is set by the diagnostic signal generator DSG, the output signal $y(t)$ (phase current I_φ, by which the air gap δbetween the rotor and the stator is estimated) is measured by the recording device RD.

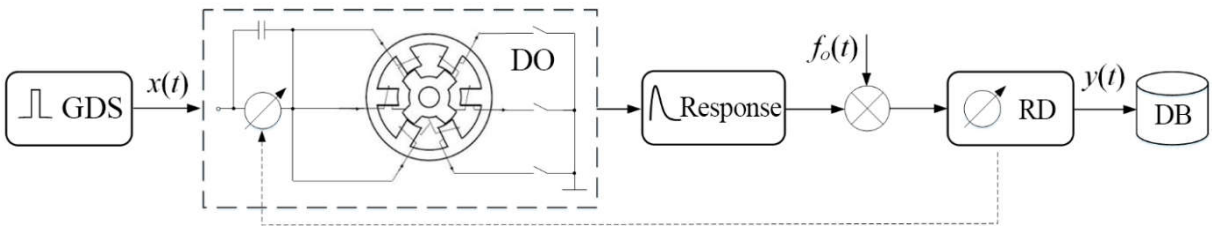

Fig. 2. Flowchart of side-measurement organisation in the valve-jet engine diagnostic task.

The valve-jet engine identification in the form of MWF is carried out using the simulation model of the VREP-57-005 engine (nominal torque – 0.04 Nm, nominal voltage – 24 V, maximum speed – 4000 rpm).

Analytical expressions for MWF of the first $w_1(t)$ order and diagonal relations of MWF of the second order $w_2(t,t)$:

$$w_1(t) = e^{-\alpha t}, w_2(t,t) = \frac{\beta}{\alpha}\left(e^{-2\alpha t} - e^{-2\alpha t}\right) \tag{6}$$

The training sample in the form of first-order MWF $w_1(t)$ (Fig. 3, a) and diagonal sections of second-order MWF$w_2(t,t)$ (Fig. 3, b) at various values of air gap δ are obtained for various states of valve-jet engine and divided into 3 classes on 100 elements in each class: for

δ_ε [δ_n, 1.3δ_n] (normal mode – class *A*), δ_ε (1.3δ_n, 1.6δ_n) (failure mode – class *B*), $\delta>\delta_n$ (emergency mode – class *C*), δ_n–nominal value of air gap δ.

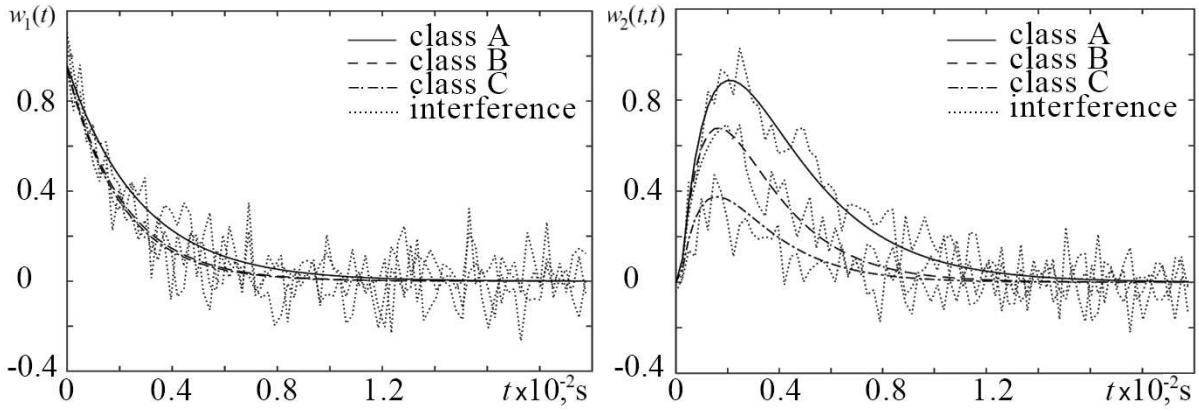

Fig. 3. On the left are first-order MWF $w_1(t)$; on the right are diagonal sections of second-order MWF $w_2(t,t)$ at different values of the air gap δ (classes *A*, *B*, *C*).

Information model sampling.

The MWF samples and their sections obtained with step Δt= 2.5 ms were used for experimental investigations.

The space of diagnostic features $\mathbf{x} = (x_1, \ldots, x_l)'$ in the form of samples of MWF diagonal sections $w_k(t-\tau_1, \ldots, t-\tau_k)$ of order k = 1, 2 with dimension l = 81 samples was formed.

Evaluation of the features.

Calculation of the primary DO model diagnostic value *I*: WMF samples $w_1(t)$ (Fig. 4, a) and WMF diagonal sections of the second order $w_2(t,t)$ (Fig. 4, b) is carried out using criterion (2).

As a result, the resulting vectors of features $\mathbf{x}^1 = (x_1, \ldots, x_1)'$, ranked by value *I*.

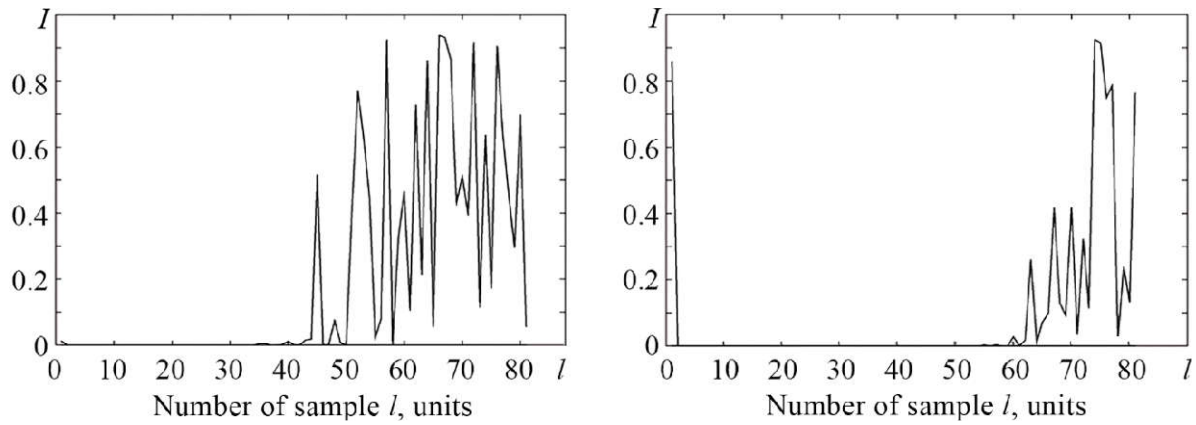

Fig. 4. Diagnostic value *I* of samples according to criterion (3): on the left –the first-order MWF $w_1(t)$; on the right– the second-order WMF diagonal section $w_2(t,t)$.

Feature filtering.

From the elements of the diagnostic features vector $\mathbf{x}^1$ a subspace $\mathbf{x}^2 = (x_1, \ldots, x_p)'$ is formed by filtering the features with the maximum value index *I*. The dimension *p* of the space $\mathbf{x}^2$ is chosen so as to ensure a given reliability of diagnosis. In this paper, the reliability

is estimated by solving the problem of classifying the objects of the examination sample by the maximum likelihood method [10].

To form a reduced space of diagnostic features, 2 methods are compared: by means of model samples according to expression (1) and by means of correlation coefficients.

The calculation of diagnostic value I of DO features –*s*amples of MWF of the first order $w_1(t)$ (Fig. 5, a) and diagonal samples of MWF of the second order $w_2(t,t)$ (Fig. 5, b) are presented in Fig. 5.

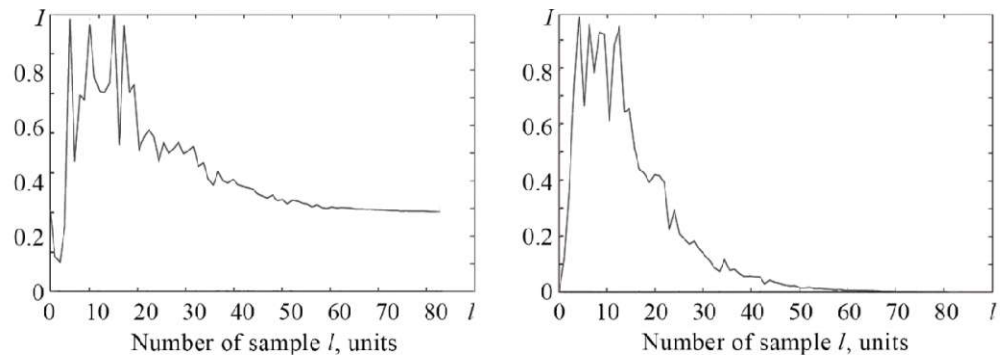

Fig. 5. Correlation coefficient of samples (ANOVA method): on the left –MWF of the first order $w_1(t)$; on the right – diagonal sections of MWF of the second order $w_2(t,t)$

In this task, at p = 5, the diagnostic model of valve-jet engine, constructed using the correlation filtering of features $\mathbf{x}^1$, provides a given level of diagnostic reliability P = 0.99.

For comparison, the value of each feature I of space $\mathbf{x}$ was determined by estimating the diagnostic reliability P for each count of the first-order MWF (Fig. 5, a) and the diagonal links of the second-order MWF (Fig. 5, b).

The comparison of the values of the corresponding MWF models samples (Fig. 4-5) shows that the diagnostic attributes obtained by filtering based on correlation significantly coincide with the attributes selected by the classification of the examination sample objects using the maximum likelihood decisive rule. The computational complexity of obtaining the result by filtering based on correlation is 6-8 times less than that based on classification results.

Research of the valve-jet engine diagnostic model under conditions of interference.

The reliability index P (probability of correct recognition) of forming diagnostic features spaces is studied: samples $x_k=f(t_k)$, $t_k=k\Delta t$, k=1, 10of the first order MWF $w_1(t)$ (diagnostic space $\mathbf{Y}_1$) and diagonal sections of the second order MWF $w_2(t,t)$ (diagnostic space $\mathbf{Y}_2$). The results of research of diagnostic models reliability P depending on different measurement errors and interferences of the system response: 0, 3, 5 and 10% are presented in Fig. 6.

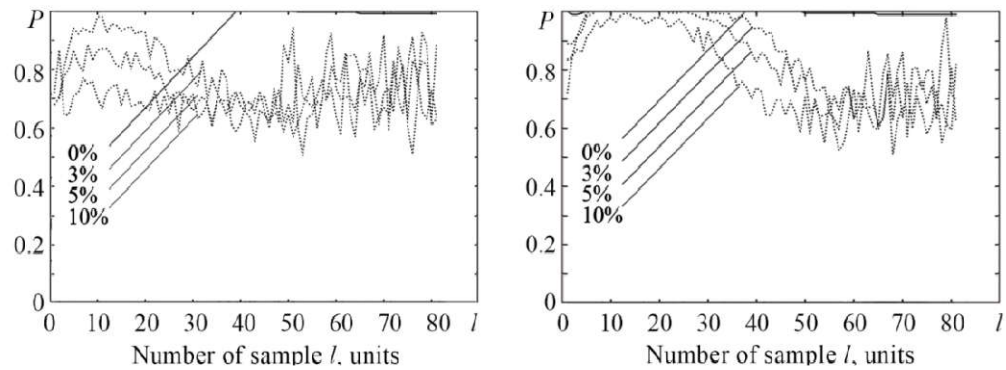

Fig. 6. Reliability P of samples: on the left– first-order MWF $w_1(t)$; on the right– diagonally sections of second-order MWF $w_2(t,t)$.

Conclusions

The paper successfully solved the problem of increasing the reliability and speed of diagnosis of nonlinear dynamic objects by forming diagnostic models while increasing the dimensionality of describing objects of diagnosis and under conditions of interference.

To achieve the goal a review of diagnostic models building methods. It was found that filtering methods are computationally more effective.

Analysis of existing methods and recent trends in building diagnostic models allowed solving the problem of improving the reliability and speed of diagnosis of nonlinear dynamic objects in the primary space features of large dimensionality from a pragmatic point of view – to develop a hybrid method of building of diagnostic models. Under such conditions, application of filtering methods does not provide a given reliability of diagnosis, and it is difficult to apply wrapping methods because of significant growth of computational complexity of the problem (the curse of dimensionality).

The method of building a diagnostic features space of nonlinear dynamic objects based on information models in the form of MWF by applying single-factor and multifactor correlation analysis as a stage of filtering of features with subsequent enumeration of combinations of features provides maximum reliability of diagnosis. The use of this approach can simultaneously provide high reliability of diagnosing objects under a priori uncertainty through the use of primary information models based on MWF and rapid diagnostic procedure due to filtering based on a correlation analysis of the diagnostic space. A stepwise algorithm of the method with the representation of the incoming, outgoing information and the data model used at each step is given.

The proposed method is tested on the real data of the task of diagnosing a nonlinear dynamic object – a valve-jet engine. The method demonstrates greater noise immunity of reliability value than existing methods of constructing diagnostic feature spaces based on the primary diagnostic model.

References

1. Guyon I., Elisseeff A. An introduction to variable and feature selection. *Journal of Machine Learning Research*. 2003. No 3. P. 1157–1182.
2. Gantz J., E. Reinsel. Extracting Value from Chaos. IDC's Digital Universe Study, 2011. 12 p.
3. Yan H., Wan J., Zhang C., Tang S., Hua Q., Wang Z. Industrial big data analytics for prediction of remaining useful life based on deep learning. *IEEE Access*. 2018. Vol. 6. P. 17190–17197.
4. Zhao R., Yan R., Chen Z., Mao K., Wang P., Gao R.X. Deep learning and its applications to machine health monitoring. *Mechanical Systems and Signal Processing*. 2019. Vol. 115. P. 213–237.
5. Fomin O., Derevianchenko O. Improvement of the Quality of Cutting Tools States Recognition Using Cloud Technologies. *Advances in Design, Simulation and Manufacturing III. Proceedings of the 3rd International Conference on Design, Simulation, Manufacturing: The Innovation Exchange, DSMIE*, Kharkiv, Ukraine, 2020. Vol. 1. P. 243-252.
6. Henao H., Capolino G-A, Fernandez-Cabanas M., Filippetti F., Bruzzese C., Strangas E., Pusca R., Estima J., Riera-Guasp M., Hedayati-Kia S. Trends in fault diagnosis for electrical machines: a review of diagnostic techniques. *IEEE Industrial Electronics Magazine*. 2014. Vol. 2, No. 8. P. 31–42.
7. Tang J., Alelyani S., Liu H. Feature selection for classification: A review. *Data Classification: Algorithms and Applications.* CRC Press, 2014. P. 37–64.

8. Shahana A.H., Preeja V. Survey on feature subset selection for high dimensional data. *2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT)*, Nagercoil, India, 2016. P. 1–4.
9. Jain D., Singh V. Feature selection and classification systems for chronic disease prediction: A review. *Egyptian Informatics Journal*. 2018. Vol. 19, Issue 3. P. 179–189.
10. Fainzilberg L.S. Mathematical methods for evaluating the usefulness of diagnostic features. Kiev: Osvita Ukrainy, 2010.152 p. [in Russian].
11. Liu H., Hiroshi M. Feature Selection for Knowledge Discovery and Data Mining. *The Springer International Series in Engineering and Computer Science*, 1998. 214 p.
12. Kohavi R., John G. Wrappers for feature selection. *Artificial Intelligence.* 1997. Vol. 97, Issues 1–2. P. 273–324.
13. Medvedew A., Fomin O., Pavlenko V., Speranskyy V. Diagnostic features space construction using Volterra kernels wavelet transforms *Proceedings of the 2017 IEEE 9th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, 2017. P. 1077–1081.
14. Qu G., Hariri S., Yousif M. A new dependency and correlation analysis for features. *IEEE Transactions on Knowledge and Data Engineering*. 2005. Vol. 17, No. 9. P. 1199–1207.
15. Gopika N., Meena-Kowshalaya M.E. Correlation Based Feature Selection Algorithm for Machine Learning *Proceedings of the International Conference on Communication and Electronics Systems (ICCES)*, 2018. P. 692–695.
16. Dumas S. Karhunen-Loeve transform and digital signal processing – part 1. SETI League, 2016. 39 p.
17. Fomin O., Ruban O., Fedorova H., Bartalyov P., Katsiuk D. Construction of the nonlinear dynamic objects diagnostic model based on of multiple factors variance analysis *Herald of Advanced Information Technology*. 2020. Vol. 3, No.2. P. 52–60.
18. Fomin O., Masri M., Pavlenko V. Intelligent Technology of Nonlinear Dynamics Diagnostics using Volterra Kernels Moments *International journal of mathematical models and methods in applied sciences*. 2016. Vol. 10. P. 158–165.
19. Mansouri M., Harkat M.-F., Nounou H., Nounou M. Data-driven and model-based methods for fault detection and diagnosis. Elsevier, 2020. 322 p.
20. Grigorenko S.N., Pavlenko S.V., Pavlenko V.D., Fomin A.A., Information technology of diagnostics of electric motor condition using Volterra models. *Eastern-European Journal of Enterprise Technologies*. 2014. Vol. 4, No 11(70). P. 38–43.

ФОРМУВАННЯ ДІАГНОСТИЧНИХ МОДЕЛЕЙ ОБ'ЄКТІВ З НЕПЕРЕРВНИМИ ХАРАКТЕРИСТИКАМИ НА ОСНОВІ КОРЕЛЯЦІЙНОЇ ФІЛЬТРАЦІЇ В УМОВАХ ДІЇ ЗАВАД

О.О. Фомін, О.Д. Рубан

Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044; Україна; fomin@opu.ua

В роботі вирішується задача побудови діагностичних моделей для об'єктів нелінійної динаміки з неперервними характеристиками. Розглянуто проблеми використання існуючих методів діагностики означених об'єктів, в тому числі, в умовах апріорної невизначеності. Завади обумовлені експлуатацією об'єкта в широкому діапазоні зовнішніх умов і наявності великої кількості збурюючих впливів і перешкод навколишнього середовища. Метою роботи є підвищення достовірності і швидкодії діагностування неперервних об'єктів в умовах дії завад. Поставлена мета досягається шляхом розвитку методу модельної діагностики на основі кореляційних методів фільтрації ознак. Найбільш вагомі результати: запропоновано гібридний метод формування діагностичних моделей неперервних об'єктів шляхом послідовного застосування фільтрації ознак за допомогою кореляційних методів для побудови діагностичного простору та побудови діагностичної моделі методом обертання з використанням повного перебору діагностичних ознак та методу найбільшої правдоподібності. Наведено покроковий алгоритм формування діагностичних моделей за допомогою запропонованого методу. Значення отриманих результатів: застосування запропонованого методу дозволяє одночасно забезпечити високу достовірність діагностування об'єктів в умовах дії завад завдяки використанню безперервних інформаційних моделей і забезпечити оперативність діагностичної процедури завдяки кореляційній фільтрації ознак. Запропонований метод апробовано на прикладі діагностування нелінійного динамічного об'єкту з неперервними характеристиками – вентильно-реактивного двигуна. Побудовано діагностичні моделі на основі комбінування кореляційних характеристик. Запропоновано сімейство діагностичних моделей вентильно-реактивного двигуна в умовах збурюючих впливів і перешкод навколишнього середовища.

Ключові слова: неперервні об'єкти, діагностичні моделі, редукція моделей, кореляційна фільтрація.

DOI 10.15276/imms.v10.no 3-4.136
УДК 004.056.53

Informatics and Mathematical Methods in Simulation
Vol. 10 (2020), No. 3-4, pp. 136-141

РОЗРОБКА МЕТОДУ ПЕРЕДАЧІ СЕКРЕТНИХ ПОВІДОМЛЕНЬ НА БАЗІ ХЕШУВАННЯ ЦИФРОВИХ АУДІОФАЙЛІВ

В.В. Зоріло, О.Ю. Лебедєва, В.В. Конофольський

Одеський національний політехнічний університет,
пр. Шевченка, 1, Одеса, 65044, whiteswanhelena@gmail.com

Стеганографія та криптографія перебувають на піку розвитку в наші дні. Один з видів стеганографії – хеш-стеганографія. Це принципово новий напрямок в галузі передачі секретної інформації. Методи хеш-стеганографії засновані на тому, що замість вбудовування секретної інформації в контейнер, ми передаємо визначену послідовність цифрових сигналів та за їх хеш-кодами відновлюємо повідомлення. Для роботи за даними принципами зазвичай використовують цифрові зображення. Проте цифрові аудіо-файли завдяки різноманітним сервісам та месенджерам стають все популярнішим методом передачі інформації. Тому актуальною є розробка методів хеш-стеганографії, заснованих на використанні аудіо-сигналів. Метою даної роботи є підвищення ефективності передачі секретного повідомлення шляхом модифікації метода хеш-стеганографії. Даний метод не використовує вбудовування додаткової інформації в аудіофайл як контейнер. В даному методі запропоновано використовувати хеш-код (далі хеш), отриманий з аудіофайлів для побудови стеганоповідомлення. Але при передачі та конвертації аудіофайлів можливе порушення цілісності їх хеш-коду через можливі втрати якості і шуми. Це може стати перешкодою при встановленні відповідності отриманих файлів та їх хеш-кодів та при відновленні секретного повідомлення. Один з популярних сервісів ідентифікації аудіо-файлів – програмний додаток Shazam. Додаток Shazam дозволяє вірно ідентифікувати аудіо-треки навіть за наявності шумів, сторонніх звуків тощо. Розглянемо основні кроки даного алгоритму для використання їх при отриманні стійких до атак хеш-кодів аудіо-сигналів. Даний алгоритм дає змогу представити аудіо у вигляді набору особових точок, які далі методом MD5 перетворюються на хеш-коди. З даних хеш-кодів відновлюються секретні повідомлення після отримання визначеної послідовності аудіо-сигналів. Розроблений алгоритм не має аналогів для порівняння, проте є стійким до атак.

Ключові слова: хеш-стеганографія, аудіо-файл, хеш-код.

Вступ

Інформаційна безпека в наш час – особливо гостра та актуальна проблема. Інформатизація суспільства сягає таких масштабів, що важко знайти галузь людської діяльності, де б не використовували в тому чи іншому обсязі електронну інформацію. Разом з цим методи несанкціонованого доступу до цієї інформації, методи модифікації та знищення її також розвиваються дуже швидко. На заміну портативним комп’ютерам швидко ідуть сучасні смартфони, які часто є більш потужними за технічними параметрами, ніж деякі комп’ютери. Це дозволяє в будь-який момент мати доступ до певної інформації, або мати змогу «зламати» захист інформаційної системи та порушити інформаційну безпеку. Наслідки цих дій можуть бути як незначними, так і катастрофічними. Ситуація загострюється ще й через можливість працювати з великими масивами інформації та передавати цю інформацію в мережах. У сучасному світі передача великого обсягу інформації є нормою завдяки великій пропускній спроможності каналів зв'язку. Окрім цього, в певних галузях виникає необхідність передавати секретну або конфіденційну інформацію. Таку інформацію як правило не передають відкрито, для передачі використовують закриті канали зв’язку, або передають інформацію у зашифрованому вигляді. Для передачі секретних повідомлень

використовують криптографію, стеганографію та комбінацію тих і інших методів. Сучасні криптографічні методи є дуже надійними. Ефективність криптографічних алгоритмів визначається довжиною ключа. Сучасна техніка та інформаційні технології дозволяють зробити ключ настільки довгим, що підібрати ключ займатиме забагато часу. Сам злам втрачає свою актуальність через часові витрати на процес. Проте криптографія має і свої недоліки. При використанні криптографії в чистому вигляді зашифровані повідомлення привертають увагу. І хоч розшифрувати повідомлення, не маючи ключа, вкрай важко, або, навіть, неможливо, але сам канал зв'язку може бути розсекречено.

На зміну криптографічним методам прийшли стеганографічні. Стеганографія також передає зашифроване повідомлення, проте це повідомлення вбудовують у контейнер (цифрове відео, аудіо, цифрове зображення тощо). При передачі стеганоповідомлення самі контейнери не привертають уваги. Але і стеганографія має недоліки. При використанні стеганографічних методів завжди постає питання про пропускну спроможність сигналу-контейнеру та про стійкість метода до атак. Крім того, сьогодні часто використовують гібридні методи – у стеганографічний контейнер вбудовують повідомлення, зашифроване криптографічним алгоритмом. Таким чином значно підвищується ефективність засекречування. Але і недоліки у гібридних методів такі самі, як і в криптографічних та стеганографічних.

Однак сьогодні є альтарнатива, хеш-стеганографія. Хеш-стеганографія – передача повідомлення у вигляді послідовності цифрових файлів, хеш-коди яких в результаті аналізу формують повідомлення. Таким чином, не треба вбудовувати додаткову інформацію в контейнер. Послідовність контейнерів – це і є інформація.

У відкритому друці не знайдено робіт та посилань на використання аудіо-сигналів у хеш-стеганографії. Цифрові зображення – зручний та добре досліджений варіант. Оскільки аудіофайли є одним з основних форматів даних для передачі інформації в останні роки, питання приховування інформації в аудіофайл набуває все більшої актуальності. Існує безліч сервісів, що надають людям можливість прослуховувати і завантажувати аудіофайли різних форматів і якості, а також дедалі популярнішим стає спосіб спілкування голосовими повідомленнями. Усе це робить актуальним дослідження аудіо-файлів для передачі секретних повідомлень.

Мета даної роботи – підвищення ефективності передачі секретного повідомлення шляхом модифікації метода хеш-стеганографії.

Зараз хеш-стеганографія тільки починає свій розвиток. У відкритому друці знайдено роботи про вбудовування додаткової інформації в цифрові зображення: метод молодшого значущого біта, метод фазового кодування, методи розширення спектра [1], проте рідко згадуються методи хеш-стеганографії, засновані на використанні аудіо-сигналів.

Кодування методом молодшого значущого біта (LSB) – найпростіший спосіб вбудувати інформацію в цифровий аудіо-файл [2]. Замінюючи молодший біт кожної точки вибірки двійковим повідомленням кодування LSB дозволяє вбудувати великий обсяг даних. Однак в деяких реалізаціях кодування LSB два молодших біта вибірки замінюються двома бітами повідомлення. Це збільшує обсяг даних, які можуть бути закодовані, але також збільшує кількість результуючого шуму в файл-контейнер. Саме через шум методи LSB є нестійкими до всіх видів атак, а виявлення LSB-кодованого сигналу здійснюється за аномальними характеристикам розподілу значень діапазону молодших бітів [3]. Головною перевагою методу кодування LSB є низька обчислювальна складність алгоритму, в той час як його основним недоліком є те, що разом з тим, як збільшується кількість використовуваних найменших значущих бітів, збільшується й шанс виявлення застосування цього методу.

Фазове кодування вирішує недоліки шумових методів аудіостеганографії. Таке кодування спирається на той факт, що фазові компоненти звуку не так відчутні для

людського вуха, як шум. Замість того, щоб вводити спотворення, цей метод кодує біти повідомлення як фазові зсуви у фазовому спектрі цифрового сигналу, досягаючи нечутного кодування з точки зору відношення сигналу до сприйманого шуму. Цей метод має багато переваг перед LSB-кодуванням, найголовніша із яких є не виявляння для людського вуха. Як і всі методи, описані до цього часу, його слабкість все ще полягає в недостатній стійкості до змін в аудіо-файлах. Будь-яка окрема звукова операція або зміна даних призведе до спотворення інформації та запобігання її отриманню.

В аудіо-стеганографії метод розширеного спектру використовує для передачі секретних відомостей частотний спектр звукового сигналу. Проте, на відміну від методу LSB, метод розширеного спектру поширює секретну інформацію по спектру частот звукового файлу, використовуючи код, котрий не залежить від фактичного сигналу. В результаті кінцевий сигнал має високий рівень стійкості до атак, проте займає смугу пропускання, яка розміром більше, ніж необхідний розмір для передачі.

В роботі [4] описано метод хеш-стеганографії, заснований на використанні цифрових зображень. В основі даного методу лежить використання хеш-кодів зображення для формування послідовності зображень, кожне з яких відповідають певному символу секретного повідомлення (рис.1).

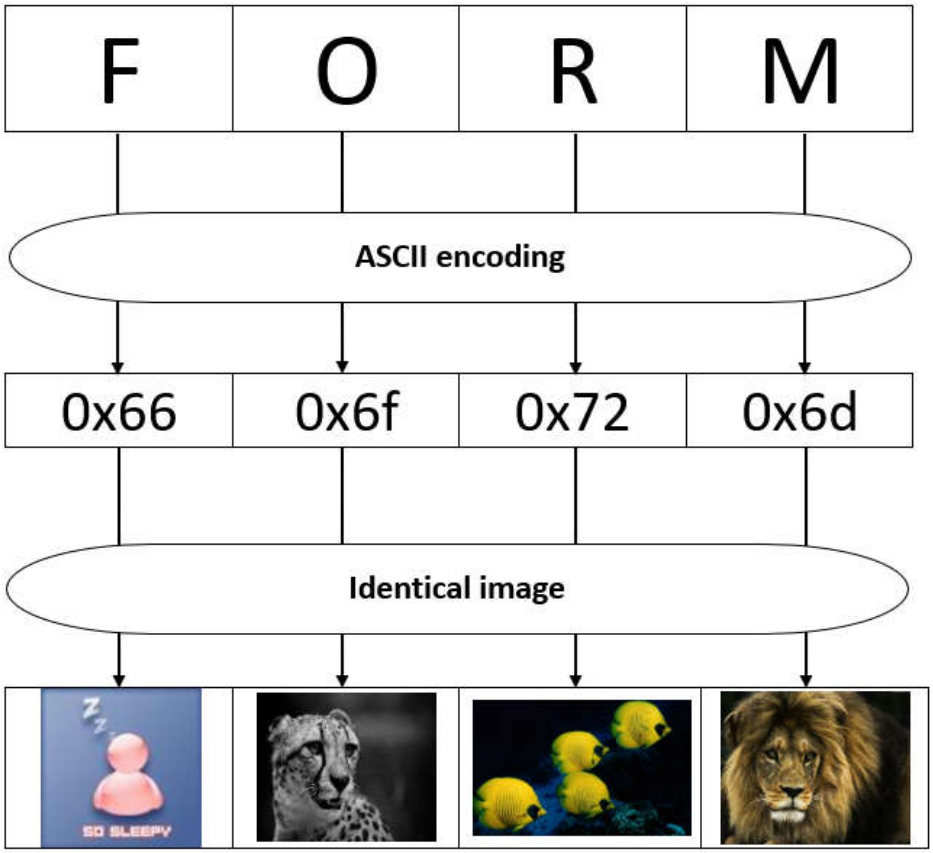

Рис. 1. Кодування повідомлення

Хеш-коди є дуже чутливими до будь-яких змін інформації. Ця їх властивість може стати перешкодою при передачі секретних повідомлень, адже при передачі інформації каналами зв’язку так чи інакше виникають шуми дискретизації тощо. Тому в роботі описано алгоритм модифікації використовуваних файлів перед обчисленням їх хеш-кодів таким чином, щоб вони були стійкими до атак. Описаний метод взято за основу в даній роботі. Його досліджено на цифрових зображеннях, даний метод має високу ефективність відновлення повідомлень навіть після застосування атак до

повідомлення. Проте проведемо дослідження на предмет використання замість цифрових зображень аудіо-файлів.

Основна частина

На відміну від перерахованих вище методів, даний метод не використовує вбудовування додаткової інформації в аудіофайл як контейнер у звичному розумінні. Повідомлення представляє собою послідовність аудіо файлів, хеш-коди яких після певних перетворень утворюють повідомлення, що передається.

В даному методі запропоновано використовувати хеш-код (далі хеш), отриманий з аудіофайлів для побудови стеганоповідомлення. Але при передачі та конвертації аудіофайлів можливе порушення цілісності їх хеш-коду через можливі втрати якості і шуми. Це може стати перешкодою при встановленні відповідності отриманих файлів та їх хеш-кодів та при відновленні секретного повідомлення. Один з популярних сервісів ідентифікації аудіо-файлів – програмний додаток Shazam. Додаток Shazam дозволяє вірно ідентифікувати аудіо-треки навіть за наявності шумів, сторонніх звуків тощо. Розглянемо основні кроки даного алгоритму для використання їх при отриманні стійких до атак хеш-кодів аудіо-сигналів.

1) Попередньо необхідно створити базу даних із зразків аудіо-файлів. Для цього буде використано мікрофон телефону, чи аудіо-гарнітури, підключеної до персонального комп’ютеру.

2) Зчитування та аналіз даних аудіо-зразків у байт-масиві. Для візуалізації даних байт-масив відобразимо у вигляді лінійного графіка (рис. 2).

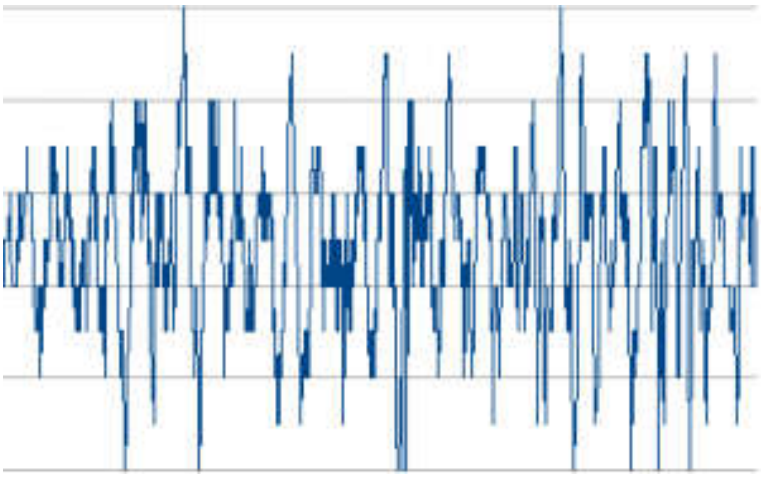

Рис. 2. Візуалізація отриманих даних

Ці дані зазвичай називають часовою областю. Представлення звукового файлу в такому вигляді дозволяє проводити його аналіз у відношенні до часу [4]. Але отримання цих даних є лише початком, бо для алгоритму Shazam є необхідним отримання спектрального аналізу замість прямих даних часової області.

3) Спектральний аналіз. На даному етапі до файлу застосовують дискретне перетворення Фур’є, що перетворить дані с часової області в частотну. Коли дані перетворюються в частотну область, втрачається кожний біт інформації про час. Таким чином, отримується величина всіх частот, але без інформації про те, коли вони з’являються. Для вирішення цієї проблеми дані розподіляються на сегменти та перетворюються у цих сегментах по одному. Завдяки цьому можна визначити дані всіх частот на утвореному сегменті.

4) Визначення ключових точок в аудіофайлі та збереження їх у вигляді хеш-коду. Для кожної лінії спектрального аналізу обираються точки з найбільшою величиною із певного діапазону (рис. 3).

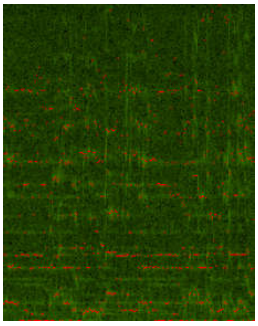

Рис. 3. Отримання ключових точок аудіо-файлу

5) Отримання «зовнішніх» аудіофайлів та порівняння їх з існуючими у базі даних за допомогою отриманих ключових точок.

Розглянемо можливість застосування даного алгоритму з метою передати секретне повідомлення через послідовність аудіо-файлів. Створимо базу даних з аудіофайлів і отриманих з них хеш-кодів. Для бази даних необхідна велика кількість унікальних аудіофайлів. Хеш-код аудіофайлів отримуємо наступним чином.

1. За допомогою алгоритму Shazam отримуємо ключові точки аудіо-файлу, значення яких переведемо у тип цілих чисел. Далі для послідовності отриманих чисел обчислимо хеш-код за допомогою алгоритму MD5. Одному символу повідомлення поставимо у відповідність чотири зразки аудіо-сигналів таким чином, щоб ASCII-код символу повідомлення співпадав з двома першими символами хеш-кодів аудіофайлів (рис. 4).

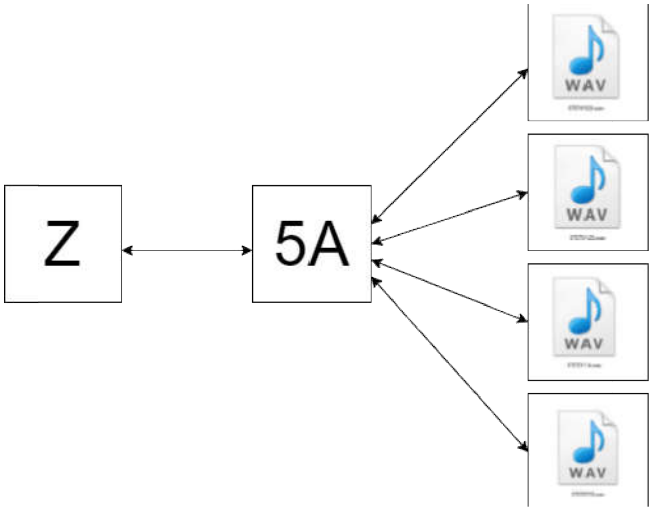

Рис. 4. Схема відповідності «символ-аудіо»

2. Перетворюємо наше повідомлення у ASCII-послідовність та поділяємо її на рівні частини по два символи.

3. Кожній парі символів ASCII-послідовності ставимо у відповідність аудіо-файл. Отримаємо послідовність аудіо-файлів, що є контейнером стеганоповідомлення та готова до передачі.

4. Після отримання послідовності аудіо-файлів одержувач записує у ряд перші два символи з хеш-кодів файлів, в результаті чого отримує ASCII-послідовність, котру необхідно перевести в текст для отримання оригінального повідомлення.

Висновки

В роботі представлено метод хеш-стеганографії, заснований на використанні хеш-кодів цифрових аудіо-сигналів. Алгоритм даного методу є стійким до різноманітних видів атак та на даний час не має аналогів для порівняння. Подальші зусилля авторів спрямовано на дослідження можливостей даного методу та підвищення його ефективності.

Список літератури

1. Иваненко В.Г., Пивошенко Я.И. Способ защиты авторского права на аудио сигналы основанный на пакетной вейвлет-декомпозиции. *Безопасность информационных технологий.* 2013. № 1. С. 72–74.
2. Roy S., Manasmita M. A novel approach to format-based test stegonography, *International conference on communication computing and security*, ICCCS 2011, Proceedings by ACM, Odisha,India. P.511-516
3. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. М.: Солон-Пресс, 2002. 272 с.
4. Бохонько М.В., Зоріло В.В. Модифікація методу хеш-стеганографії. *VII Міжнародна науково-практична інтернет-конференція «Сучасний рух науки»*, 6-7 червня 2019 р. Дніпро, 2019. С.605-608.

DEVELOPMENT OF A METHOD FOR TRANSMITTING SECRET MESSAGES BASED ON HASHING OF DIGITAL AUDIO FILES

V.V. Zorilo, O.Yu. Lebedeva, V.V. Konofolskyi

Odessa National Polytechnic University,
1, Shevchenko Ave, Odessa, 65044, Ukraine, whiteswanhelena@gmail.com

Steganography and cryptography are at their peak these days. One of the types of steganography is hash steganography. This is a fundamentally new direction in the transmission of secret information. Hash steganography methods are based on the fact that instead of embedding secret information into a container, we transmit a specific sequence of digital signals and recover messages from their hash codes. Digital images are commonly used for these principles to work. However, digital audio files, thanks to the many services and messengers, are becoming an increasingly popular method of transferring information. Therefore, the development of hash steganography methods based on the use of audio signals is urgent. The aim of this work is to improve the efficiency of transmission of a secret message by modifying the hash steganography method. In this paper, the Shazam`s algorithm is used to obtain hash codes of a digital audio signals that are resistant to attacks and file transformations. this method does not use embedding additional information in the audio file as a container. In this method, it is proposed to use a hash code (hereinafter the hash) obtained from audio files to build a stegan message. But when transferring and converting audio files, the integrity of their hash code may be compromised due to possible loss of quality and noise. This can interfere with matching files and hash codes and restoring the secret message. One of the popular audio file identification services is the Shazam software application. Shazam allows you to correctly identify audio tracks, even in the presence of noise, extraneous sounds and more. Consider the main steps of this algorithm for their use in obtaining attack-resistant hash codes of audio signals. This algorithm allows representing audio as a set of special points, which are then converted into hash codes using the MD5 method. Secret messages are recovered from these hash codes after receiving a specific sequence of audio signals. The developed algorithm has no analogues for comparison, but it is resistant to attacks.

Keywords: hash-steganography, audio-file, hash-code.

DOI 10.15276/imms.v10.no 3-4.142
УДК 681.5.015.23:658.264

Informatics and Mathematical Methods in Simulation
Vol. 10 (2020), No. 3-4, pp. 142-153

АВТОМАТИЗОВАНА СИСТЕМА УПРАВЛІННЯ ПОТУЖНІСТЮ КОМБІНОВАНОЇ ТЕПЛОФІКАЦІЙНОЇ УСТАНОВКИ КОТЕДЖНОГО БУДИНКУ

Т.М. Клябіна, К.В. Беглов

Одеський національний політехнічний університет
65044, Одеса, пр. Шевченка, 1, beglov.kv@opu.ua

В статті розглянуто автоматизовану систему управління потужністю комбінованою теплофікаційною установкою, яка складається з газового котла, електричного котла та теплового насосу. Використано математичну модель, в якій враховується залежність витрат на виробництво теплової енергії від вартості первинних енергоносіїв, тобто природного газу та електроенергії. Ця модель використовується для визначення найкращого способу розподілення навантаження між джерелами теплової енергії, які працюють на загального споживача. Визначено цільову функцію, для пошуку мінімуму якої використано модифікований сиплекс метод. Особливістю дослідження є моделювання обладнання як динамічного об'єкта управління. При цьому процедура пошуку мінімуму функції реалізована у вигляді програмного файлу. Це дозволяє оцінити час пошуку при роботі на реальному обладнанні, а також використати цей файл для програмування промислового контролера. Метою управління стає підтримка оптимального співвідношення в системі між максимальною ефективністю використовуваного устаткування і мінімумом вартості витрачених ресурсів при заданій якості управління. З розвитком технічних засобів автоматизації та широким використанням цифрових контролерів для об'єктів керування з невеликим інформаційним навантаженням, таких наприклад як індивідуальні опалювальні котельні, розумні будинки тощо, з'являється можливість використовувати досить складні методи керування, а саме оптимальне керування. Більш того, можна розглянути новий підхід до управління технічними структурами не лише за параметрами, але і по структурі взаємозамінного устаткування системи, яке відрізняється своєю надійністю, ефективністю і вартістю. Тому проведено дослідження автоматизованої системи керування, яка дозволить зменшити витрати на опалення котеджного будинку за рахунок найбільш раціонального розподілення навантаження між елементами установки, яка виробляє теплову енергію.

Ключові слова: керування, комбіноване джерело енергії, навантаження, оптимізація, симплекс метод

Вступ

Від сучасних АСУТП очікують надійну адаптацію до зміни середовища їх використання за відсутності або з мінімальним втручанням оператора при їх функціонуванні. Сучасний рівень розвитку теорії оптимального управління та теорії адаптивних АСУ дозволяє розглянути новий підхід до управління технічними структурами не лише за параметрами, але і по структурі взаємозамінного устаткування системи, яке відрізняється своєю надійністю, ефективністю і вартістю.

В нинішній час активно ведуться дослідження систем керування які дозволяють змінювати структуру об'єкта керування в залежності від технологічних потреб або економічних показників роботи таких об'єктів.

Метою ж управління стає підтримка оптимального співвідношення в системі між максимальною ефективністю використовуваного устаткування і мінімумом вартості витрачених ресурсів при заданій якості управління.

З розвитком технічних засобів автоматизації та широким використанням цифрових контролерів для об’єктів керування з невеликим інформаційним навантаженням, таких наприклад як індивідуальні опалювальні котельні, розумні будинки тощо, з’являється можливість використовувати досить складні методи керування, а саме оптимальне керування.

Тому варто провести дослідження автоматизованої системи керування яка дозволить зменшити витрати на опалення котеджного будинку за рахунок найбільш раціонального розподілення навантаження між елементами установки, яка виробляє теплову енергію.

Аналіз останніх досліджень і публікацій

Класичним методом розподілу навантаження між джерелами теплової енергії, що працюють на загального споживача, являється розподіл по найменшому відносному приросту витрати палива [1]. З причини своєї класичності, цей метод застосовують на багатьох енергогенеруючих підприємствах (котельних, ТЕЦ, ТЕС), модифікований для реалізації в сучасних АСУ ТП. Але знову і знову з'являються роботи, що дозволяють підвищити якість рішень з автоматизованого управління обладнанням. До таких робіт можна віднести [2, 3, 4].

В роботі [2, с. 71-77] проведений опис програмного забезпечення, що дозволяє керувати розподілом теплового та електричного навантаження між енергоблоками. Цільовою функцією в цьому випадку обрано мінімізацію витрати палива в цілому по електростанції. В якості програмного забезпечення використовується SCADA система на базі сучасних цифрових обчислювальних систем.

В роботі [3, с. 25-27] розглянуто методику визначення годинної витрати палива на основі відносних приростів витрати палива блоку. Для рішення задачі застосовується числові методи. Критерієм оптимальності являється умова рівності відносних приростів витрати палива для котлів, що працюють на різних потужностях.

В роботі [4, с. 15-20] проведений аналіз алгоритмів оптимального управління технологічними процесами що відбуваються на енергоблоках ТЕС. Важливим з точки зору керування різнорідним обладнанням є висновок, що з керувати економічністю технологічного процесу за допомогою пошуку мінімуму відносного приросту витрати палива некоректно. Це обумовлено перехідними процесами, що відбуваються в системі «котел - турбіна — генератор» при зміненні потужності. Застосування цього критерію можливе тільки для строго стаціонарних режимів роботи обладнання без будь-яких зовнішніх і внутрішніх збурень. При перехідних процесах в тепловому обладнанні питома витрата палива коливається іноді непередбачуване й не вірно відображає миттєву економічність його роботи.

Таким чином при оперативному управлінні котельним устаткуванням, наприклад, при збуреннях, пов'язаних зі зміною складу палива, оптимізація його роботи не робиться. Однією з причин цього є той факт, що пошукові процедури ґрунтовані на розрахункової залежності питомої витрати палива від навантаження котла, але при відхиленні складу палива від розрахункового отримати вказані залежності не представляється можливим, як це показано в роботі [5].

Більш того, якщо обладнання має різні джерела енергії, а саме газ та електроенергію, то відносну витрату палива розглядати взагалі не має сенсу. Така ситуація спостерігається при одночасному використанні газових та електричних котлів, а також теплових насосів.

Дослідження критеріїв для пошукових систем керування проведено в роботі [6]. Подальший розвиток це дослідження отримало у роботі [7], де розглянуто змінення структури енергосистеми для найбільш ефективного навантаження енергоблоків з

точки зору мінімізації вартості ціни на електроенергію, але при цьому з обмеженнями на мінімальні навантаження енергоблоків.

Подальший розвиток дослідження систем керування об'єктами зі змінною структурою отримало у роботі [8]. В неї розглянуто метод пошуку найбільш ефективної структури біотенкової установки.

В роботах [9] та [10] була розглянута задача розподілення навантаження між котлами, які працюють на загального споживача. Але в цих випадках вважалось, що обладнання має однакову потужність та розрізняється коефіцієнтом корисної дії.

Мета роботи

Таким чином можна сформулювати мету цієї роботи: дослідити автоматизовану систему керування, яка виконує пошук такого розподілу навантаження між елементами теплофікаційної установки, яке забезпечує найменші експлуатаційні витрати на генерацію теплової енергії. Дослідити зміну експлуатаційних витрат теплофікаційної установки при роботі на частковій потужності кожного з джерел.

Викладення основного матеріалу

Для визначення найкращого навантаження кожного виду джерела теплової енергії пропонується використовувати критерій, що враховує коефіцієнт корисної дії джерела та вартість первинного енергоресурсу, а саме вираз:

$$I(v) = \sum_{j=1}^{n} a_j \cdot S[\eta(v_j), C_j] \qquad (1)$$

де n - кількість джерел енергії;
a_j - ваговий коефіцієнт для j-го джерела;
S - витрати на експлуатацію джерела теплової енергії;
$\eta(v_j)$ - коефіцієнт корисної дії j-го джерела теплової енергії, який залежить від навантаження джерела;
v_j - відносне навантаження, $v_j = [0,1]$;
C_j - ціна енергоресурса, який використовується у j-му джерелі теплової енергії (ціна газу або електроенергії).

Ваговий коефіцієнт a_j застосовується для вибору пріоритету у використанні джерела. Це можна робити, наприклад, для зменшення годин експлуатації обладнання, для подовження його ресурсу.

Метою роботи АСР є мінімізація функції I, а саме експлуатаційних витрат установки теплофікації при роботі на частковій потужності кожного з агрегатів.

Для реалізації процедури пошуку пропонується використовувати модифікований симплекс метод (Нелдера - Міда). Цей метод був вибраний виходячи з того, що він не вимагає знаходження похідної функції. В порівнянні з градієнтними методами, симплекс методу вимагає меншої кількості точок розрахунку. Так для одного кроку розрахунку градієнтним методом потрібна, як мінімум, 4 точки, для симплекс методу треба 3 точки розрахунку.

Алгоритм розрахунку оптимальних значень навантаження обладнання зроблено за допомогою роботи [9] та реалізовано в пакеті Matlab (ліцензія 1–4 AE K761327 ВД, № 308918). Причому, робота обладнання з обчисленням значень η і $I(v)$, моделювалася в пакеті Simulink, а обчислювальна пошукова процедура виконувалася шляхом виклику

функції з командного рядка Matlab. Таким чином були враховані динамічні властивості котлів і враховані перехідні процеси, викликані зміною завдань регуляторам.

Для досягнення поставленої мети, були виконані такі завдання:

1) За відомими математичними моделями котеджу, газового котла, електричного котла і ТНУ були розроблені імітаційні моделі в середовищі Simulink пакета Matlab.

2) Для сформульованого критерію оптимальності (мінімум експлуатаційних витрат) був обраний метод знаходження мінімуму цільової функції. Для числової реалізації був обраний симплекс метод, як не вимагає знаходження градієнта цільової функції і, відповідно, вимагає менших обчислювальних процедур. Обчислення цільової функції в 4 точках, замість обчислення в 6 точках для функції 3 змінних.

3) Побудована динамічна модель АСР була змодельована в пакеті Simulink. Промоделювати пошук мінімуму цільової функції для комбінації початкових умов:

- температура навколишнього середовища -5, -10, -20 С;
- ціна електроенергії 1; 1,5; 5 грн/кВт год.
- ціна природного газу 3,62 грн/м^3

За основу для розробки динамічних моделей об’єкта керування були взяті моделі, що наведені у роботах [11] та [12].

Динамічна модель котеджу

З точки зору управління температурою повітря в приміщенні котедж являє собою теплообмінник. Конкретні числові значення для математичної моделі були взяті з джерела [12]. Структура моделі показані на рис. 1, числові значення коефіцієнт приведені в табл. 1.

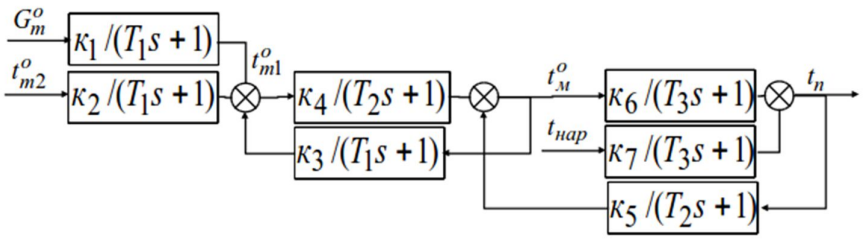

Рис. 1. Структурна схема математичної моделі котеджу

Таблиця 1.

Динамічні характеристики моделі котеджу

№ каналу	Канал	Коефіцієнт	T
1 канал	$G_m^o \to t_{m1}^o$	κ_1 = 1,4 К/(кг·с$^{-1}$)	T_1 = 30 с
2 канал	$t_{m2}^o \to t_{m1}^o$	κ_2 = -0,008 К/К	
3 канал	$t_м^o \to t_{m1}^o$	κ_3 = 1,008 К/К	
4 канал	$t_{m1}^o \to t_м^o$	κ_4 = 0,957 К/К	T_2 = 0,124 с
5 канал	$t_n \to t_м^o$	κ_5 = 0,042 К/К	
6 канал	$t_м^o \to t_n$	κ_6 = 0,85 К/К	T_3 = 351 с
7 канал	$t_{нар} \to t_n$	κ_7 = 0,167 К/К	

Динамічні моделі газового котла, електричного котла та ТНУ

З точки зору керування температурою води після теплоносія, який подається на опалення котеджу, газовий котел, електричний котел і ТНУ також представляють собою теплообмінники. Однак, керуючим впливом для газового котла є витрата палива, для електричного котла і ТНУ — витрата електроенергії. Також, для розрахунку кількості тепла, що виробляє джерело, в моделях враховується температура теплоносія на вході в джерело.

Конкретні числові значення для математичної моделі були взяті з роботи [3]. Структури моделей показані на рисунках 2, 3, 4, числові значення коефіцієнт приведені в табл. 2, 3, 4.

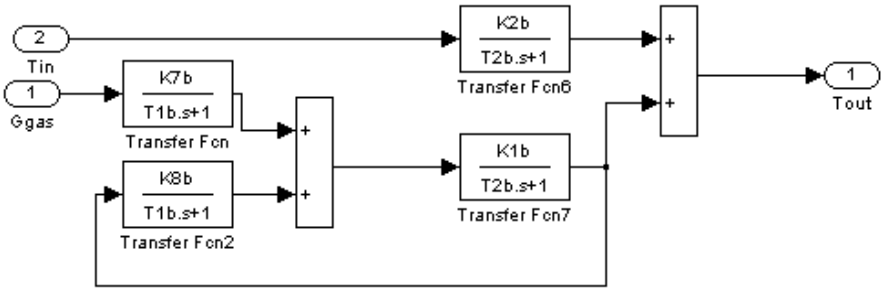

Рис. 2. Структурна схема математичної моделі газового котла

Таблиця 2.

Динамічні характеристики моделі газового котла

№ каналу	Канал	Коефіцієнт	T
1 канал	$G_г \to t^p_м$	K_7 = 1679 К/(кг·с$^{-1}$)	T_1 = 6 с
2 канал	$t^p_{m2} \to t^p_м$	K_8 = 1 К/К	
3 канал	$t^p_{m1} \to t^p_{m2}$	K_2 = 0,2 К/К	T_2 = 7 с
4 канал	$t^p_м \to t^p_{m2}$	K_1 = 0,8 К/К	

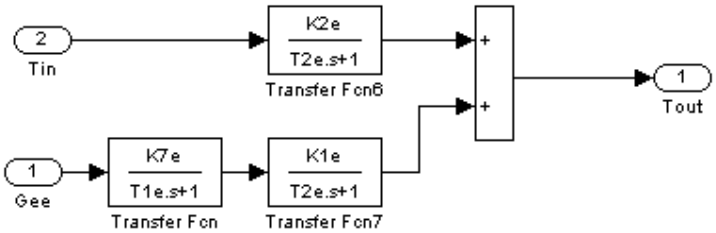

Рис. 3. Структурна схема математичної моделі електричного котла

Таблиця 3.

Динамічні характеристики моделі електричного котла

№ каналу	Канал	Коефіцієнт	T
1 канал	$G_г \to t^p_м$	K_7 = 0,00024 К/(кг·с$^{-1}$)	T_1 = 120 с
2 канал	$t^p_{m1} \to t^p_{m2}$	K_2 = 1 К/К	T_2 = 140 с
3 канал	$t^p_м \to t^p_{m2}$	K_1 = 6,8 К/К	

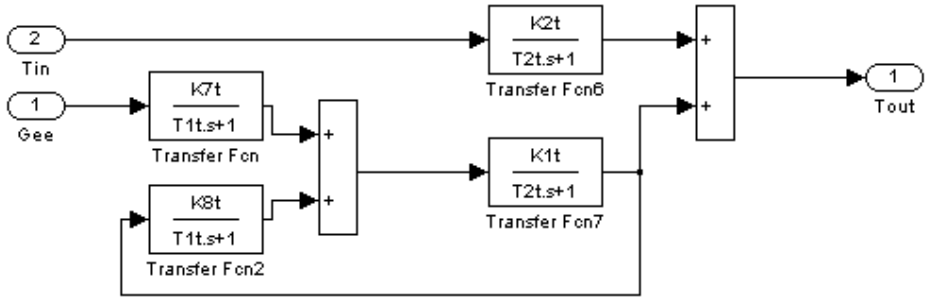

Рис. 4. Структурна схема математичної моделі ТНУ

Таблиця 4.

Динамічні характеристики моделі ТНУ

№ каналу	Канал	*к*	*T*
1 канал	$G_г \to t^p_м$	K_7 = 0,00024 К/(кг·с$^{-1}$)	T_1 = 10 с
2 канал	$t^p_{m2} \to t^p_м$	K_8 = 1 К/К	
3 канал	$t^p_{m1} \to t^p_{m2}$	K_2 = 1 К/К	T_2 = 14 с
4 канал	$t^p_м \to t^p_{m2}$	K_1 = 6,8 К/К	

Прийнято, що кожне джерело теплової енергії має локальний регулятор; закон регулювання пропорційно-інтегральній. Виходячи з властивостей об'єкта управління були отримані значення параметрів налаштування для всіх регуляторів.

Вибір методу оптимізації

Пошук мінімуму функції виконувався за допомогою симплекс методу. Реалізація методу була взята з джерела [9].

Даний метод був вибраний виходячи з того, що він не вимагає знаходження похідної функції. У порівнянні з градієнтними методами, симплекс методу вимагає меншої кількості точок розрахунку. Так для одного кроку розрахунку градієнтним методом необхідно, як мінімум, 4 точки, для симплекс методу потрібно 3 точки розрахунку.

Метод пошуку був реалізований у вигляді програми мовою Matlab.

Побудова динамічної моделі в Simulink

Математичні моделі газового котла, електричного котла і ТНУ були доповнені блоками розрахунку теплової енергії, яку виробляє обладнання, ККД джерела та витрат на експлуатацію.

Кількість теплової енергії, що виробляє джерело розраховується за формулою:

$$Q = M \cdot c_p (t_{out} - t_{inp}) = k\Delta t$$

де M — масова витрата води через джерело теплової енергії;
c_p — теплоємність води;
t_{out} — температура на виході з джерела енергії;
t_{inp} — температура на вході в джерело енергії.

Витрата води підтримується постійною, теплоємність води також можна вважати постійною для робочого діапазону температур. Тому кількість теплової енергії пропорційна різниці температур на вході та виході джерела енергії.

Коефіцієнт корисної дії газового котла та теплонасосної установки розраховуються за формулою [10]

$$\eta(v) = \frac{\eta_{max}}{Q_{max}^2} \cdot \left(Q - Q_{max}\right)^2 + \eta_{max} = 2 \cdot \eta_{max} \cdot v \cdot \left(1 - v\right)$$

де η_{max} — максимальний ККД установки,

Коефіцієнт корисної дії електричного котла вважається постійним та незалежним від потужності.

Витрати на експлуатацію газового котла розраховуються за формулою:

$$S_{ГК} = \left(\frac{v \cdot Q_{max}}{Q_H^p \cdot \eta}\right) \cdot C_Г$$

де Q_H^p - теплота згоряння природного газу.

Витрати на експлуатацію електричного котла розраховуються за формулою:

$$S_{ГК} = \left(\frac{v \cdot Q_{max}}{\eta}\right) \cdot C_{EE}$$

Витрати на експлуатацію теплонасосної установки розраховуються за формулою:

$$S_{ГК} = \left(\frac{v \cdot Q_{max}}{A \cdot \eta}\right) \cdot C_{EE}$$

де $A = 3{,}351 + 0{,}082 \cdot t_{НС}$ - розрахункове значення коефіцієнту перетворення теплового насосу (*Coefficient of Performance, COP*) в залежності від температури навколишнього середовища $t_{НС}$.

Для моделювання АСР динамічні моделі котеджу, джерел теплової енергії (ГК, ЕК, ТНУ) регуляторів були зведені в одну схему показану на рис. 5. Крім того, на схемі розташовані блоки const, які задають ціну електроенергії, ціну газу і температуру навколишнього середовища і номінальне значення температури в приміщенні. Так само, розташовані елементи для контролю значень витрат теплової потужності і температур теплоносія і всередині приміщення.

Для реалізації пошукового алгоритму в робочої області Matlab зберігаються значення теплової втрати котеджу, сумарна теплова потужність виробляється джерелами тепла і сумарні витрати на експлуатацію.

Моделювання АСР

Для дослідження АСР були прийняті наступні початкові умови:
- температура повітря в приміщенні 20 °С;
- температура навколишнього середовища -5, -10, -20 °С;
- ціна газу 3,62 грн/м^3;
- ціна електроенергії 1; 1,5; 5 грн/кВт год;

- за результатами теплового розрахунку котеджу прийнято максимальні теплові втрати при температурі -20 С - 28 188 Вт;
- максимальна теплова потужність газового котла — 21,1 кВт, при цьому максимальна витрата газу 9 м^3/год;
- максимальна теплова потужність електричного котла - 17 кВт;
- максимальна теплова потужність ТНУ - 16 кВт.

Приклади результатів моделювання зведені в таблицях 5–7.

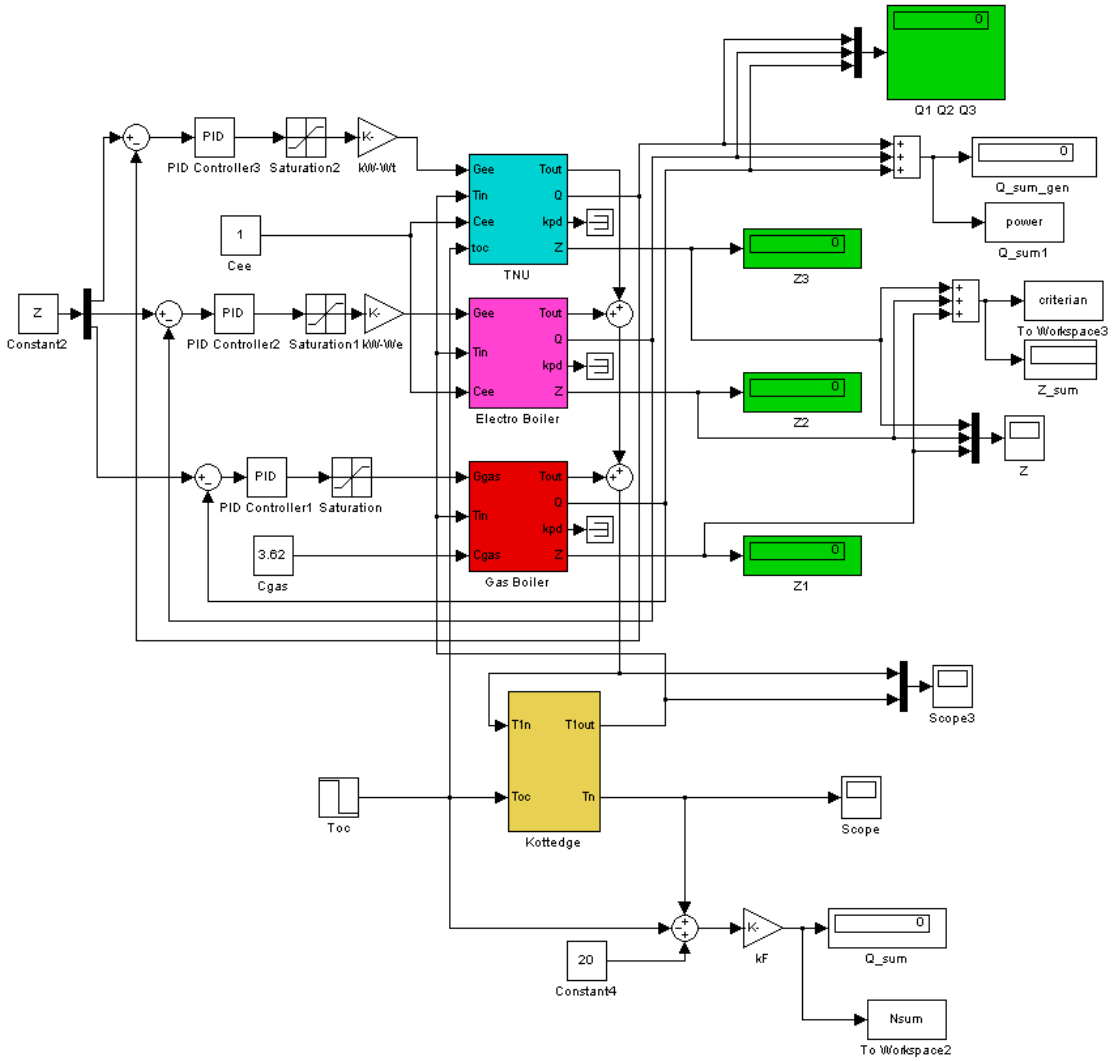

Рис. 5. Схема моделювання АСР теплопостачання котеджу

Таблиця 5.

Дані першого експерименту

toc = -20°C		ТНУ	ЭК	ГК
Сээ = 1,5 грн/кВт год	$\nu_{нач}$	0.5790	0.5449	0.4411
Знач = 168.8	$Q_{нач}$, кВт	9.2634	9.2634	9.2634
Зопт = 159,4	$\nu_{опт}$	0.7771	0.5379	0.2290
	$Q_{опт}$, кВт	12.434	9.144	4.809

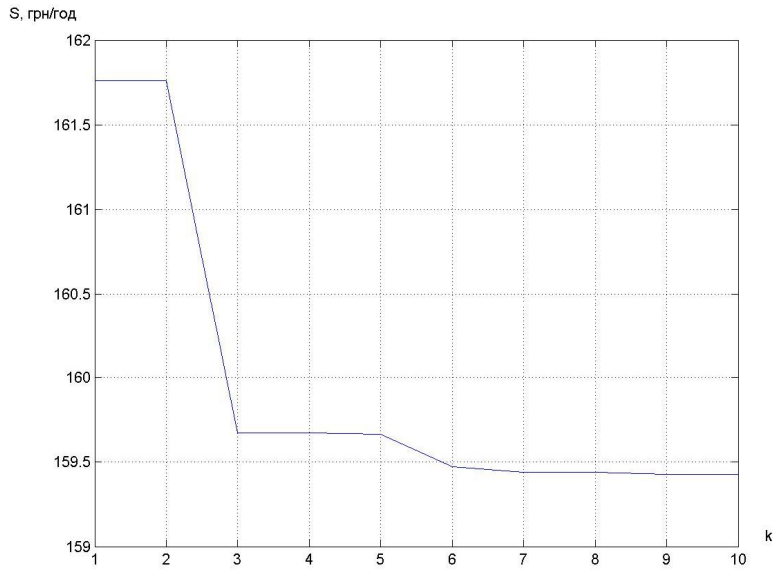

Рис. 6. Зміна сумарних витрат від номеру ітерації при даних табл. 5

Таблиця 6.

Дані другого експерименту

toc = -20°C		ТНУ	ЭК	ГК
Сээ = 5 грн/кВтгод	$\nu_{нач}$	0.5790	0.5449	0.4411
Znач = 275.8	$Q_{нач}$, кВт	9.2634	9.2634	9.2634
Zопт = 266.75	$\nu_{опт}$	0.2791	0.7342	0.5300
	$Q_{опт}$, кВт	4.466	12.482	11.130

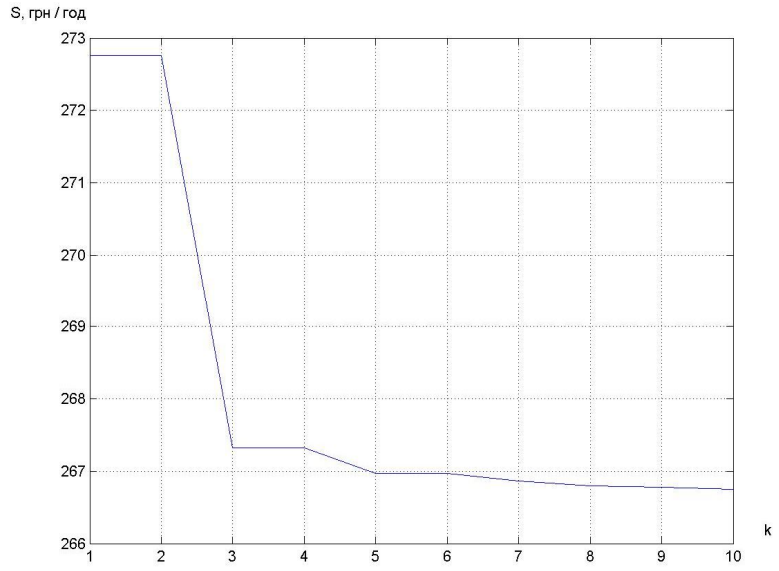

Рис. 7. Зміна сумарних витрат від номеру ітерації при даних табл. 6

Таблиця 7.

Дані третього експерименту

toc = -5		ТНУ	ЕК	ГК
Сээ = 1,5 грн/ кВтгод	$\nu_{нач}$	0.3842	0.3616	0.2927
Znач= 150.2	$Q_{нач}$, кВт	6.1472	6.1472	6.1472
Zопт= 149.15	$\nu_{опт}$	0	0.7712	0.2645
	$Q_{опт}$, кВт	0	13.111	5.554

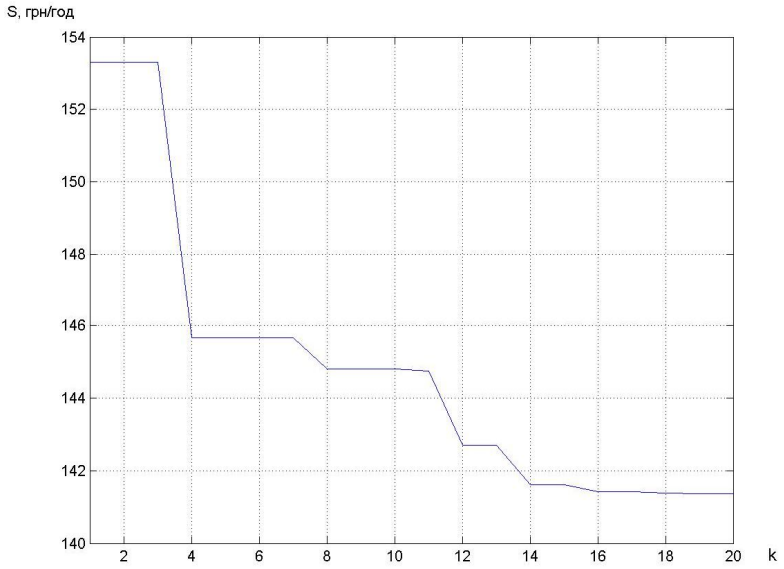

Рис. 8. Зміна сумарних витрат від номеру ітерації при даних табл. 7

Висновок

В роботі досліджено роботу АСР, яка виконує пошук мінімуму інтегрального показника роботи обладнання.

Для досягнення поставленої мети були виконані такі завдання:

1) За відомим математичним моделям котеджу, газового котла, електричного котла і ТНУ були розроблені імітаційні моделі в середовищі Simulink пакета Matlab

2) Для сформульованого критерію оптимальності (мінімум експлуатаційних витрат) був обраний метод знаходження мінімуму цільової функції. Для числової реалізації був обраний симплекс метод, як не вимагає знаходження градієнта цільової функції і, відповідно, вимагає менших обчислювальних процедур. Обчислення цільової функції в 4 точках, замість обчислення в 6 точках для функції 3 змінних.

3) Побудована динамічна модель АСР була змодельована в пакеті Simulink. Виконаний пошук мінімуму цільової функції для комбінації початкових умов:

- температура навколишнього середовища -5, -10, -20 °С;
- ціна електричної енергії 1; 1,5; 5 грн/кВт * год.
- ціна газу 3,62 грн/м^3;

Результати моделювання наведені в таблиці 5.1 — 5.3.

За результатами моделювання можна відзначити наступне: у всіх випадках процедура пошуку мінімуму виконується, тобто відбувається зменшення експлуатаційних витрат. При низьких температурах навколишнього середовища (-20 °С) всі джерела теплопостачання працюють на частковому навантаженні. При середніх температурах (-10 °С) і тарифі за електроенергію менш ніж тариф на природний газ в

роботі знаходяться лише електричний котел і ТНУ. При тарифі на електроенергію вище ніж тариф на газ включається в роботу газовий котел. При високих температурах навколишнього середовища (-5 °С) експлуатація газового котла економічно недоцільна і теплове навантаження покривають частково електричний котел і теплонасосна установка.

Список літератури

1. Кожевников Н.Н. Басова Т.Ф., Борисов Е.И., Бологова В.В. и др. Экономика и управление энергетическими предприятиями. М.: Академия, 2004. 432 с.
2. Макарчьян В.А. Черняев А.Н., Андрюшин А.В. и др. Программный комплекс распределения нагрузок ТЭЦ со сложным составом оборудования, схемами отпуска тепла и электроэнергии. *Теплоэнергетика.* 2013. №5. С. 71-77.
3. Реймов К.М. Определение критерия оптимального распределения активной нагрузки между агрегатами ТЭС. *Автоматизированные технологии и производства*. 2016. № 2 (12). С. 25-27.
4. Аракелян Э.К. Васильев Е.Д., Хуршудян С.Р. Проблемы современных автоматизированных систем управления технологическим процессом на базе программно-технических комплексов и возможный путь их решения. *Вестник МЭИ*. 2014. № 1. С. 15-20.
5. Maksimov M.V., Lozhechnikov V.F., Dobrovolskaya T.S., Bondarenko A.V. Mathematical model of non-certified burning fuels. *East European Journalof Advanced Technologies.* 2014. V. 2.No8 (68). P. 44-52.
6. Максимова О.Б., Максимов М.М., Силина В.С., Орищенко А.В. Разработка метода определения целевой функции оптимизации электростанции. *Автоматизация технологических и бизнес-процессов*. 2017. Т.9, № 2. С. 28–35.
7. Максимова О.Б., Максимов М.М., Силина В.С., Орищенко А.В. Анализ эффективности баланса энергосистемы, обеспечиваемого различными группами генерирующих электростанций. *Автоматизация технологических и бизнес-процессов*. 2017. Т.10, № 4. С.47–55.
8. Maksymov, M., Beglov, K., Maksymova, O., &Maksymov, O. (2020). The method of finding the most natural structure of a biotank power plant. *Odes'kyi Politechnichnyi Universytet. Prats.* 2020. #1.P. 82-96.
9. Лысюк, А., Беглов К. Автоматизация распределения нагрузки между параллельно работающими котлами. *Автоматизация технологических и бизнес-процессов*. 2017. V.*9,* #3. P.37-46.
10. Концур В.О., Беглов К.В.. Оптимізація режиму роботи групи котлів під час спалювання несертифікованого палива. *Вчені записки Таврійського національного університету імені В.І. Вернадського*. 2020. Т. 31 (70). Ч.1.No 3, С.115 – 120.
11. Максименко И.Н. Тодорцев Ю.К. Объектно-ориентированная модель системы теплоснабжения. Информационные модели. *Труды Одесского политехнического университета*. 2005. Вып. 2 (24). С. 160 – 164.
12. Максименко И.Н. Тодорцев Ю.К., Беглов К.В. Модели элементов установки теплоснабжения как объекта автоматизации. *Автоматика. Автоматизация. Электротехнические комплексы и системы*. 2005. № 2 (16). С. 27 – 31.

CONTROL SYSTEM FORPOWER COMBINED HEATING INSTALLATION OF COTTAGE HOUSE

T.M. Klyabina, K.V. Beglov

Odessa National Polytechnic University
65044, Odessa, 1 Shevchenko Ave., beglov.kv@opu.ua

The article considers a control system with the combined district heating system, which consists of a gas boiler, an electric boiler and a heat pump. A mathematical model is used, which takes into account the dependence of the costs of thermal energy production on the cost of primary energy sources, i.e. natural gas and electricity. This model is used to determine the best way to distribute the load between heat sources that work on the general consumer. The objective function is determined, for the search of the minimum of which the modified simplex method is used. A feature of the study is the modeling of equipment as a dynamic object of control. The procedure for finding the minimum function is implemented in the form of a program file. This allows you to estimate the search time when working on real equipment, as well as use this file to program an industrial controller. The purpose of control is to maintain the optimal ratio in the system between the maximum efficiency of the equipment used and the minimum cost of resources spent at a given quality of control. With the development of technical means of automation and the widespread use of digital controllers for control objects with low information load, such as individual heating boilers, smart homes, etc., it is possible to use quite complex control methods, namely optimal control. Moreover, it is possible to consider a new approach to management of technical structures not only on parameters, but also on the structure of the interchangeable equipment of the system which differs in the reliability, efficiency and cost. Therefore, a study of the automated control system, which will reduce the cost of heating a cottage due to the most rational distribution of load between the elements of the installation, which produces heat.

Keywords: control, combined energy source, load, optimization, simplex method

DOI 10.15276/imms.v10.no 3-4.154
УДК 629.5.063 - 047.37

Informatics and Mathematical Methods in Simulation
Vol. 10 (2020), No. 3-4, pp. 154-166

МОДЕЛЮВАННЯ ПРОЦЕСУ УТВОРЕННЯ ШКІДЛИВИХ ВИКИДІВ У ВИХІДНИХ ГАЗАХ СУДНОВИХ ПАРОВИХ КОТЛІВ

В.С. Михайленко[1], В.А. Щербінін[1], В.В. Лещенко[1], Р.Ю. Харченко[1], Н.В. Ложечнікова[2]

[1]Національний університет «Одеська морська академія», вул. Дідріхсона 8, Одеса, 65029, Україна;
e-mail: romannn30@gmail.com
[2]Одеський національний політехнічний університет, пр.-т Шевченка, 1, Одеса, 65022, Україна;
e-mail: fontan.lev@gmail.com

За причиною посилення вимог Міжнародної конвенції по запобіганню забрудненню від суден, зокрема, Положення про запобігання забруднення повітряного середовища від судів, стає актуальним впровадження нових методів контролю і обмеження концентрації шкідливих викидів суднових агрегатів в атмосферу. У роботі проведено дослідження методів зниження концентрації вмісту викидів оксидів азоту NO_x у вихідних газах суднових парових котлів. Розглянуто сучасні наукові підходи в області зниження шкідливих викидів, зокрема проаналізовані їх переваги та недоліки. Зміст NOx у вихідних газах може бути досягнуто шляхом впливу на максимальну температуру горіння, що забезпечується введенням газів рециркуляції. Димові гази з температурою 300-400 °С відбираються перед повітряним підігрівачем і рециркуляційних димососів і подаються в топку. В результаті максимальна температура в топці знижується на 120-130 °С і падає концентрація кисню в зоні горіння, що також зменшує утворення паливних NOx. При цьому ККД парового котла знижується порівняно мало (0,01-0,03% на 1% рециркулюючих газів). Ефективність зменшення утворення оксидів азоту при введенні газів рециркуляції визначається наступними факторами: місцем відбору газів на рециркуляцію; умовами їх введення в топку; ступенем рециркуляції r,%; розподілом газів рециркуляції за обсягом камери згоряння; станом котла. Запропоновано метод, який реалізує нейромережевий алгоритм в системі управління рециркуляцією димових газів, який відрізняється можливістю мінімізації змісту значень оксидів азоту NO_x при роботі суднового котла при різних теплових навантаженнях. Порівняльне моделювання запропонованої нейромережевої і традиційної системи автоматичного управління процесом рециркуляції димових газів при роботі суднового котла з 50% навантаженням показало перевагу нейромережевої системи управління, навченої на досягнення мінімально можливого вмісту шкідливих викидів в атмосфері.

Ключові слова: Шкідливі викиди, судновий барабанний водотрубний паровий котел, нейромережевий алгоритм, система управління рециркуляцією димових газів, теплове навантаження.

Вступ

Останні вимоги міжнародних конвенцій (МК): МАРПОЛ 73/78, Паризької конференції, затвердили нормативи шкідливих викидів та відходять газами суднових енергетичних установок (СЕУ). У зв'язку з цим на суднах, що експлуатуються 10 і більше років, установка нового устаткування для зниження шкідливих викидів від агрегатів СЕУ, зокрема, суднових дизелів та парових котлів стало економічно не вигідна. Дана проблема передбачає пошук нових більш економічних шляхів модернізації систем горіння суднового палива й очищення газів с метою зниження концентрації шкідливих викидів в атмосферу [1] без значних капіталовкладень.

Аналіз основних досліджень і публікацій

Зараз діє цілий ряд підходів щодо зменшення концентрації шкідливих газів в атмосфері від обладнання СЕУ: первинні методи, які полягають в придушенні викидів, зокрема, NO_x в топках котлів або камерах згоряння дизелів, і вторинні методи зниження викидів NO_x, які полягають в обробці димових газів після котла або дизеля [2]. Попри великий обсяг виконаних досліджень, роботи більшості вчених спрямовані на зниження викидів оксидів азоту методами селективного каталітичного і некаталітичного відновлення оксидів азоту [2]. Зазначені методи хоча і забезпечують високий ступінь очищення димових газів, але при цьому пов'язані зі значними фінансовими витратами і засновані на використанні небезпечних хімічних реагентів. Також за даними [1] коштовні апарати очищування – скрубери встановлені на не більш ніж на 1% від загального числа судів, і галузеві аналітики пророкують, що до 2021 року їх число навряд чи перевищить 10-20%. Тому проблема розробки та впровадження на суднах нових, економічно відносно недорогих та екологічно ефективних методів очищення відпрацьованих газів суднових дизелів і котлів від оксидів азоту і сірки в зв'язку зі строгими вимогами Додатка VI МК МАРПОЛ є актуальною.

Мета роботи

Дослідження процесу мінімізації шкідливих викидів газів суднових парових котлів, зокрема оксидів азоту (NOx).

Основна частина

Згідно з дослідженнями [3] зниження концентрації шкідливих викидів, зокрема, зміст NO_x у вихідних газах може бути досягнуто шляхом впливу на максимальну температуру горіння, що забезпечується введенням газів рециркуляції. Димові гази з температурою 300-400 °С відбираються перед повітряним підігрівачем і рециркуляційних димосмоків і подаються в топку. В результаті максимальна температура в топці знижується на 120-130 °С і падає концентрація кисню в зоні горіння, що також зменшує утворення паливних NOx. При цьому ККД парового котла знижується порівняно мало (0,01-0,03% на 1% рециркулюючих газів). Ефективність зменшення утворення оксидів азоту при введенні газів рециркуляції визначається наступними факторами: місцем відбору газів на рециркуляцію; умовами їх введення в топку; ступенем рециркуляції r,%; розподілом газів рециркуляції за обсягом камери згоряння; станом котла.

Ефективність рециркуляції тим більше чим вище температура в зоні горіння. Вона знижується при:

- зменшенні навантаження котла;
- зменшенні температури горіння палива;
- збільшенні коефіцієнта надлишку повітря;
- підвищення вмісту азотовмісних сполук в паливі.

Залежність вмісту азоту в продуктах згоряння суднового котла від коефіцієнта надлишку повітря визначається по формулі

$$\alpha = \frac{N_2}{N_2 - 3{,}76O_2} \tag{1}$$

Як типовий об'єкт дослідження обрано судновий допоміжній двобарабанний паровий котел (СПК) фірми Mitsubishi типу MAC 50, продуктивністю 50 тон пари на

годину, робочим тиском пари 1.57 МПа (16 кгс/см^2), температурою пари 280 ^{o}С і ККД 82,5% (рис. 1). Цим типом котлів обладнані багато суден танкерного флоту [4].

Оскільки більшу частину часу СПК функціонує в стаціонарному режимі роботи на навантаженні, що приблизно дорівнює 50% від номінального з дотриманням принципу суперпозиції, а також у зв'язку з поширеності в САУ об'єктів СЕУ, лінійних ПІД - регуляторів (до 85% від усіх алгоритмів), вводилося допущення про можливість опису найбільш ймовірних режимів роботи СПК за допомогою лінійних математичних моделей, тобто вводилися спрощуючи припущення. Нелінійності, що входять в рівняння динаміки параметрів СПУ, відносяться до класу лінеарізуємих. Це дає можливість застосувати метод малих відхилень, що забезпечує цілком прийнятну точність не тільки при вирішенні задачі стійкості, але і при визначенні динамічних характеристик.

Так нелінійну модель СПК доцільно замінити спектром моделей, лінеаризованих щодо кількох режимів функціонування.

Вхідними керуючими впливами математичної моделі СПК як об'єкта управління (рис. 2) є: зміни витрати палива ΔB_T, положення напрямних апаратів дуттєвого вентилятора Δn_L і димососа $\Delta n_Г$, витрати живильної $\Delta D_{ПВ}$ і продувочної води $\Delta D_{ПР}$. Контрольованими вихідними параметрами є: зміна концентрації кисню в димових газах ΔC_{O2}, розрідження в топці ΔP_P, рівня води в барабані котла $\Delta h_б$, тиску пари в паровій магістралі ΔP_M або витрати пари ΔD_n (в залежності від режиму роботи котла), солевмісту в барабані котла ΔCa [4]. Основними збурюючими впливами є зміни витрати Δn_n і тиску пари в паропроводі ΔP, обумовлені зміною теплового навантаження споживача пари агрегатами СЕУ.

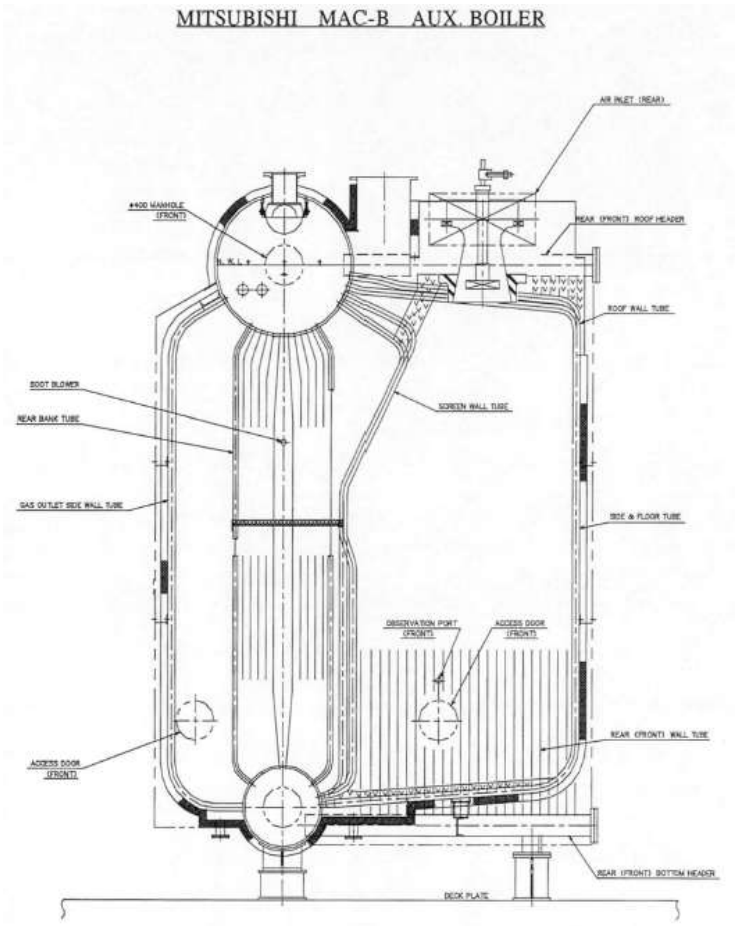

Рис. 1. Конструктивний вид допоміжного СПК

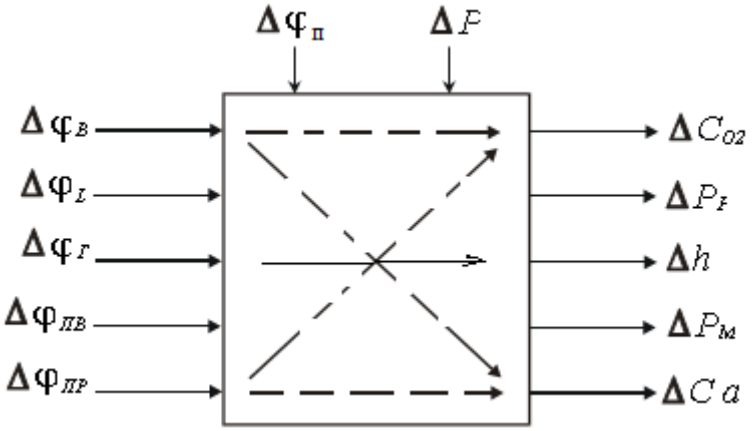

Рис. 2. Параметрична схема СПК

При розрахунку багатовимірної і типової систем автоматичного регулювання та моделюванні їх роботи масові витрати палива ΔB_T , живильної $\Delta D_{ПВ}$ і продувної $\Delta D_{ПР}$ води будуть виражені через положення відповідних регулюючих клапанів $\Delta\varphi_B$, $\Delta\varphi_{ПВ}$ і $\Delta\varphi_{ПР}$.

У зв'язку з наявністю істотних нелінійностей в системі управління рециркуляцією, маючи на увазі специфічні умови роботи СПУ і часту зміну режимів навантаження, пропонується замість стандартного лінійного ПІД - регулятора скористатися адаптивним нелінійним нейромережевим регулятором. Реалізація нейромережевого регулятора або контролера (FFC) (рис. 3) може бути виконана на базі нейрочипа CM1K фірми The Cogni Mem Technologies. Даний чіп містить 1024 нейрона, які працюють паралельно [5].

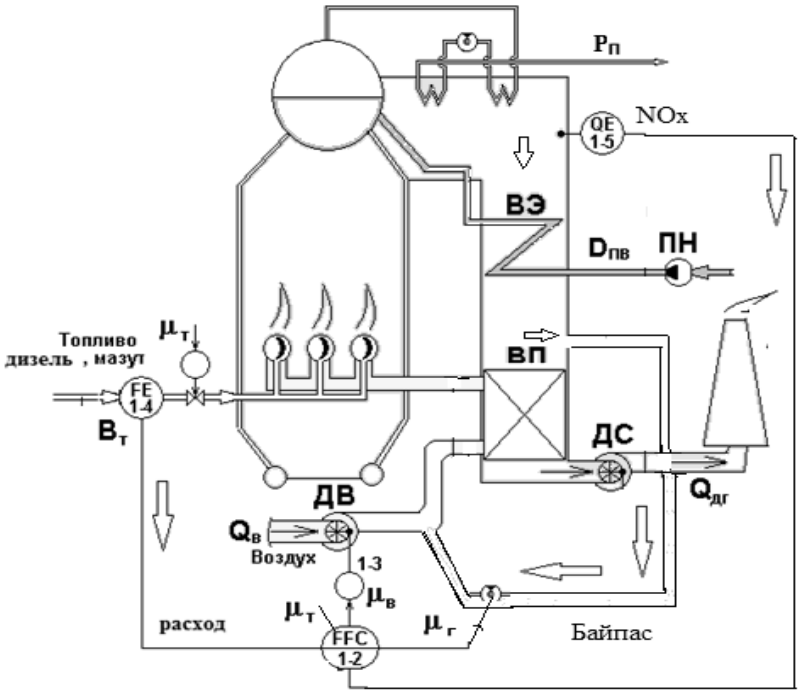

Рис. 3. Схема нейромережевої системи управління процесом рециркуляції димових газів парогенератора марки Mitsubishi Marin Main Boiler MB паровою продуктивністю 150 т/год. ДС - димосос; ДВ - дуттєвой вентилятор; ВП - повітряний підігрівач; ВЕ - водяний економайзер; ПН - живильний насос; QE - газоаналізатор; FFC - регулятор рециркуляції (нейромережевой); FE - витратомір; μ - керуючі впливи.

Основним структурним елементом математичної моделі СПК, необхідним для апробації системи управління рециркуляції димових газів, є газо-повітряний тракт, який складається з газоходу і повітроводу. Регульованими параметрами для цієї ділянки є розрідження димових газів у верхній частині топкової камери і надлишок повітря, що характеризує економічність процесу горіння.

При виведенні диференціальних рівнянь газоходу і повітроводу, як ділянок регулювання розрідження в топці, були прийняті наступні допущення: газохід після димососа і повітропровід після дуттєвого вентилятора дуже короткий і зворотна реакція тиску в топці на витрату мазуту і повітря на вході впливає мало; акумулююча ємність топки і газоходів зосереджена в одному об'ємі, а дроселююча здатність газоходів і поверхонь нагріву зосереджена в одній точці. Регулювання здійснюється шляхом зміни положення направляючого апарату димососа і дуттєвого вентилятора. З урахуванням перерахованих припущень регульовані ділянки можуть бути замінені спрощеною системою, що складається з ємності, дроселя і димососа (дуттєвого вентилятора).

Регульованою величиною є відхилення тиску в топці ΔP_P від заданого значення; вхідний величиною (регулюючим впливом) – зміна положення направляючого апарату димососа $\Delta\varphi_Г$. В якості зовнішнього збурення приймемо зміну витрати газів на притоці ΔM. Таким чином, диференціальні рівняння в приростах з урахуванням лінеаризації в робочих точках мають такий вигляд [6]:

$$T_1^{21}\frac{d\Delta P_p}{dt} + \Delta P_P = k_1^{21}\Delta\varphi_Г + k_2^{21}\Delta M \ .$$

$$T_1^{21} = (a_L^Г - a_P^Г)\frac{m_Г}{\overline{P}_Г}\alpha;\ k_1^{21} = -b_P^Г;\ k_2^{21} = a_L^Г - a_P^Г, \qquad (2)$$

де $m_Г$ – маса димових газів в газоході котла в стаціонарному режимі роботи, кг;

$\overline{P}_Г$ – тиск димових газів у верхній частині топкової камери, Па;

$a_P^Г, a_L^Г, b_P^Г$ – визначаються графічно за витратними характеристикам газоходу і димососа; k_i^n і T_i^n - коефіцієнти, які мають постійне значення в заданому режимі функціонування котла (n - відповідає номеру диференціального рівняння, і - порядковий номер коефіцієнта); α - коефіцієнт (для мазуту 0.65).

Вихідні дані для розрахунку коефіцієнтів диференціальних рівнянь визначені по напірним характеристикам відцентрового димососа одностороннього всмоктування DN-12,5 [7] і гідравлічної характеристиці газоходу мазутного водотрубного барабанного котла ГМ 50 (аналог суднових допоміжних котлів середньої потужності типу МАС) представлені в [4]:

$$m_г = 78{,}2 \text{ кг}; P_г = 1{,}01 \text{ кПа}; \alpha = 1{,}15; \alpha_L^г = 2\text{kQ}$$

$$k = \frac{\Delta H_p}{Q_p^2} = \frac{5000-1200}{70000^2} = 0{,}7\cdot 10^{-6} \text{ мм.вод.ст.}\cdot\text{год}^2/\text{м}^6$$

$$\alpha_L^г = 2\cdot 0{,}7\cdot 10^{-6}\cdot 72\cdot 10^3 = 50.4\cdot 10^{-3}\text{мм.вод.ст.}\cdot\text{год/м}^3 = 0{,}5 \text{ Па}\cdot\text{год/м}^3 = 23{,}6 \text{ Па}\cdot\text{с/кг}$$

$$\alpha_L^г = \frac{\Delta H_p}{Q_p^2} = \frac{40{,}4}{5{,}5\cdot 10^3} = 7{,}3\cdot 10^{-3} \text{ мм.вод.ст.}\cdot\text{год}^2/\text{м}^3 = 0{,}07 \text{ Па}\cdot\text{год/м}^3 = 1{,}89 \text{ Па}\cdot\text{с/кг}$$

$$b_p^г = \frac{\Delta H_\phi}{\Delta_\phi} = \frac{80{,}2}{50} = 1{,}6 \text{ мм.вод.ст./\%} = 15{,}7 \text{ Па/\% ходу}$$

$$T_1^{21} = (23,6 - 1,9) \cdot \frac{78,2}{1,01 \cdot 10^3} \cdot 1,15 = 1,93 \text{ с}$$

$$k_1^{21} = -15,7 \text{Па/\% ходу}$$

$$k_1^{21} = 21,7 \text{ Па} \cdot \text{с/кг}$$

Таким чином, після підстановки коефіцієнтів в рівняння (2) отримали

$$1,93 \frac{dP_p}{dt} + P_P(t) = -15,7\varphi_\Gamma(t) + 21,7M(t) \cdot \qquad (3)$$

Після виконання перетворення Лапласа (3) отримані передаточні функції за каналами управління $W(s)_{\mu\text{-р}}$ (зміна положення направляючого апарату – зміна тиску димових газів) і збурення $W(s)_{M\text{-р}}$ (зміна витрати газів – зміна рециркуляційного тиску в газоході)

$$W(s)_{\mu\text{-р}} = \frac{-15,7}{1,93s+1}; \quad W(s)_{M-p} = \frac{21,7}{1,93s+1}.$$

Тривимірна модель направляючого апарату димососа з зазначенням зміни кута положення $\Delta\varphi_\Gamma$ представлена на рис. 4.

Після виконання розрахунків для двох найбільш часто працюючих режимів СПУ (50% і 25% від номінального парового навантаження) отримані наступні значення коефіцієнтів диференціального рівняння (2) на трьох режимах теплового навантаження (табл.1).

Таблиця 1.

Розрахункові коефіцієнти рівняння (1)

Навантаження від номінального	25%	50%	75%
T^1_{21}	1,9	5,8	7,6
k^1_{21}	-15,7	- 23,4	-56,2
k^2_{21}	21,7	34,3	42,8

Таким чином, отримана система диференціальних рівнянь для трьох режимів роботи СПУ має вигляд:

$$\left.\begin{aligned} 1,93\frac{dP_p}{dt} + P_P(t) &= -15,7\varphi_\Gamma(t) + 21,7M(t) \\ 5,8\frac{dP_p}{dt} + P_P(t) &= -23,4\varphi_\Gamma(t) + 34,3M(t) \\ 7,6\frac{dP_p}{dt} + P_P(t) &= -56,2\varphi_\Gamma(t) + 42,8M(t) \end{aligned}\right\}$$

Зміна кута лопатей направляючого апарату димососа показано на рис. 4

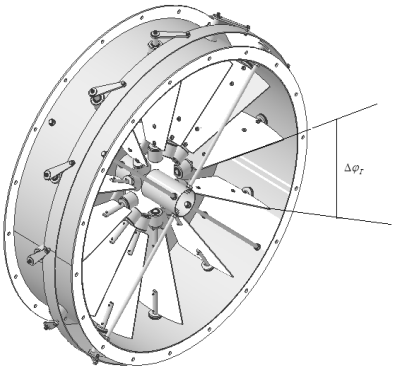

Рис. 4. Тривимірна модель направляючого апарату

Перехідні характеристики представленої системи рівнянні по каналах керування й збурення представлені на рис. 5-6.

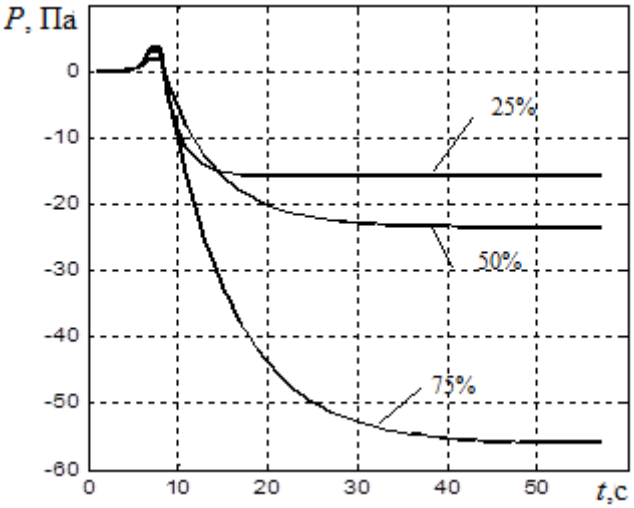

Рис. 5. Зміна тиску димових газів для трьох режимів роботи СПК при роботі направляючого апарату

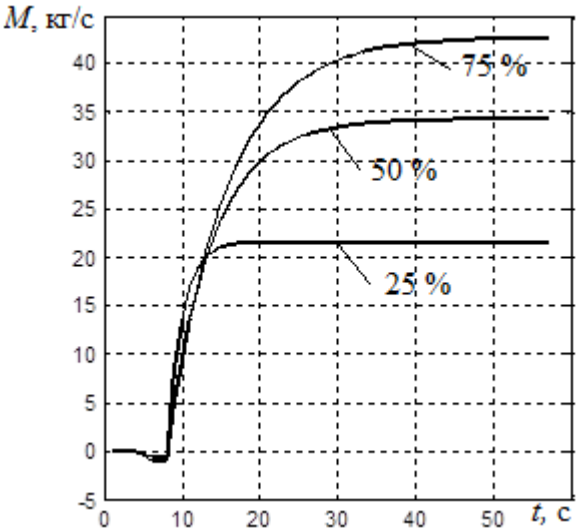

Рис. 6. Зміна витрати димових газів при трьох режимах роботи

Втрата теплоти з газами q_2 є найбільшою з усіх теплових втрат в суднових парогенераторах. Для СПУ вона коливається в межах від 5 до 23% і більше [7]. Величина q_2 залежить від ентальпії відхідних газів, яка визначається за формулою:

$$I_{ух} = V_Г \times C_Г \times V_{ух}.$$

де $V_Г$ - обсяг відхідних газів, м^3; $C_Г$ - об'ємна ізобарна теплоємність продуктів згоряння, кДж / (м^{3}К); $V_{ух}$ - швидкість газів, м / с.

При контролі $V_{ух}$ необхідно враховувати, що температура стінки хвостових поверхонь нагріву $t_{ст}$ СПК повинна бути вище точки роси $t_р$, при якій суміш водяної пари сірчаної кислоти що знаходиться в продуктах згоряння конденсується. При виникненні умов коли $t_{ст} < t_р$, суміш парів починає конденсуватися на поверхнях нагріву і під впливом сірчаної кислоти починає відбуватися інтенсивне руйнування металів труб, тобто починається процес низькотемпературної корозії. У продуктах згоряння сірчистих мазутів завжди присутні пари води і сполуки сірки, які утворюють при з'єднанні один з одним сірчану кислоту. При обмиванні газами відносно холодних хвостових поверхонь нагріву пари сірчаної кислоти конденсуються на них і викликають корозію металу [8].

Таким чином, з урахуванням впливу швидкості $V_{ух}$ димових газів, що відходять, на процеси утворення низькотемпературної корозії $\Delta N^T_к$, пропонується доповнити рівняння (2) параметром, що характеризує корозійний процес.

$$T_1^{21}\frac{d\Delta P_p}{dt} + \Delta P_P = k_1^{21}\Delta\varphi_Г + k_2^{21}\Delta M + k_4^{21}\Delta N_k^T,$$

$$k_4^{21} = t_s + 2\cdot 10^3\sqrt[3]{\Delta\varphi_г / Q_н^p}$$

де t_s – температура насичення водяної пари, відповідна їх парціальному тиску в продуктах згоряння, ^{0}С; $\Delta\varphi_г$ – положення направляючого апарату димососа,%; $Q_{нр}$ – нижча теплота згоряння робочої маси палива, кДж/кг. Для режиму навантаження 75%, отримали:

$$k_4^{21} = 201 + 2000\cdot\sqrt[3]{70/1400} = 941,$$

після підстановки коефіцієнта, рівняння (2) має наступний вигляд:

$$7{,}6\frac{dP_p}{dt} + P_P(t) = -56{,}2\varphi_Г(t) + 42{,}8M(t) + 941\,\Delta N_k^T(t)$$

У подальших рівняннях залежність від часу (t) не відображається.

Аналогічним чином можна отримати значення коефіцієнта k_4^{21} і для інших навантажувальних режимів роботи СПК.

Динамічні властивості повітряводу, що визначають залежність між зміною подачі повітря в топку котла і положенням направляючого апарату дуттєвого вентилятору $\Delta\varphi_B$, описуються рівнянням виду [9]:

$$T_2^{22}\frac{d^2\Delta M_L}{dt^2} + T_1^{22}\frac{d\Delta M_L}{dt} + \Delta M_L = k_1^{22}\frac{d\Delta\varphi_B}{dt} + k_2^{22}\Delta\varphi_B. \quad (4)$$

$$T_2^{22} = \frac{-a_P^B (a_L^B)^2}{a_L^B - a_P^B}\left(\frac{m_B}{\overline{P}_B}\alpha\right)^2;\ T_1^{22} = \frac{-2a_P^B a_L^B + (a_L^B)^2}{a_L^B - a_P^B}\left(\frac{m_B}{\overline{P}_B}\alpha\right);\ k_1^{22} = \frac{b_P^B a_L^B}{a_L^B - a_P^B}\left(\frac{m_B}{\overline{P}_B}\alpha\right);$$

$$k_2^{22} = \frac{b_P^B}{a_L^B - a_P^B},$$

де m_B – маса димових газів в повітроводі котла в стаціонарному режимі роботи, кг;

$\overline{P}_B$ – середнє значення тиску повітря в повітроводі, Па;

a_P^B, a_L^B, b_P^B – визначаються графічно за витратними характеристикам повітряводу і дуттєвого вентилятора; ML - витрата повітря, м^3/год. Розрахункові значення коефіцієнтів для трьох режимів роботи СПК представлені в табл. 2.

Таблиця 2.

Розрахункові коефіцієнти рівняння (4)

Навантаження від номінального	25 %	50 %	75 %
T_2^{22},с	3,9	6,8	9,3
T_1^{22},с	4,2	9,1	16,1
k_1^{22}, кг/ %	2,3	4,5	7,4
k_2^{22} кг/с%	8,1	26,1	28,3

Система диференціальних рівнянь що описують динамічні властивості повітряводу при трьох режимах роботи СПК має вигляд:

$$\left.\begin{aligned}
&3{,}9\frac{d^2\Delta M_L}{dt^2} + 4{,}2\frac{d\Delta M_L}{dt} + \Delta M_L = 2{,}3\frac{d\Delta\varphi_B}{dt} + 8{,}1\Delta\varphi_B \\
&6{,}8\frac{d^2\Delta M_L}{dt^2} + 9{,}1\frac{d\Delta M_L}{dt} + \Delta M_L = 4{,}5\frac{d\Delta\varphi_B}{dt} + 26{,}1\Delta\varphi \\
&9{,}3\frac{d^2\Delta M_L}{dt^2} + 16{,}1\frac{d\Delta M_L}{dt} + \Delta M_L = 7{,}4\frac{d\Delta\varphi_B}{dt} + 28{,}3\Delta\varphi_B
\end{aligned}\right\}$$

З метою подальшого моделювання САУ об'єктів СПК з ПІД - регуляторами, кожне з рівнянь системи представлено у вигляді передаточних функцій:

$$\begin{aligned}
W(s)_{M_L-\varphi} &= \frac{2{,}3s + 8{,}1}{(3{,}9s^2 + 4{,}2s + 1)} \\
W(s)_{M_L-\varphi} &= \frac{4{,}5s + 26{,}1}{(6{,}8s^2 + 9{,}1s + 1)} \\
W(s)_{M_L-\varphi} &= \frac{7{,}4s + 28{,}3}{(9{,}3s^2 + 16{,}1s + 1)}
\end{aligned}.$$

Для визначення динаміки процесу зміни коефіцієнта надлишку повітря, що впливає на концентрацію NOx, використовується експериментальна залежність (рис. 7)

[10, 11]. На основі цієї залежності відбувається навчання нейромережевого регулятора (НСК), керуючого процесом рециркуляції димових газів.

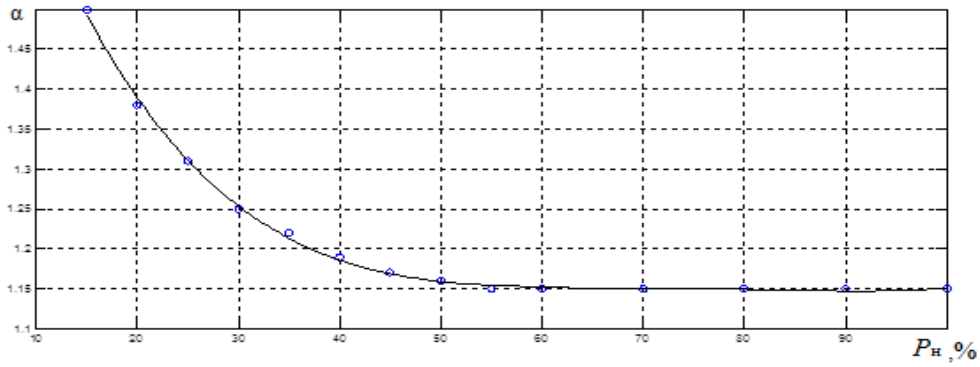

Рис. 7. Статична характеристика α = f (Рн)

Навчальна вибірка для НСК оптимального режиму горіння палива за критерієм мінімізації NOx представлена в табл.3. З урахуванням наявності бібліотеки елементів нейронної мережі, для навчання нейромережевого контролера (НСК) були використані спеціалізовані програмні редактори в пакеті MatLab [10], що реалізують методи еталонного управління і діють на основі алгоритму навчання –- зворотного поширення помилки [12, 13]. Нейрони 1-го шару мають активаційну функцію – гіперболічний тангенс, а у нейронів 2-го шару активаційні функції лінійні. Детальна схема навчання НСК представлена в роботі [12]

Таблиця 3.

Навчальна вибірка для НСК

Навантаження котла,%	10	30	50	70	90
α	*1,5*	*1,25*	*1,16*	*1,15*	*1,1*
NOx * 100 мг/м^3	*2,7*	*4,6*	*6,0*	*8,2*	*8,8*

Перехідні процеси, отримані в результаті моделювання нейромережевої і традиційної САУ рециркуляції СПК на трьох режимах теплового навантаження, представлені на рис. 8-9.

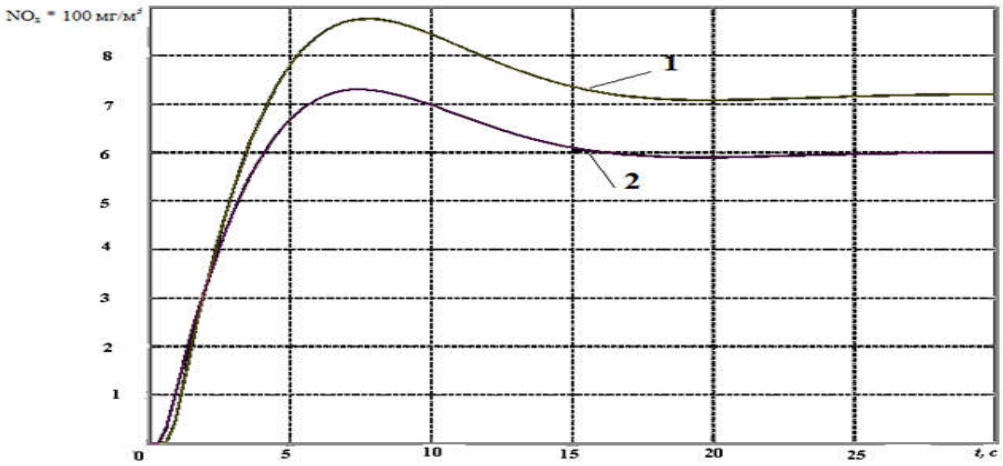

Рис. 8. Перехідні процеси регулювання змісту NOx у вихідних газах суднового котла: 1 – традиційна САУ з ПІД - регулятором (α = 1,3); 2 – нейромережева САУ (α = 1,16 див. табл.3) при тепловому навантаженні СПК, що дорівнює 0,5 від номінального.

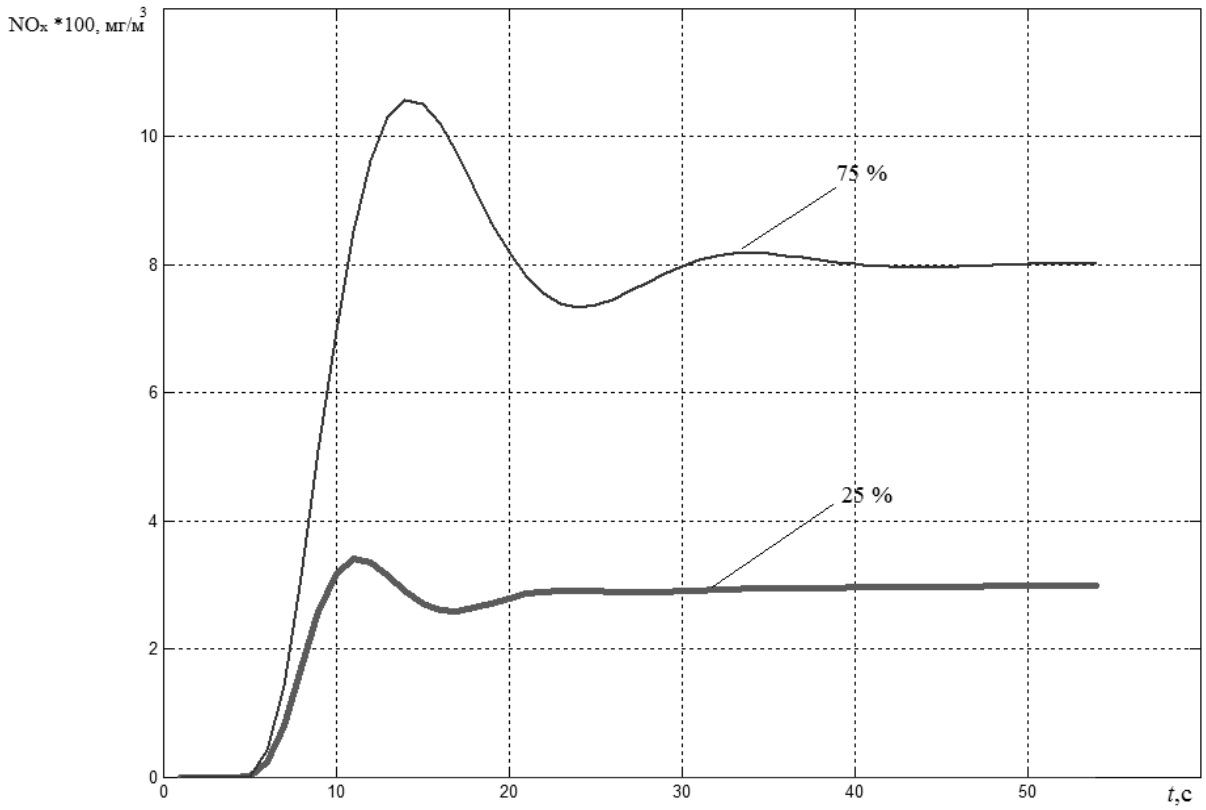

Рис. 9. Перехідні процеси регулювання змісту NOx у вихідних газах суднового котла при роботі на двох теплових режимах 25, 75%

Висновки

Порівняльний аналіз перехідних процесів САУ (див. рис. 8-9) продемонстрував зменшення вмісту NOx в середньому на 25% в порівнянні з типовою системою управління. Таким чином, використання запропонованої структури управління представляється перспективним для впровадження на судах різного типу і дозволяє виконати вимоги Міжнародних конвенцій без істотних капіталовкладень в закупівлю нового обладнання або модернізації старого.

Список літератури

1. ИМО 2020 – перспективы судоходной отрасли и нефтеперерабатывающих заводов URL: https://modcon.ru/applications/судоходство-и-морские-перевозки.
2. Хачоян М.М. Снижение выбросов оксидов азота с отработавшими газами судовых дизелей и котлов абсорбцией водой: автореферат диссертации кандидата тех. наук. Новороссийск: ГМУ им. Ф.Ф. Ушакова, 2013. URL: http://www.dslib.net/sudovenergoustanovki/snizhenie-vybrosov-oksidv-azota-s-otrabotavshimi-gazami-sudovyh-dizelej-i-kotlov.html.
3. Электроэнергетика и охрана окружающей среды. Функционирование энергетики в современном мире URL: http://energetika.in.ua/ru/books/book-5/intro
4. Профос П. Регулирование паросиловых установок. М.: Энергия, 1967. 368 с.
5. Нейронный процессор URL: https://ru.wikipedia.org/wiki/Нейронный_процессор.

6. Boiler Construction and Design. URL: www.marineinsight.com
7. Серов Е.П., Корольков Б.П. Динамика парогенераторов. М.: Энергия, 1972. 416с
8. Вентиляторный завод Укрвентсистемы URL: ukrvent.com/dn-12-5_dymosos-html
9. Бураков, М.В. Нейронные сети и нейроконтроллеры. СПб.: ГУАП, 2013. 284 с.
10. Михайленко В.С., Ложечников В.Ф. Усовершенствование системы управления рециркуляцией дымовых газов судового вспомогательного котла. *Автоматизация судовых технических средств*. 2019. №.25. С. 53 – 62.
11. Mac type aux. boiler operation and maintenance instructions. URL: https://ru.scribd.com/doc/219150052/Operation-and-Maintenance-1.
12. Mikhailenko V.S. Kharchenko Yu. Analysis of traditional and neuro-fuzzy adaptive system of controlling the primary steam temperature in the direct flow steam generators in TPS. *Automatic Control and Computer Sciences*, 2014, V. 48, No. 6, P. 334–344.
13. Михайленко В.С. Харченко Р.Ю. Решение задач идентификации и управления температурным контуром системы охлаждения судового дизеля. *Науковий вісник Херсонської державної морської академії*. 2017. №2 (17). С. 69-77.

MODELING THE PROCESS OF HAZARDOUS EMISSIONS FORMATION IN THE EXHAUST GASES OF SHIP'S STEAM BOILERS

V.S. Mikhailenko[1], V.A. Shcherbinin[1], V.V. Leshchenko[1], R.Yu. Kharchenk[1], N.V. Lozhechnikova[2]

[1]NU "Odessa Maritime Academy", Odessa, Ukraine, 8, Didrikhson str., Odessa, 65029, Ukraine, e-mail: romannn30@gmail.com
[2]Odessa National Polytechnic University, Shevchenko ave., 1, Odessa, Ukraine; e-mail:fontan.lev@gmail.com

In view of the tightening of the requirements of the International Convention for the Prevention of Pollution from Ships, in particular, the Regulation on the Prevention of Air Pollution from Ships, it becomes urgent to introduce new methods for monitoring and limiting the concentration of harmful emissions from ship units into the atmosphere. The NOx content in the exhaust gases can be achieved by influencing the maximum combustion temperature provided by the introduction of recirculation gases. Flue gases with a temperature of 300-400 ° C are selected in front of the air heater and recirculation smoke extractors and fed into the furnace. As a result, the maximum temperature in the furnace is reduced by 120-130 ° C and the oxygen concentration in the combustion zone decreases, which also reduces the formation of fuel NOx. The efficiency of the steam boiler is reduced relatively little (0.01-0.03% per 1% of recirculation gases). The efficiency of suppression of the formation of nitrogen oxides during the introduction of recirculation gases is determined by the following factors: the place of selection of gases for recirculation; the conditions of their introduction into the furnace; the degree of recycling r,%; distribution of recirculation gases by the volume of the combustion chamber; boiler condition. The study of methods for reducing the concentration of NOx in the exhaust gases of ship steam boilers. The modern scientific approaches in the field of reducing harmful emissions are

considered, in particular, their advantages and disadvantages are indicated. A method is proposed that implements a neural network algorithm in a flue gas recirculation control system, which is characterized by the ability to minimize the content of NOx values when a ship's boiler is operating at different thermal loads.
Comparative modeling of the proposed neural network ACS and traditional ACS of the flue gas recirculation process when a ship's boiler is operating at 50% load has shown the advantage of a neural network control system trained to achieve the lowest possible content of harmful emissions in the atmosphere.
Keywords: harmful emissions, ship drum water-tube steam boiler, neural network algorithm, flue gas recirculation control system, heat load.

DOI 10.15276/imms.v10.no 3-4.167
УДК 004.62

Informatics and Mathematical Methods in Simulation
Vol. 10 (2020), No. 3-4, pp. 167-176

МЕТОДИ ТА ЗАСОБИ ВИЯВЛЕННЯ НЕАКТУАЛЬНОЇ ТА НЕДОСТОВІРНОЇ ІНФОРМАЦІЇ НА WEB-РЕСУРСАХ

А.М. Мельник

Західноукраїнський національний університет,
вул. Львівська, 11, м. Тернопіль, 46020, Україна, e-mail: melnyk.andriy@gmail.com

У статті розглянуто важливу науково-прикладну задачу виявлення неактуальної та недостовірної інформації на веб-ресурсах, яка є актуальним напрямком розвитку та реалізації методів інтелектуального аналізу даних. Проведено аналіз сучасних методів та засобів оцінки неактуальної та недостовірної інформації з точки зору оцінки інформаційних джерел та виділено основні проблемні напрямки, які виникають в процесі їх функціонування. Запропоновано систему показників фільтрування недостовірної та неактуальної інформації, яка отримана на основі кількох джерел. На основі даної системи реалізовано метод перевірки інформації з веб-ресурсів на актуальність та достовірність. В основі даного підходу покладено можливість використання наперед визначеного ресурсу, дані з якого носять тільки достовірний характер.Розроблено метод виявлення недостовірної та неактуальної інформації, враховуючи особливості її поширення через відповідні сторінки у соціальних мережах та використання багатозадачної класифікації інформації, яка отримується із різних джерел даних.Використання запропонованих інтелектуальних методів обробки даних разом із іншими методами інтелектуального аналізу, які використовуються для оцінки інформації отриманої з інтернету, дозволить значно підвищити ефективність процесу встановлення неактуальності та недостовірності інформації, а також дозволить побудувати оцінку конкретного веб-ресурсу на предмет публікації та розповсюдження такої інформації.

Ключові слова: актуальність та достовірність інформації, web-ресурс, інформаційне джерело, соціальні мережі.

Вступ

Виявлення неактуальної та недостовірної інформації є важливим елементом в процесі інформаційної обізнаності та прийняття. Велика кількість інформації, яка розповсюджується через Інтернет, вимагає її всебічної оцінки, а це в свою чергу породжує також питання оцінювання відповідного інформаційного джерела [1-3].

На відміну від друкованих матеріалів, таких як книги та статті, веб-сторінки не повинні відповідати стандартам якості, точності та статистичної достовірності. Ця відсутність контролю якості створює особливі проблеми для встановлення відповідного ступеня довіри [4], в межах якого необхідно оцінювати кожну веб-сторінку на предмет точності, достовірності, актуальності та об’єктивності [5].

В Інтернеті кожна адреса веб-сайту має домен як частину адреси, що дозволяє ідентифікувати власника веб-сайту. Домен або його приналежність до довіреної зони може бути швидким способом оцінити якість веб-ресурсу перед йоговідвідуванням. Як правило, .edu, .gov та .org частіше мають якіснішу інформацію, ніж домени .com [5-7].

У цій роботіреалізовується процедура оцінкидостовірності та актуальності інформації із конкретного веб-ресурсу. Застосування такої процедури також дозволяє провести загальну оцінку відповідного інформаційного джерела на предмет достовірності та актуальності.

Аналіз досліджень та публікацій

Більшість публікацій з даної тематики зорієнтовані на використання методів інтелектуального аналізу [2,3,5,8], а саме штучних нейронних мереж, дерева рішень, використання символьних правил при побудові результуючих характеристик,правила, підходи на основі методів найближчого сусіда, методу опорних векторів, байєсових мереж,лінійної регресії, методів кореляційно-регресійного аналізу; методів кластерного аналізу,зокрема ієрархічні та неієрархічні методи кластерного аналізу [8]; методи пошуку асоціативних правил, метод Apriori; методи обмеженого або часткового перебору перебору, генетичні алгоритми в рамках еволюційного програмування, різноманітні методи візуалізації даних [2]. Більшість перерахованих методів були реалізовані в рамках штучного інтелекту [4-7]. В межах інтелектуального аналізу даних виникає кілька ключових задач, які вимагають розв'язку, виходячи із специфіки предметної області, в якій вони сформовані [7-9]. До таких задач треба віднести такі: класифікації, кластеризації, прогнозування, асоціація, візуалізації, аналіз виявлення відхилень, оцінювання, аналіз зв'язків, підведення підсумків [2,4,7-11].

Водночас, специфіка інформації, яка накопичується в інтернеті, або отримується з нього, вимагає реалізації додаткових підходів, які можна буде легко реалізувати та програмно інтерпретувати в рамках заданої предметної області [12-14]. Особливо актуальним є напрямок розробки методів аналізу інформації на предмет актуальності та достовірності [8].

Мета і задачі дослідження

Отже, метою даної роботи є розробка методів та засобів виявлення неактуальної та недостовірної інформації, яка розміщується на офіційних веб ресурсах організацій та поширюється через відповідні соціальні мережі.

Для досягнення поставленої мети потрібно вирішити такі задачі:

- проаналізувати особливості процесу виявлення неактуальної та недостовірної інформації на веб-ресурсах;
- обґрунтувати використання метрики оцінки достовірності інформації для оцінювання інформації, яка отримується із веб-ресурсів;
- розробити процедуру перевірки інформації з веб-ресурсів на актуальність та достовірність;
- реалізувати метод перевірки інформації з веб-ресурсів на основі аналізу даних, отриманих із соціальних мереж;
- провести експериментальні дослідження та оцінити отримані результати на прикладі веб-ресурсу закладу вищої освіти.

Основна частина

Перевірка веб-ресурсів на наявність неактуальної та недостовірної інформації вручну вимагає великих часових витрат. Така перевірка недостовірної інформації не масштабується за обсягом новоствореної інформації, особливо коли певна організація має кілька ресурсів, включаючи ресурси в різних соціальних мережах. Використання засобів, які спрямовані на автоматизацію такої перевірки, або часткове використання методів автоматичної перевірки в основному ґрунтуються на автоматизації процесів пошуку інформації, методів обробки природної мови, машинного навчання, графової теорії [5,6,11].

У загальному, представленуактуальну інформацію можна моделювати наступним відношенням [1,3,5]:

$$Kw = \langle S, P, O \rangle, \quad (1)$$

де Kw - інформація, яка моделюються наступною трійкою: S - предметна область, P - предикат, O - об'єкт.

Наприклад, розглянемо наступний інформаційний блок на веб-ресурсі класичного закладу освіти: «Західноукраїнський національний університет здійснює підготовку спеціалістів за спеціальністю інженерія програмного забезпечення». В даному блоці можна виділити наступні інформаційні блоки:

$$Kw = \langle ЗУНУ, \text{спеціальність}, \text{Інженерія програмного забезпечення} \rangle.$$

Більшість відомих засобів автоматичного видобування інформаціїгрунтуються на представлені (1) та його відповідній інтерпретації.

Для пошуку неактуальної або недостовірної інформації та побудови відповідно системи її класифікації дані спочатку витягуються з відкритих джерел, які відносяться до однієї категорії або групи відповідних веб-ресурсів деякої установи чи організації. Такий процес часто відноситься до видобування даних або відповідних відношень між ними. Видобування даних можна класифікувати на видобуток даних з одного джерела або з відкритим кодом. Одне джерело видобування даних в основному грунтується на порівняно надійному веб-ресурсі (наприклад, офіційна веб-сторінка установи). Даний спосіб для отримання релевантної інформації є відносно ефективний, але часто призводить до встановлення неповної інформації, оскільки залежить від рівня наповнюваності або актуальності розміщеного контенту.

Пошук актуальної інформації на основі даних із кількох відкритих джерел є менш ефективним, але дозволить значно розширити формування повних та достовірних інформаційних блоків.Для пошуку неактуальної та недостовірної інформації необхідно також сформувати наступні множини (2), (3), (4):

$$At \in Kw, \quad (2)$$

де At - представляє фрагмент даних, який вдалося верифікувати.

$$BaseAt = \{At\}, \quad (3)$$

де $BaseAt$ - представляє множину верифікованих даних.

$$Base\mathrm{Re}lation = \{BaseAt, \mathrm{Re}lationAt\}, \quad (4)$$

де $Base\mathrm{Re}lation$ - представляє множину зв'язків між сутностями, які описані за допомогою відповідних відношень $\mathrm{Re}lationAt$.

Для того, щоб сформувати базу із достовірною інформацією, яка отримана на основі кількох джерел, їх потрібно додатково відфільтрувати, враховуючи наступні особливості:

- Надлишковість представлених даних в одному контексті (наприклад, $Kw = \langle ЗУНУ, \text{спеціальність}, \text{Інженерія програмного забезпечення} \rangle$) та

$$Kw_1 = \left\langle \begin{matrix} \text{Західноукраїнський національний університет, спеціальність,} \\ \text{Інженерія програмного забезпечення} \end{matrix} \right\rangle$$

Kw_1 буде надлишковим представленням, оскільки «ЗУНУ» та «Західноукраїнський національний університет» відповідають одній і тій же сутності;

- Недійсність – показник, який залежить від конкретного інтервалу часу, наприклад, $Kw = \langle ТНЕУ, університет, Україна \rangle$ неактуальна інформація і повинна бути оновлена. Один із варіантів подолання даної проблеми – представлення даних із певним набором часових характеристик або розширення отриманого набору за допомогою встановлення додаткових тверджень;
- Суперечливість представлених даних (наприклад $Kw = \langle ЗУНУ, адреса, Тернопіль \rangle$ та $Kw = \langle ЗУНУ, адреса, Вінниця \rangle$ є суперечливими даними, які вимагають додаткового аналізу);
- Недостовірність веб-ресурсу (складність ідентифікації ресурсу до довіреної зони в рамках заданої предметної області). Достовірність веб-ресурсу можна встановити наприклад через приналежність його доменної адреси до довіреної зони;
- Повнота – наявність інформації, яка отримана із веб-ресурсівне завжди дозволяє встановити її достовірність та актуальність.

Процедура перевірки інформації з веб-ресурсів на актуальність та достовірність. Щоб оцінити достовірність інформації, яка розміщується на офіційних веб-ресурсах установ та організацій, необхідно порівняти дані, які отримані та представлені за допомогою відношення (1) з інформацією, яка отримана з достовірних джерел.

Як правило, процедура перевірки даних для трійки $Kw = \langle S, P, O \rangle$ полягає в оцінці можливості того, що межі, позначені предикатом P, сформовані із врахуванням приналежності S, до вузла, що представляє O в множині $BaseAt$. Зокрема, цей процес можна описати за допомогою наступних кроків, які формалізовано представлені на рисунку 1.

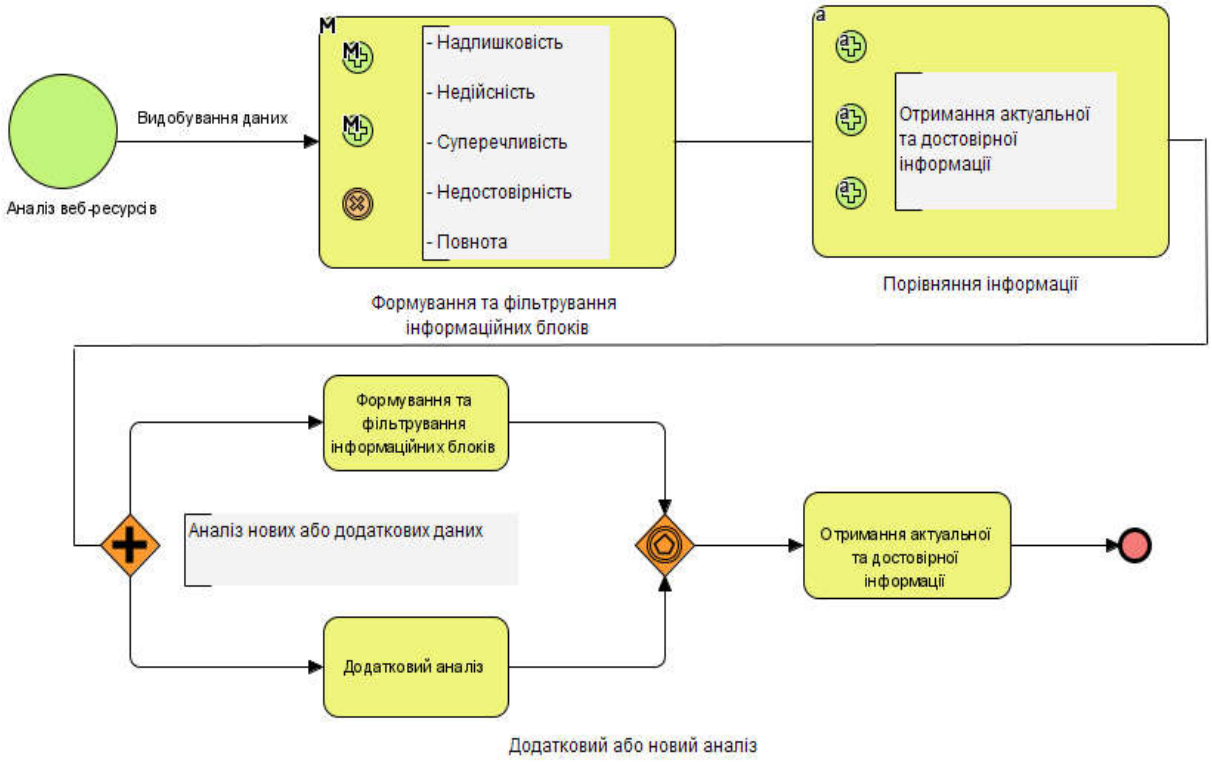

Рис. 1. Схема аналізу інформації з веб-ресурсів із використанням показників оцінки достовірності інформації.

1. Розташування сутності. Тема S, так само як і об'єкт O спочатку повинні відповідати елементу із множини достовірних даних в $BaseAt$, який представляє ту саму сутність.

2. Перевірка відношень. Інформація, яка описується за допомогою (1) вважається актуальною та достовірною, якщо межа позначене предикатом від елемента, що представляє S, до елемента, що представляє O, існує в множині опису зв'язків $Base\mathrm{Re}lation$. В іншому випадку інформація вважається хибною, або такою що потребує додаткових уточнень.

3. Встановлення достовірності інформації. Коли $Kw=\langle S,P,O\rangle$ не входить у множину $Base\mathrm{Re}lation$, ймовірність для меж сутності, яка позначена предикатом в межах певної предметної області можна визначити, використовуючи показник семантичної близькості [5], який дозволяє провести попарну оцінку елементів із множини $\langle S,P,O\rangle$, які знаходяться між собою в семантичних відношеннях (синоніми, гіперо-гіпонімічнівідношення, асоціативність), і нульові значення для всіх інших пар.

Розглянемо специфіку описаного процесу перевірки. Припустимо, що верифікований на офіційному веб-ресурсі інформаційний блок можна представити як формалізований набір тверджень $Kw=\langle s_i,p_i,o_i\rangle, i=1,2,...n$. Множина W_{BaseAt} сформована на основі верифікованих наборів даних $st_j,\ pt_j,\ ot_j,\ j=1,2,...m$.

Перевірка інформаційних блоків, які розміщені на суміжних до досліджуваного веб-ресурсу буде зводитися до побудови функцій Fa із знайденими показниками автентичності $Af_i\in[0;1]$ для кожного блоку $\langle s_i,p_i,o_i\rangle$, попарно їх порівнюючи із $\langle st_j,pt_j,ot_j\rangle$ із врахування опису відношень із $Base\mathrm{Re}lation$:

$$Af_i=1,\ \textit{якщо блок верифікований як достовірний};$$
$$Af_i=0,\ \textit{якщо блок верифікований як недостовірний}.$$

Загальний показник автентичності ресурсу Af буде визначатися як агрегована величина усіх Af:

$$Fa:(s_i,p_i,o_i)\xrightarrow{W_{BaseAt}}Af_i \tag{5}$$

$$Af=O(Af_i),\ \textit{де}\ i=1,..,n, \tag{6}$$

де O – вибрана функція агрегування (наприклад, середньозважена).

Інформація, яку необхідно перевірити, є достовірною при умові $Af=1$, а при $Af=0$ вказана інформація повністю недостовірна:

$$Fa\big((s_i,p_i,o_i),W_{BaseAt}\big)=P\big(\textit{межа}\ p_i,\ \textit{що зв'зує}\ s_i\ \textit{та}\ o_i\ \textit{в}\ W_{BaseAt}\big), \tag{7}$$

де P – ймовірність відповідності s_i,o_i до достовірних даних st_j,ot_j в W_{BaseAt}.

$$s_i=\underset{st_j}{\arg\min}\left[U\left(s_i,st_j\right)\right]<\theta, \tag{8}$$

$$o_i = \underset{ot_j}{\arg\min}\left[U\left(o_i, ot_j\right)\right] < \theta, \qquad (9)$$

де U – відстань між двома елементами відповідних сутностей, яку можна розрахувати за допомогою формули Джакардової відстані[5,12,13]. Величина U буде відображати ідентифікацію двох сутностей між собою, наприклад, якщо $U\left(o_i, o_{i+1}\right) = 0$, то o_i та o_{i+1} ті самі сутності.

У результаті отримаємо множину видобутих даних та множину верифікованих достовірних даних. Однією із основних проблем при побудові множини достовірних даних буде джерело (джерела), з якого ці дані можна отримати. В якості відповідного джерела може використовуватися наперед визначений ресурс, дані з якого носять тільки достовірний характер.

Метод перевірки інформації з веб-ресурсівна основі аналізу даних, отриманих із соціальних мереж.

Виявлення недостовірної інформації, враховуючи особливості її поширення через відповідні сторінки у соціальних мережах, можна реалізовувати, використовуючи методи аналізу структури інформації в процесі їх поширення або дублювання. Виявлення недостовірної інформації на основі її розповсюдження можнасформулювати як задачу багатозадачної класифікації інформації, яка отримується із різних джерел даних. Вхідними даними даного методу поширення може бути впорядкованамножина, елементами якої є інформаційні блоки та відповідні показники їх ідентифікації (час, джерело, профіль).

Таку впорядковану множину можна представити через деревоподібну структуру, яка, враховуючи відповідні показники,фіксує ступінь поширення певної інформації через соціальні мережі. Кореневий елемент такої структури визначає джерело, з якого інформація була взята в початковому вигляді, а інші вузли представляють користувачів, які поширювали інформацію, враховуючи їх взаємозв'язок із батьківським джерелом (наприклад, офіційна сторінка організації в соціальній мережі та сторінки користувачів, які є учасниками відповідної групи або просто «друзями»).

Оцінку достовірності інформації, яка поширюється через відповідні профілі у соціальних мережах, можна здійснювати через врахування показника потужності множини або через їх оцінку через часові характеристики.

На рисунках 2 та 3 наведено ілюстрацію оцінки достовірності інформації, яка отримується через соціальні мережі із використанням зазначених вище методів оцінки.

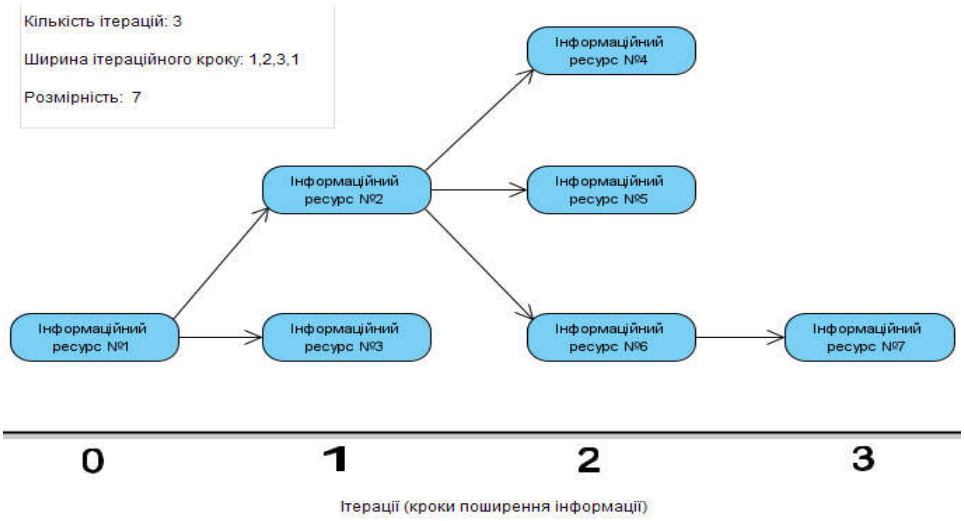

Рис. 2. Оцінка достовірності інформації на основі ітераційної оцінки множин

Основними критеріями, які використовуються при використанні ітераційної оцінки множин, є:

- кількість ітерацій - максимальна кількість ітерації, на яких відбувалося поширення інформаційних блоків;
- ширина ітераційного кроку – кількість джерел інформації в межах ітераційного кроку;
- розмірність – загальна кількість джерел інформації, через які відбувається поширення;

На рисунку 3 відображено ці показники, виходячи із побудованої деревовидної структури.

Основними критеріями, які використовуються в процесі використання часової оцінки, є:

- період існування інформаційного елемента–час, протягом якого інформація поширювалася через відповідні інформаційні джерела;
- режим реального часу – кількість джерел інформації, які поширювали інформацію в певний час;
- кількість джерел поширення інформації – загальна кількість джерел інформації, через які відбувається поширення;

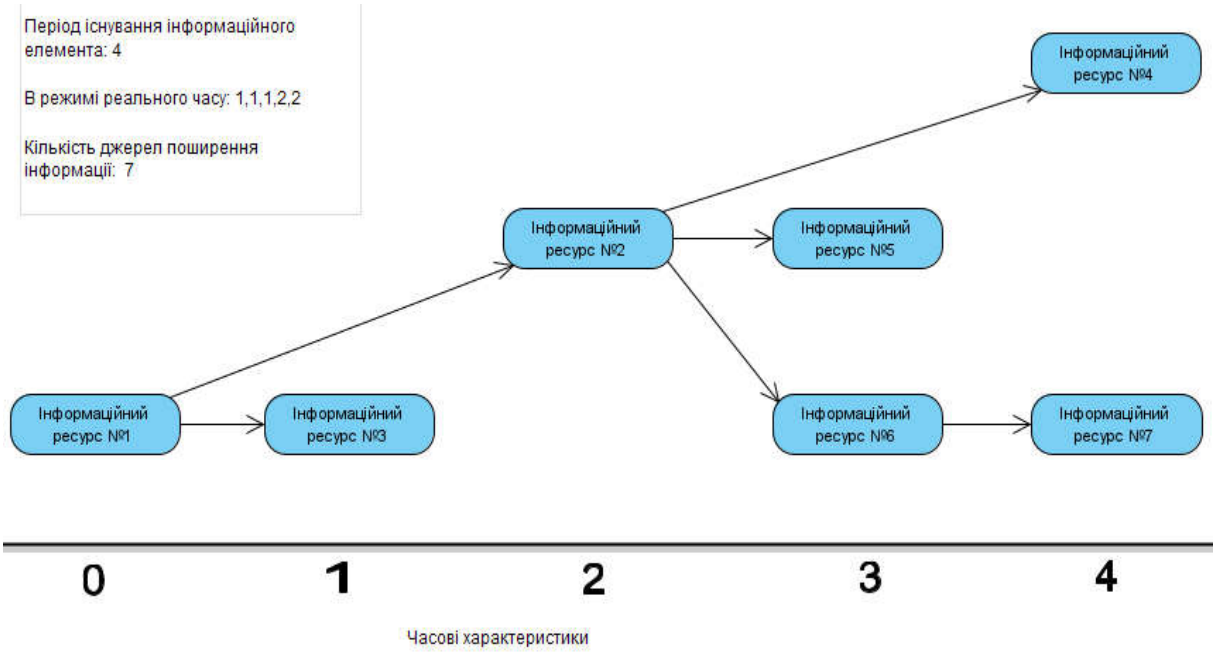

Рис. 3. Оцінка достовірності інформації на основі часової оцінки множин

Складність застосування такого методу визначення достовірної інформації полягає у розширені кількості вузлів на кожному етапі ітерації, наприклад, через велику чисельність активних користувачів, які належать до кореневого вузла. Крім того, часто доводиться фільтрувати додаткові показники, які можуть нарощуватися на кожній ітерації. В загальному випадку достовірність інформації буде визначатися, виходячи із її близькості до кореневого вузла поширення із врахуванням актуальних часових характеристик.

Експериментальні дослідження

На основі запропонованого підходу було проведено ряд експериментальних досліджень. Суть даних досліджень зводилася до оцінки інформації веб-ресурсу класичного університету Тернополя (https://www.wunu.edu.ua/) та відповідних джерел

інформації, які до нього повністю, частково або не прив'язані. На рисунку 4 представлено схему, яка відображає результати оцінки відповідних джерел інформації із врахуванням параметрів на кожному ітераційному кроці.

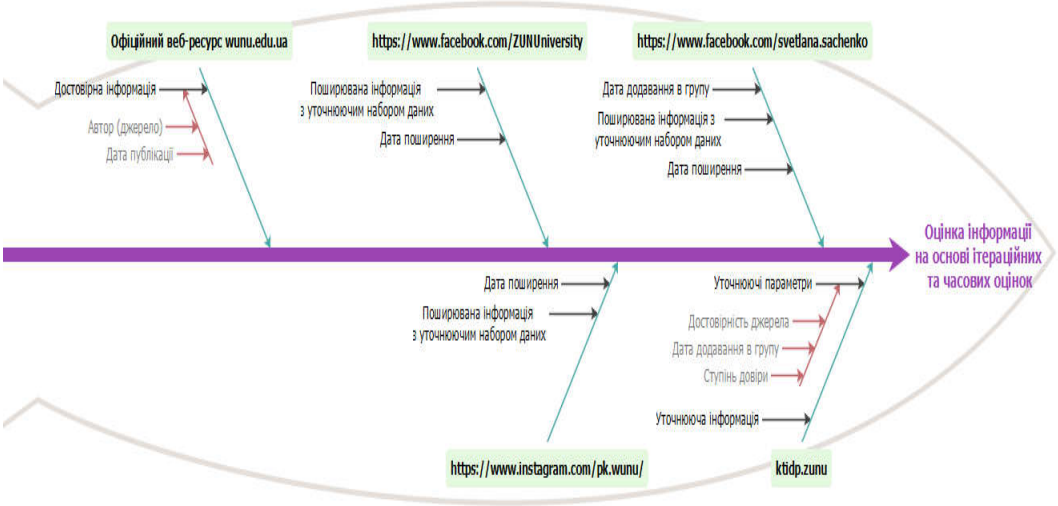

Рис. 4. Оцінка достовірності інформації на основі ітераційних та часових характеристик на прикладі даних, отриманих з ресурсу https://www.wunu.edu.ua/

В результаті експертного оцінювання з елементами використання автоматизованих інструментальних засобів аналізу контенту було підтверджено достовірність інформації, яка відображалася на кожному кроці оцінювання. Відповідні результати наведено у таблиці 1.

Оцінка достовірності здійснювалася на основі агрегованої оцінки кожного інформаційного джерела. В результаті встановлено, що на трьох інформаційних ресурсах, інформація, яка поширюється, може вважатися достовірною, а на двох - частково достовірною.

Таблиця 1.

Результати оцінювання достовірності інформації на основі поширення її через соціальні мережі в рамках структури відношень домена https://www.wunu.edu.ua/

Параметри оцінювання	https://www.wunu.edu.ua/ (достовірне джерело)	https://www.facebook.com/ZUNUniversity	https://www.facebook.com/svetlana.sachenko	https://www.instagram.com/pk.wunu/	ktidp.zunu
Автор	Прес-центр	Прес-центр	Саченко	Приймальна комісія	Кафедра історії держави
Дата публікації (поширення)	20.01.2021	20.01.2021	21.01.2021	21.01.2021	20.01.2021
Достовірність джерела	Достовірне	Достовірне	Частково достовірне	Достовірне	Достовірне
Дата реєстрації джерела в достовірному домені	-	20.09.2020	31.10.2020	21.09.2020	30.09.2020
Ступінь довіри	Високий	Високий	Середній	Високий	Середній
Оцінка достовірності	Достовірна	Достовірна	Частково достовірна	Достовірна	Частково достовірна

Висновки

У роботі розглянуто особливості процесу оцінки інформації на предмет актуальності та достовірності. Відсутність належних підходів, які прості у використанні та реалізації, спонукали до розробки відповідної системи показників та методів оцінки недостовірної та неактуальної інформації. Використання запропонованих в рамках даної роботи методів дозволило підвищити ступінь розпізнавання джерела інформації на предмет розміщення неактуальної та недостовірної інформації (Таблиця 1.)

Створені методи програмно реалізовані як надбудова до існуючих рішень в рамках окремих програмних модулів і можуть ефективно використовуватися для оцінки достовірності інформації. Ефективність запропонованих методів підтверджена експериментально на прикладі оцінки веб-ресурсів закладу вищої освіти - Західноукраїнського національного університету, а також пов'язаних із ним інформаційних ресурсів.

Список літератури

1. Vo N., Lee K. The Rise of Guardians: Fact-checking URL Recommendation to Combat Fake News. *The 41st International ACM SIGIR Conference on Research & Development in Information Retrieval*. 2018, P. 275–284. URL: https://doi.org/10.1145/3209978.3210037
2. Колодчак О.М. Інтелектуальний аналіз даних. *Вісник Національного університету "Львівська політехніка". Комп'ютерні системи та мережі*. 2013. № 773. С. 49-58.
3. Ye J., Skiena S. Media Rank: Computational Ranking of Online News Sources. *Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data MiningJuly*. 2019. P. 2469–2477 URL: https://doi.org/10.1145/3292500.3330709.
4. Yu B., Zhang Z., Tingwen L., Wang B., Li S., Li Q. Beyond Word Attention: Using Segment Attention in Neural Relation Extraction. *IJCAI*. 2019. P. 5401-5407.
5. Chao W. Relation Extraction. *Proceedings of the Twenty-Eighth International Joint Conference on Artificial Intelligence. International Joint Conferences on Artificial Intelligence Organization*, 5401–5407. URL: https://doi.org/10.24963/ijcai.2019/750.
6. Xinyi Z., Reza Z. A Survey of Fake News: Fundamental Theories, Detection Methods, and Opportunities. *ACM Comput. Surv*. V.53, N5, Article 109. 2020, 40 p. DOI: https://doi.org/10.1145/3395046.
7. Ray O., Qian J., Wang W.Y. A Survey on Natural Language Processing for Fake News Detection. *ArXiv* abs/1811.00770 (2020): n. pag.
8. Dyvak M., Papa O., Melnyk A., Pukas A., Porplytsya N., Rot A. Interval Model of the Efficiency of the Functioning of Information Web Resources for Services on Ecological Expertise. *Mathematics,* 2020. V. 8 No. 12, 2116. URL: https://doi.org/10.3390/math8122116.
9. Nørregaard J., Horne B.D., Adalı S. A Large Multi-Labelled News Dataset for the Study of Misinformation in News Articles. *Proceedings of the International AAAI Conference on Web and Social Media*, 2018. V. 13., P. 630–638.
10. Trivedi R., Sisman B., Dong, X., Faloutsos C., Ma J., Zha H., Link N. Bed: Multi-Graph Representation Learning with Entity Linkage. 2018. P. 252-262. URL: doi10.18653/v1/P18-1024.

11. Vilone G., Longo L. Explainable Artificial Intelligence: a Systematic Review. 2020.
12. Kovbasistyi A., Melnyk A., Dyvak Brych V., Spivak I. Method for detection of non-relevant and wrong information M. based on content analysis of web resources. *XIII International Conference on Per-spective Technologies and Methods in MEMS Design (MEMSTECH)*. Lviv, 2017, P. 154-156, URL: doi: 10.1109/MEMSTECH.2017.7937555.
13. Dyvak M.P., Kovbasistyi A.V., Melnyk A.M., Turchyn L.Y., Martsenyuk Y.O. System for web resources content structuring and recognizing with the machine learning elements. *Radio Electronics, Computer Science, Control*, 2018. N 3. https://doi.org/10.15588/1607-3274-2018-3-14.
14. Дивак М.П., Мельник А.М., Ковбасістий А.В., Папа О.А. Підхід до математичного моделювання ефективності web-ресурсів. *Оптико-електронні інформаційно-енергетичні технології.* 2020. Т. 38, N. 2. P. 29–37. URL: https://doi.org/10.31649/1681-7893-2019-38-2-29-37.

METHODS AND TOOLS OF DETECTING CURRENT AND RELIABLE INFORMATION ON WEB-RESOURCES

A.M. Melnyk

West Ukrainian National University,
11, Lvivska Str., Ternopil, 46020, Ukraine; melnyk.andriy@gmail.com

The article considers an important scientific and applied task of identifying irrelevant and unreliable information on web resources, which is an important area of development and implementation of methods of data mining. The analysis of modern methods and means of estimation of irrelevant and unreliable information from the point of view of estimation of information sources is carried out and the basic problem directions which arise in the course of their functioning are allocated.

A system of indicators for filtering unreliable and irrelevant information, which is obtained on the basis of several sources, is proposed. Based on this system, a method of checking information from web resources for relevance and reliability has been implemented. This approach is based on the possibility of using a predefined resource, the data from which are only reliable.

A method of detecting inaccurate and irrelevant information has been developed, taking into account the peculiarities of its distribution through relevant pages in social networks and the use of multitasking classification of information obtained from various data sources.

The use of the proposed intelligent data processing methods together with other methods of intellectual analysis used to evaluate information obtained from the Internet, will significantly increase the efficiency of the process of establishing irrelevance and inaccuracy of information, and will build an assessment of a particular web resource for publishing and disseminating such information.

Keywords: relevance and reliability of information, web-resource, information source, social networks.

DOI 10.15276/imms.v10.no 3-4.177
УДК 004.056.53:005.004.7

Informatics and Mathematical Methods in Simulation
Vol. 10 (2020), No. 3-4, pp. 177-189

ВИЯВЛЕННЯ КІБЕРАТАК В ІНФОРМАЦІЙНИХ МЕРЕЖАХ

І.Р. Опірський[1], Ю.М. Ткач[2], В.О. Хорошко[3]

[1]Національний університет «Львівська політехніка», м. Львів, 79013, вул. С. Бандери, 12, Україна;
e-mail: iopirsky@gmail.com
[2]Національний університет «Чернігівська політехніка», м. Чернігів, 14035, вул. .Шевченка, 95, Україна;
e-mail: tkach_ym@ukr.net
[3]Національний авіаційний університет, 03058, м. Київ, просп. Любомира Гузара,1, Україна;
e-mail: professor_va@ukr.net

Усе більшого значення в забезпеченні національної безпеки різних держав світу набуває кібернетична безпека. Кібернетичні атаки та кібернетичні впливи все частіше стають одними з головних дій для досягнення мети контролю над різними об'єктами, такими як людина, організація, регіон, держава тощо в сучасному світі. Таким чином, у світі з'явилось нове явище у міжнародній політиці, а саме можливість досягненню власних політичних цілей, економічного та духовного підпорядкування народів інших держав без застосування військової сили, а лише з допомогою інформаційного впливу. Тому в світі доволі активно розвиваються кібернетичні атаки та кібернетичні впливи. В наслідок цього для ефективної роботи сучасних інформаційно-телекомунікаційних мереж та засобів їх захисту, а також для надійного виявлення та передбачення кібернетичних атак та несанкціонованих дій необхідно розвивати нові підходи та методи кібернетичної безпеки. Метою статті є виявлення кібернетичних атак в інформаційно-телекомунікаційних мережах. Зокрема, розглянуто задачу виявлення кібернетичної атаки на фоні білого гаусівського шуму за умови неперервного часу спостереження. Наведено теоретичне обґрунтування усередненого об'єкту прогнозування. При послідовному аналізі усередненого об'єкту прогнозування в загальному випадку з'ясовано, що він не дає достатню статистику в задачі послідовного виявлення кібератак. З вищесказаного слідує, що одним з головних питань при синтезі оптимальних послідовних і непослідовних кібератак з випадковими моментами появи є розробка алгоритмів формування усередненого об'єкту прогнозування. У результаті проведених досліджень запропоновано методику виявлення несанкціонованого доступу з невідомим моментом виникнення в дискретному часі спостереження.

Ключові слова: інформаційні системи, кібератака, усереднений об'єкт прогнозу.

Вступ

Поступовий перехід в розвитку людства від «інформаційного суспільства» та «високотехнічного» обумовлено еволюційним підходом до забезпечення безпеки в нових умовах на різних рівнях. Відбувається поступова трансформація концепції інформаційної громадянина, суспільства та держави до необхідності її поповнення новою концепцією кібернетичної безпекою. При цьому має місце процес розмежування різних видів безпеки за геополітичними рівнями та розумінням ролі кібернетичної безпеки на кожному з них. Необхідність розуміння ролі кібернетичної безпеки пов'язана в першу чергу з активізацією міжнародних терористичних, екстремістських організацій та злочинних угрупувань, а також окремих держав, котрі здійснюють кібератаки та кібервплив на громадян, суспільство, державу з метою реалізації власних інтересів [1, 2, 3].

Все більшого значення в забезпеченні національної безпеки різних держав набуває кіберпезпека. Кібератаки та кібервпливи все частіше стають одними з головних дій для досягнення мети контролю над різними об'єктами (людиною, організацією, регіоном, державою тощо) в сучасному світі [4]. Фактично виникло нове явище у

міжнародній політиці – можливість досягненню власних політичних цілей, економічного та духовного підпорядкування народів інших держав без застосування військової сили. Тому в світі доволі активно розвиваються кібератаки та кібервпливи.

При цьому, в умовах введення гібридних війн, протягом останніх років систематично відбуваються успішні кібератаки, кібердії та несанкціоновані дії терористів й зловмисників в інформаційно-комунікаційних мережах, що підриває оборону, економіку, військову та науково-технічну сфери не тільки держава, але й окремих галузей та підприємств.

Тому для ефективної роботи сучасних інформаційно-телекомунікаційних мереж та засобів їх захисту, а також для надійного виявлення та передбачення кібератак та несанкціонованих дій необхідно розвивати нові підходи та методи кібербезпеки. Слід відмітити, що математичний апарат, який застосовується, а також відомі методи та засоби захисту інформації в кібернетичному просторі та інформаційно-телекомунікаційних мережах з точки зору протидії зловмисникам, не забезпечують можливості прогнозуванню та виявленню кібератак для відповідного реагування на загрози інформації, але підхід в ранньому виявленні кібератаки в будь-який момент часу є досить актуальним.

Мета статті

Метою статті є виявлення кібератак в інформаційних мережах.

Основна частина

У [5,6,7] питання виявлення НСД з невідомим моментом виникнення розглядались в дискретному часі спостереження, проте ми розглядаємо задачу виявлення кібератаки $A(t)$ на фоні білого гаусівського шуму $V(t)$ інтенсивністю $N\left[MV(t)\right]=0$, $MV(t)V(a)=N\theta(1-a)$ за умови неперервного часу спостереження. Більш точно, припускаємо, що спостереженню притаманний випадковий процес виду:

$$X(t)=\theta I(t-\lambda_0)A(t)+V(t),\ t\geq 0, \tag{1}$$

де θ– параметр, який приймає значення 0 та 1 з ймовірностями $\pi_0=P(\theta=0)$ та $1-\pi_0=P(\theta=1)$; λ_0 – випадковий момент появи кібератаки $A(t)$, що являє собою в загальному випадку випадковий процес; $I(y)$ – індикаторна функція, яка дорівнює 1 при $y\geq 0$ та 0 в протилежному випадку. Будемо також вважати, що відомий апріорний розподіл $\Pi(\lambda)=P\left(\lambda_0\leq\lambda\middle|\theta=1\right)$ величини λ_0.

У подальшому для коректного використання математичного апарату перейдемо до моделі, яка еквівалентна (1) з інформаційної точки зору, припускаючи, що спостерігається процес $y(t)$ зі стохастичним диференціалом [8].

$$dy(t)=\theta I(t-\lambda_0)A(t)dt+\sqrt{N}dw(t), t\geq 0, \tag{2}$$

при $w(t)$ – стандартний вінеровський процес.

Нехай P_0 та $P_{1\lambda}$ - ймовірнісні міри, які виникли внаслідок $y(t)$ при $\theta = 0$ та $\theta = 1$, $\lambda_0 = \lambda$ відповідно; $\gamma_\lambda(t) = \frac{dP1\lambda}{dP0}(y^t)$ – область прогнозу (ОП) гіпотези $H_{1\lambda}$; $\theta = 1, \lambda_0 = \lambda$ і H_0, $\theta = 0$; $\Lambda(t) = \int_0^\infty \gamma_\lambda(t) d\Pi(\lambda)$ - усереднений об'єкт прогнозу (УОП) $\left(y^t = \{y(u), u \le t\}\right)$.

Якщо процес (2) спостерігається на інтервалі [0,T] фіксованої тривалості T, а функція втрат має вигляд відповідно до [8,9]

$$g(\theta, \lambda, \mathrm{n}, u_n) = \begin{cases} g_{01}(n),\ \theta = 0,\ u_n = 1, \\ g_{11}(n) + C\left(n - [\lambda]\right),\ \ \theta = 1,\ \ \lambda < \mathrm{n}\Delta, u_n = 1, \\ g_{11}(n), \theta = 1, \lambda \ge \mathrm{n}\Delta, u_n = 1, \mathrm{n} = \overline{1, N}. \end{cases}$$

де $u_n = 1$ – розв'язок про наявність збою на n-му кроці;
C- вартість затримки прийняття рішення про наявність збою на один крок; $[\lambda] = \mathrm{n} - 1$ *при* $(n-1)\Delta \le \lambda < n\Delta$.

Розв'язок $u_n = 0$ про відсутність збою на кроках $n = 1$, $N - 1$ ототожнюється з рішенням u_n про продовження спостережень, оскільки при подальшому спостереженні збій може виникнути та бути виявленим. На N-му кроці спостереження призупиняються з вірогідністю 1 та поряд з втратами, наведені в попередньому виразі, виникають втрати [10], які пов'язані з прийняттям рішенням $u_N = 0$:

$$g(\theta, \lambda, u_n, N) = \begin{cases} g_{00}(N),\ \theta = 0,\ u_N = 0; \\ g_{10}(N) + C\left(N - [\lambda]\right),\ \ \theta = 1,\ \ \lambda < N\Delta, u_N = 0; \\ \tilde{g}_{10}(N), \theta = 1, \lambda \ge \mathrm{N}\Delta, u_N = 0. \end{cases}$$

У цих виразах значення $g_{i1}(n)$, $g_{i0}(N), \tilde{g}_{1j}(n)$ не залежать від λ, причому $g_{11}(n) < \tilde{g}_{11}(n) \le g_{01}(n), g_{00}(N) \le g_{10}(N) \le g_{10}(N)$. Їх залежність від номеру етапу може бути обумовлена, наприклад, вартістю спостережень. Однак, в багатьох задачах покладають, що $\tilde{g}_{11}(n) = g_{01}(n)$ та $\tilde{g}_{10}(N) = g_{00}(N)$. При цьому $N\Delta = T, C\left(N - [\lambda]\right) = C(T - \lambda)$, то оптимальне байєсове непослідовне правило має вигляд:

$$u_t^0 \Lambda(T) = \begin{cases} 1, \Lambda(T) \ge H \\ 0, \Lambda(T) < H \end{cases}. \tag{3}$$

Правило (3) оптимально також в умовах екстремальній задачі, коли потрібно мінімізувати середню ймовірність пропуску при заданій ймовірності хибної тривоги α_0 (*при цьому* $H = H(\alpha_0)$ є рішенням рівняння $P_0\left[\Lambda(T) \ge \mathrm{H}(\alpha_0) = \alpha_0\right]$.

При послідовному аналізі усередненого об'єкту прогнозування (УОП) в загальному випадку не являє собою достатню статистику та в задачі послідовного виявлення [11].

З вищесказаного слідує, що одним з головних питань при синтезі оптимальних послідовних і непослідовних виявлювачів кібератак з випадковими моментами появи є знаходження алгоритмів формування УОП. Для моделі (1) ця задача детально розглянута в [12], це показано, що $\Lambda(t)$ задовольняє стохастичне рівняння:

$$d\Lambda(T) = N^{-1}[\int_0^t m_\lambda(t)\gamma_\lambda(t)d\Pi(\lambda)]dy(t), \mathrm{t} > 0, \Lambda(0) = 1 \tag{4}$$

У виразі (4) $m_\lambda(t) = M_{1\lambda}[I(t-\lambda)A(t)|y^t]$ – апостеріорне математичне сподівання, що є оптимальним в середньоквадратичному змісті фільтраційної оцінки кібератаки $A(t)$ при $\mathrm{t} \geq \lambda$ у відомому $\lambda_0 = \lambda[m_\lambda(\mathrm{t}) = 0$ при $t < \lambda; M_{1\lambda}$ – сподівання, що відповідає мірі $P_{1\lambda}]$. При цьому $\gamma_\lambda(t)$ задовольняє рівняння:

$$d\gamma_\lambda(t) = N^{-1}\gamma_\lambda(t)m_\lambda(\mathrm{t})\mathrm{dy}(\mathrm{t}); t > 0, \gamma_\lambda(0) = 1 \tag{5}$$

розв'язок якого має вигляд:

$$\gamma_\lambda(t) = \exp[N^{-1}\int_0^t m_\lambda(u)dy(u) - (2N)^{-1}\int_0^t m_\lambda^2(u)du] \tag{6}$$

де $\gamma_\lambda(t) = 1$ при $\lambda > t$.

З рівнянь (4) - (6) слідує, що в загальному випадку, коли кібератака $A(t)$ довільна, алгоритм формування УОП потребує усереднення величини $m_\lambda(\mathrm{t})$ $\gamma_\lambda(t)$ за множиною значень λ, причому знаходження функціоналу $m_\lambda(\mathrm{t})$, в цілому наштовхується на великі труднощі. Якщо $A(t), t \geq 0$, - Гаусівській процес, то $m_\lambda(\mathrm{t})$ задається лінійним функціоналом виду:

$$m_\lambda(t) = \begin{cases} \int_0^1 \mathrm{H}(t,u), d\mathrm{y}(u), \lambda \leq \mathrm{t} \\ 0, \lambda > t \end{cases}.$$

де $\mathrm{H}(t,u)$ - імпульсна характеристика фільтру, знайдена з рівняння Вінера-Хопфа.

Задача суттєво спрощується, якщо кібератака $A(t)$ є детермінованою функцією. Тоді

$$m_\lambda(t) = \begin{cases} \mathrm{A}(t),\ \lambda \leq \mathrm{t} \\ 0, \lambda > t \end{cases},$$

і, як слідує з (4) та (6), УОП задовольняє рівняння:

$$d\Lambda(\mathrm{t}) = N^{-1}A(t)\left[\Lambda(\mathrm{t}) - S_t\right]dy(t), \quad t > 0, \Lambda(0) = 1 \tag{7}$$

де $S_t = 1 - \Pi(t)$. З (2) та (7) слідує, що процеси $\{\Lambda(\mathrm{t}), F_t^y, Pi\}$, $t \geq 0$, $\mathrm{i} = 0,1$, є неоднорідними марківськими процесами. Це дозволяє довести, що в задачі

послідовного виявлення квазідетермінованої атаки з невідомим моментом появи [13] при відомих функціях втрат оптимальне послідовне правило має такий вигляд :

$$u_t^0\left[\Lambda(\mathrm{t})\right]=\begin{cases}1, & \Lambda(\mathrm{t})\geq B(t),\\ 0, & \Lambda(\mathrm{t})<B(t), \mathrm{t}\geq 0\end{cases},$$

де $B(t)$ - поріг, який є детермінованою функцією часу ($u_t^0=0$ еквівалентно продовженню спостережень).

У випадку детермінованої атаки $A(t)$ вдається знайти також рівняння для оптимальної оцінки моменту появи λ_0 по відношенню до квадратичної функції втрат. Позначимо через $\mu_n(t)=M_1\left(\lambda_0^n|y^t\right)$, $n\geq 1$, n-й апостеріорний момент величини $\lambda_0(\mathrm{M}_1\left(\bullet|y^t\right)$ – сподівання за умовною мірою

$$|P_1(S\,|\,y^t=P(\lambda_0\in \mathrm{S}\,|\,\theta=1,\ y^t)).$$

Використовуємо формулу Байєса отримуємо:

$$\mu_n(t)=\frac{\varphi_n(t)}{\Lambda(\mathrm{t})}, \tag{8}$$

де $\varphi_n(t)=\int_0^\infty \lambda^n\gamma_\lambda(t)\,d\Pi(\lambda)$.

Введемо нормовану статистику

$$\overline{\varphi}_n(t)=\frac{\varphi_n(t)}{\beta_n(0)},$$

де $\beta_n(t)=\int_t^\infty \lambda^n d\Pi(\lambda)$.

Статистика $\varphi_n(t)$, очевидно, що може бути записана у вигляді:

$$\overline{\varphi}_n(t)=\int_0^\infty \gamma_\lambda(t)\,dP_n(\lambda), \tag{9}$$

де $P_n(\lambda)=\frac{1}{\beta_n(0)}\int_0^\lambda y^n d\Pi(y)$ - нормована до одиниці міри.

До статистики (9) при виконанні умови:

$$\int_0^t |A(u)|^2\,du<\infty, t<\infty \tag{10}$$

застосовні всі розмірковування [12], які привели до диференційного рівняння (7) для статистичних $\Lambda(\mathrm{t})$, якщо розподіл $\Pi(\lambda)$ замінити на розподіл $P_n(\lambda)$, то для $\overline{\varphi}_n(t)$ справджується вираз:

$$d\overline{\varphi}_{\mathrm{n}}(t) = N^{-1}A(t)\left[\overline{\varphi}_{\mathrm{n}}(t) - \int_0^{\infty} dP_n(\lambda)\right]dy(t), \quad t > 0,\ \overline{\varphi}_{\mathrm{n}}(0) = 1.$$

Звідси слідує, що при виконанні умови (10) та при $\beta_n(0) < \infty$, статистика $\varphi_{\mathrm{n}}(t)$ задовольняє стохастичне диференціальне рівняння:

$$\begin{gathered} d\varphi_{\mathrm{n}}(t) = N^{-1}A(t)\left[\varphi_{\mathrm{n}}(t) - \int_0^{\infty} \lambda^n d\Pi(\lambda)\right]dy(t), \quad t > 0, \\ \varphi_{\mathrm{n}}(0) = \int_0^{\infty} \lambda^n d\Pi(\lambda) \end{gathered} \tag{11}$$

Таким чином, n-й апостеріорний момент величини λ_0 визначається за допомогою співвідношень (7), (8) та (11). В частинному випадку, при виконанні умови:

$$\int_0^{\infty} \lambda^n d\Pi(\lambda) < \infty, \int_0^{\infty} \lambda^2 d\Pi(\lambda) < \infty,$$

оптимальною оцінкою моменту появи кібератак є апостеріорне середнє $\mu_1(t)$, яке знаходиться за допомогою (8) та (11) при $n = 1$.

Розглянемо тепер випадок, коли атака з'являється з ймовірністю одиниці, π_0 =0. При цьому, з одиничною ймовірністю $\theta = 1$ в (1) та (2) та $\gamma_\lambda(t) = \frac{dP_\lambda}{dP_\infty}(y^t)$, де $P_\lambda(\bullet) = P(\bullet | \lambda_0 = \lambda)$ – міра, що відповідає процесу (2) при $\lambda_0 = \lambda(\theta = 1), P_\infty = P_\lambda$ при $\lambda = \infty$ (вінеровська міра).

Задача виявлення атаки в цьому випадку відрізняється від традиційної, тієї що розглянута раніше. У байєсовській постановці її слід трактувати як задачу оцінки моменту появи кібератаки, при втратах, рівних φ_0 *при* $\lambda \le t$ та $\mathrm{C}(\mathrm{t} - \lambda)$ *при* $\mathrm{t} > \lambda$, де φ_0 - втрата при хибній тривозі; С- вартість затримки в виявленні кібератаки в одиницю часу.

Якщо задано обмеження на ймовірність хибної тривоги, тобто розглядається клас правил виявлення $\Delta(\alpha)$, таких що $P[\tau(u) < \lambda_0] \le \alpha$ (де Р- міра, що відповідає $(y(t) < \lambda_0)$, $t \ge 0$; $\tau(u)$- момент зупинки, який відповідає правилу $u(x)$, то задачу виявлення кібератак з випадковим моментом появи природньо трактувати як задачу якнайшвидшого виявлення збою процесу, що спостерігається, в класі $\Delta(\alpha)$. Іншими словами, бажано знайти таке послідовне правило $u^0(x)$, яке мінімізує $\mathrm{M}(\tau(\mathrm{u}) - \lambda_0 \mid \tau(\mathrm{u}) \ge \lambda_0)$ в класі $\Delta(\alpha)$.

Розглянемо правило

$$u_t^0 = [\pi(t)] = \begin{cases} 1, \pi(t) \ge B \\ 0, \pi(t) < B, t \le 0 \end{cases} \tag{12}$$

де $\pi(t) = \mathrm{P}(\lambda_0 \le \mathrm{t} | \mathrm{y}^{\mathrm{t}})$ – апостеріорна ймовірність появи атаки (збою) в момент t; B - деяка константа. Тривалість правила (12) визначається співвідношенням:

$$\tau_0 = inf\{t \ge 0 : \pi(t) = B\} \tag{13}$$

Відмітимо, що $P(\tau_0 < \lambda_0) = \mathrm{M}\left[1 - \pi\left(\tau_0\right)\right]$ з (13) отримуємо $\mathrm{B} = 1 - \mathrm{P}(\tau_0 < \lambda_0)$. Тому при виборі порогу за формулою:

$$B = 1 - \alpha \tag{14}$$

забезпечуємо $P(\tau_0 < \lambda_0) = \alpha$ та, відповідно, приналежність правила (12) та (14) до шляху $\Delta\left(\alpha\right)$.

Очевидно, статистика буде:

$$\pi\left(t\right) = \frac{\left(\Lambda\left(t\right) - S_t\right)}{\Lambda\left(t\right)}. \tag{15}$$

Нехай S_t, $\Pi'\left(t\right) = d\Pi\left(t\right)/dt$ – неперервна функція. Тоді, застосовуючи до функції (15) формулу Винера-Хопфа с урахуванням (7) отримуємо, що $\pi\left(t\right)$ має стохастичний диференціал

$$\mathrm{d}\pi\left(\mathrm{t}\right) = \beta\left(t\right)(1 - \pi\left(\mathrm{t}\right)\mathrm{dt} + N^{-1}A\left(t\right)\pi\left(\mathrm{t}\right)(1 - \pi\left(\mathrm{t}\right)\left(\mathrm{dy}\left(\mathrm{t}\right) - \mathrm{A}\left(\mathrm{t}\right)\pi\left(\mathrm{t}\right)\mathrm{dt}\right),$$
$$\mathrm{t} > 0, \pi\left(0\right) = \Pi\left(0\right),\ \partial e \beta\left(t\right) = \frac{\Pi'\left(t\right)}{S_t}. \tag{16}$$

Рівняння (16) узагальнює рівняння (4.149) [9] на випадок довільної детермінованої функції $A\left(t\right)$ і довільного неперервного розподілу моменту виявлення кібератаки.

В частинному випадку, при постійній атаці $A\left(t\right) = A, \mathrm{t} > 0$ показовому розподілі $\lambda_0\left(\Pi\left(\lambda\right) = 1 - \exp\left(-\beta\lambda\right)\right)$, тоді $\beta\left(\mathrm{t}\right) = \beta,\ \mathrm{t} > 0,$ рівняння (16) співпадає з (4.149) з [9].

При цьому $\left\{\pi\left(t\right), t \geq 0\right\}$ задається однорідним марковським процесом та правило (12), (14) строго оптимальні в класі $\Delta\left(u\right)$[14].

У більш загальному випадку, коли $A\left(t\right)$ змінюється з часом і розподіл $\Pi\left(\lambda\right)$ не є показовим, правила (12, 14) не оптимальні в класі $\Delta\left(\alpha\right)$. Якщо асимптотично при $\beta \to 0$ вимоги показовості не грає суттєвої ролі, то вимога сталості $A\left(t\right)$ при $t > 0$ виявляється доволі обмеженою з практичної точки зору.

За аналогією з [5] побудуємо модифікацію правила (12), котра оптимальна без введення апріорного розподілу моменту збою. Нехай $\lambda \in \left[0,\ \infty\right]$ – невідомий момент збою, про властивості якого не робиться ніяких апріорних припущень. Будемо вважати, що в (2) $A\left(t\right) = 0$ при $t \geq 0,$ тобто задача полягає у виявлені зміни постійного коефіцієнту зносу винеровського процесу. Введемо наступні позначення: M_λ – математичне сподівання по мірі R_λ, яка відповідає процесу (2) при $\lambda_0 = \lambda(P_\infty$ – вінеровська міра, що відповідає (2) при відсутності збою; ΔT - клас послідовних правил $u\left(x\right)$, таких що $M_\infty \tau\left(u\right) \geq T,\ T \in \left[0, \infty\right];\ \tau_\lambda\left(u\right) = M_\lambda(\tau\left(\mathrm{u}\right) - \lambda \mid \tau\left(\mathrm{u}\right) \geq \lambda)$ - середній час запізнення у виявленні збою при умові, що збій відбувся в момент λ. Бажано забезпечити $\overline{\tau}_\lambda$ як можна менше в класі $\Delta\left(T\right)$, тобто серед правил, в яких середній час до хибної тривоги не менше заданої величини T. Оскільки правила, що

мінімізує τ_λ при всіх $\lambda \geq 0$, не існує, природньо спробуємо знайти мінімаксне правило, яке забезпечує мінімум $\mathrm{E}(\mathrm{u}) = \sup \tau_\lambda(u)$ *в класі* $\Delta(T)$. Перейдемо в (12) від статистики $\pi(t)$ до статистики $\varphi(t) = \dfrac{\pi(t)}{\left[1-\pi(t)\right]}$.

Якщо в якості апріорного розподілу виступає показникове, то нескладно переконатись:

$$\varphi(t) = \beta \int_0^t \gamma_\lambda(t) \exp(-\beta(\lambda - t) d\lambda \tag{17}$$

Позначаючи $L(t) = \dfrac{\varphi(t)}{\beta}$, при $\beta \to 0$ з (17) отримаємо:

$$L(t) = \int_0^t \gamma_\lambda(t) d\lambda = \int_0^t \exp\left\{\frac{a}{N}(y(t) - y(\lambda)\right\} - \frac{a^2}{2N}(t-\lambda) \tag{18}$$

При цьому правило (12) еквівалентно правилу:

$$u_t^0\left(L(t)\right) = \begin{Bmatrix} 1,\ L(t) \geq b \\ 0, L(t) < b, t \geq 0 \end{Bmatrix} \tag{19}$$

де $b = \lim\limits_{\beta \to 0} \dfrac{B}{(1-B)\beta}$

Таки чином , якщо $B \to 0$, $\beta \to 0$ так , що $b = const$, то (19) є границею байєсовського правила (12). В інтерпретації [5], придатної для задач контролю систем, це означає, що періодично, але дуже зрідка виникають збої, ймовірність хибної тривоги наближається до 1 (див. 14). Отже $\dfrac{(1-\alpha)}{\beta} = b < \infty$, причому після оголошення наявності збою відбувається перевірка її справжнього стану та процес відновлюється [10]. Позначимо через $\bar{E}(\alpha, \beta) = M(\tau_0 - \lambda_0 \mid \tau_0 \geq \lambda_0)$ середнє запізнення у виявленні виявлення кібератаки в правилах (12), (14) (M - сподівання за мірою P, породженою вектором $\left[y(t), \lambda_0\right]$. З наведених суджень слідує, що при $\alpha \to 1$, $\beta \to 0$ значення $\bar{E}(\alpha, \beta)$ співпадає з середнім значенням з правила (19) і, як показано в [5], при $b \to \infty$ визначається рівністю

$$\bar{E}(b) = \frac{1}{q}\left\{\ln(qb) - 1 - Э + G\left(\frac{1}{qb}\right)\right\}, \tag{20}$$

де $\mathrm{q} = a^2 / 2N; Э = 0.577$ константа Ейлера, G – коефіцієнт, що характеризує складність задачі, яка розв'язується. Будемо вважати, що b в (19) обирається виходячи із заданого допустимого часу за хибною тривогою T. При цьому процес спостереження може відновитись після прийняття рішення про наявність збою або його відсутності в залежності від конкретної розв'язуваної задачі, що розв'язується.

Оскільки $\gamma_\lambda(t)$ являться мартингалом для $t \geq \lambda$, то процес $L(t)-t,\ t \geq 0,$ також є мартингалом з нульовим середнім (відносно міри P_∞) й, зрозуміло, для будь-якого обмеженого марківського моменту $M_\infty L(\tau) = M_\infty \tau$. Так як, крім того, для моменту зупинки:

$$\tau_0 = inf\left\{t : L(t) = b\right\} \tag{21}$$

справджується рівність $L(\tau_0) = b$, $mo\, M_\infty \tau_0 = b.$ Таким чином, при виборі

$$b = T \tag{22}$$

забезпечується рівність $M_\infty \tau_0 = T$ і тому правило (19), (22) належать до класу $\Delta(T)$.

Детальний аналіз правила (19) та (22), а також його порівняння з правилом Пейджа, яке засноване на порівнянні статистики

$$\tilde{L}(t) = \frac{a}{N}\left\{y(t) - \frac{a}{2N}t - \min_{\lambda \leq t}\left[y(\lambda) - \frac{a}{2N}\lambda\right]\right\}$$

З порогом b_t, визначеним для забезпечення $M_\infty \tau = T$ (r – момент зупинки, що відповідає цьому правилу) з рівняння $\frac{1}{2}qT = \exp(b_t) - b_t - 1$, наведені в [15]. Використовуючи результати цієї роботи можна показати, що для $E(u^0) = \sup_{\lambda \geq 0} \tau_\lambda(u^0)$ правила (19) та (22) справджується рівність:

$$E(u^0) = q^{-1}\left\{\ln(qT) - Э + G\left(\frac{\ln(qT)}{qT}\right)\right\}\ T \to \infty, \tag{23}$$

Більш того, в [15] отримані асимптотичні рівності для τ_λ правила Ширяєва (19) та (22), та правила Пейджа у випадку, коли зміни коефіцієнта зсуву процесу відбувається на величину μ, оj відрізняється від a, на яку «налаштовані» ці правила. Аналіз показує, що при $\mu = a$ середнє затримки у виявленні збою у вказаних правилах практично однакові, при $\mu > a$ правило Пейджа дещо краще, а при $\mu < a$ виграє правило Ширяєва. Якщо використовувати розклад для середньої затримки виявлення для правила, заснованого на порівнянні статистики, що отримується усередненням $L(t)$ за деякою мірою на множині значень a, яке пристосоване для випадку невідомого значення a, то аналіз виявив, що останнє правило є асимптотично оптимальним за першим порядком, в той час як правила Пейджера та Ширяєва все не є актуальними при збільшенні a.

Порівняння (23) та (20) свідчить про те, що головні члени асимпотичних розкладів для середньої затримки $\bar{E}(u^o)$ та максимальної затримки $\bar{E}(u^o)$ співпадають. Це дає підстави покладати, що правило Ширяєва (19) та (22) є асимтотичномінімаксним (у сенсі першого порядку) при $T \to \infty$ в класі $\Delta(T)$, хоча і не є строго мінімаксним в цьому класі. Останнє витікає з тих же міркувань, що й для дискретного часу [13].

Можна «відредагувати» статистику $L(t)$ шляхом рандомізації в момент $t=0$ так, щоб правило (19) опинилося мінімаксним при всіх $T>0$.

Статистика (18), як нескладно показати, за допомогою формули Винера-Хопфа, має стохастичний диференціал:

$$dL(t)=dt+L(t)\frac{a}{N}dy(t),\ L(0)=0 \tag{24}$$

Введемо статистику $L^*(t)$, яка задовольняє стохастичному рівняння (24) з початковою умовою $L^*(0)=z\in[0,bt]$, де z – випадкова величина з розподілом $(y)=P(z\le y)$, зосередженим на інтервалі $[0,b_m]$, таким, що розподіл $P_\infty\left(L^*(t)\le y\middle|\tau^*\right\rangle t)$ не залежить від t. Тут $t^*=inf\left\{t:L^*(t)=b_t\right\}$ - момент зупинки, який відповідає правилу $u^*(x)$, що співпадає з правилом (19) при заміні $L(t)$ на $L^*(t)$. Тоді $\overline{\tau_\lambda^*}(y)=M_\lambda(\ \tau^*-\lambda)r^*>\lambda,\ L^*(\lambda)=y)$ *не* залежить від λ, так як на множині $\left\{\tau^*>\lambda\right\}$ для будь – якого $\lambda\ge 0$ умови однакові, якщо фіксується $L^*(\lambda)$. Тому середній час запізнення можна записати так: $\overline{r_\lambda}(u^*)=\int_0^{bt}r_\lambda(y)d\psi_m(y)=E(u^*)$ також не належить від λ і правило $u^*(x)$ являється мінімальним.

Для забезпечення приналежності правила $u^*(x)$ класу $\Delta(T)$, *більш точно, для виконання умови* $M_\infty\tau^*=T$, поріг b_t необхідно обирати за формулою:

$$b_t=T+M_\infty L^*(0) \tag{25}$$

Це випливає з мартингальних властивостей статистики $L^*(t)-t$, в силу яких $M_\infty\left(L^*(\tau^*)-\tau^*\right)=M_\infty L^*(0)$, і тієї обставини, що $L^*(\tau^*)=b_t$. Знаходження необхідного розподілу $\psi_m(y)$ і, відповідно, порогу b_t при довільному значенню T, не є можливим. Однак цю задачу можна розв'язати при великих значеннях T.

Дійсно, якщо $T\to\infty$, то в якості розподілу $P_\infty(L(\infty)\le y)$ марківського процесу $L(t)(t\to\infty)$, що задовольняє (24) при $y(t)=\sqrt{N}\,\omega(t)$. Можна показати, що це розподіл

$$\psi_m(y)=\exp\left(-\frac{1}{qy}\right),\ y\in(0,\infty) \tag{26}$$

Використовуючи (26), знаходимо

$$M_\infty L^*(0)=\exp\left(\frac{1}{qb_t}\right)\int_{(qbt)^{-1}}^{\infty}y^{-1}\exp(-y)\,dy=\frac{1}{q}E_1\left(\frac{1}{qb_t}\right)\exp\left(\frac{1}{qb_t}\right) \tag{27}$$

де $E_1(x)-$інтегральна показникова функція.

При $b_t \to \infty$ з (27) маємо

$$M_\infty L^*(0) = \frac{1}{q}\left\{ lnqb_t - Э + G\left(\frac{1}{qb_t}\right)\right\} \tag{28}$$

З (25) та (28) слідує, що при великих значення T поріг b_t є розв'язком транспортного рівняння

$$b_t = T + \frac{1}{q} lnqb_t \tag{29}$$

Оскільки в якості розподілу початкового значення $L^*(0)$ при великих T наступає стаціонарний розподіл $\{L(t)\}$, то зрозуміло, що для $\mathrm{E}(u^*)$ справджується розклад (20) при заміні b на b_t;

$$\mathrm{E}(\mathrm{u}^*) = \frac{1}{\mathrm{q}}\left[\ln(\mathrm{qb_t}) - 1 - Э + \mathrm{G}\left(\frac{1}{\mathrm{qb_t}}\right)\right] \quad T \to \infty \tag{30}$$

Якщо покласти $b_t = T + \frac{1}{\mathrm{q}}\ \mathrm{lnqT}$, то в силу (28) та (30) маємо

$$\mathrm{M}_\infty \tau^* = \mathrm{T} + \frac{1}{\mathrm{q}}\mathrm{lngT} - \frac{1}{\mathrm{g}}\ln(\mathrm{qT} + \mathrm{lngT}) = \mathrm{T} - \mathrm{G}\left(\frac{\mathrm{lnT}}{\mathrm{T}}\right),\ T \to \infty \tag{31}$$

$$E(u^*) = \frac{1}{q}\left\{\ln(qT) - 1 - Э + G\left(\frac{lnqT}{qT}\right)\right\},\ T \to \infty \tag{32}$$

Висновки

Таким чином з (31) та (32) слідує, що $u^*(x)$ «майже», належить класу ΔT, та головний член асимтотичного розкладу максимального за λ значення ризику дорівнює аналогічному головному члену асимптотичного розкладу ризику правилі (19). Звідси випливає, що обидва правила асимтотично мінімаксні в сенсі першого порядку.

Список літератури

1. Грищук Р.В., Даник Ю.Г. Основи кібернетичної безпеки. Житомир: ЖНАЕУ, 2016. 636 с.
2. Brailovskyi N., Kozura V., Kondakova S., Khoroshko V. Analysis of the Cyber security Status of the Information Space. *Scientific and Practical Cyber Security Journal*, V2, №4, 2018. P. 64-74.
3. Іванченко І.С., Хорошко В.О. Інформаційне протиборство в геополітичному просторі. *Сучасна спеціальна техніка*, 2019. №3 (58), С. 26-37.
4. Пирцхалава Л.Г., Хорошко В.А., Хохлачова Ю.Е., Шелест М.Е. Информационное противоборство в современных условиях. К.: ЦП "КОМПРИНТ", 2019. 226 с.
5. Опірський І.Р. Загальні проблеми прогнозування НСД в інформаційних системах держави. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*, 2015. Вип. 2(30). С. 31-34.
6. Козюра В.Д., Ткач Ю.М., Шелест М.Є., Козюра В.Д. та ін. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах. Ніжин : ФОП Лук'яненко В.В., ТПК «Орхідея», 2019. 144 с.
7. Козюра В.Д., Ткач Ю.М., Шелест М.Є. та ін. Захист інформації в комп'ютерних системах. Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2020. 236 с.
8. Закс Ш. Теория статистических выводов. М: Мир, 1995. 776с.
9. Ширяев А.Н. Статистический последовательный анализ. Оптимальные правила остановки. М.: Наука, 1999. 272с.
10. Креденцер Б.П., Миночкин А.И., Могилевич Д.И. Оценка эксплуатационно-технических характеристик объектов телекоммуникаций при априорной неопределенности. К.: Феникс, 2012. 336с.
11. Кокс Д., Льюис П. Статистический анализ последовательностей событий. М.: Мир, 1999. 312 с.
12. Опірський І.Р. Оптимізація послідовних процесів прийняття рішень при умовно екстремальній постановці задачі. *Інформаційна безпека*, 2014. №4(16). С. 120-127.
13. Опірський І.Р. Проблематика основного постулату прогнозування НСД. *Сучасна спеціальна техніка*.2015. №2(41). С. 3-8.
14. Дудикевич В.Б., Опірський І.Р., Гаренюк П.І., Ваврічен О.А. Оптимальність не усеченної процедури Вальда в задачах перевірки двох простих прогнозів НСД в інформаціних мережах держави. *Інформатика та математичні моделі в моделюванні*. 2016. Т.6, №3. С. 215-226.
15. Pollak M., Siegmund D. A Diffusion Process and Its Applications to Detecting a Change in the Drift of Brownian Motion. *Biometrika.* 1995. V.72, №2. P.267-280.

CYBER ATTACKS DETECTION IN INFORMATION NETWORKS

I.R. Opirsky[1], Y.M. Tkach[2], V.O. Khoroshko[3]

[1]National University "Lvivska Politechnika",
Ukraine, Lviv, 79013, ul. S. Banderi, 12, e-mail: iopirsky@gmail.com
[2]National University "Chernigivska Politechnika",
Ukraine, Chernigiv, 14035, ul. Shevchenko, 95, e-mail: tkach_ym@ukr.net
[3]National Aviation University, 03058,
Ukraine, Kiyiv, prosp. Lyubomyr Guzara, 1, e-mail: professor_va@ukr.net

Cyber security is becoming increasingly important in ensuring the national security of various countries. Cyber attacks and cyber influences are increasingly becoming one of the main actions to achieve the goal of control over various objects (person, organization, region, state, etc.) in the modern world. Thus, a new phenomenon in international politics has emerged in the world - the ability to achieve their own political goals, economic and spiritual subordination of the peoples of other states without the use of military force. Therefore, cyber attacks and cyber influences are developing quite actively in the world. Therefore, for the effective operation of modern information and telecommunication networks and means of their protection, as well as for the reliable detection and prediction of cyber attacks and unauthorized actions, it is necessary to develop new approaches and methods of cyber security. The purpose of the article is to detect cyber attacks in information networks. The problem of detecting a cyber-attack A (t) against the background of white Gaussian noise V (t) under the condition of continuous observation time is considered. The theoretical substantiation of the averaged forecasting object (AOP) is given. A consistent analysis of UOP in the general case revealed that it is not a sufficient statistic in the problem of sequential detection of cyber attacks. From the above it follows that one of the main issues in the synthesis of optimal sequential and inconsistent detector of cyber attacks with random moments of occurrence is to find algorithms for the formation of UOP. As a result of the conducted researches the technique of detection of NSD with the unknown moment of occurrence in discrete time of supervision is offered.
Keywords: information systems, cyber-attack, averaging about forecasting.

DOI 10.15276/imms.v10.no 3-4.190
УДК 681.51

Informatics and Mathematical Methods in Simulation
Vol. 10 (2020), No. 3-4, pp. 190-196

ЗАСТОСУВАННЯ НЕЧІТКОГО РЕГУЛЯТОРА ДЛЯ РЕГУЛЮВАННЯ РІВНЯ ВОДИ В БАРАБАНІ ПАРОВОГО КОТЛА Е-50

А.С. Рура, О.С. Тарахтій

Одеський національний політехнічний університет
проспект Шевченка, 1, Одеса, 65044, Україна;
e-mail: rurandrew@gmail.com, tarakhtij@opu.ua

Рівень води в барабані парового котла є одним із найважливіших параметрів, що характеризує надійність роботи котлоагрегату. В даний час все більшого поширення набувають нечіткі регулятори, які реалізують на практиці нечіткі алгоритми управління агрегатами, механізмами, а також технологічними процесами. Застосування технології нечіткої логіки, орієнтованої на обробку логіко-лінгвістичних моделей подання знань, відкриває широкі перспективи для створення інтелектуальних систем управління складними динамічними об'єктами, що діють в умовах неповної інформативності, прогнозувати поведінку системи, формувати множину альтернативних дій, виконувати формальний опис нечітких правил прийняття рішень. Оперативна ж зміна налаштованих параметрів регулятора дозволяє якісно перейти на більш високий рівень управління технологічними процесами, які супроводжують діяльність людини. Метою цієї роботи є проведення аналізу якості стабілізації рівню води в барабані парового котла за умови впровадження нечіткого регулятора, а також спрощення структури системи регулювання. У статті пропонується порівняльний аналіз моделі класичної3-імпульсної автоматичної системи регулювання (АСР) рівня з ПІ-регулятором з одноконтурною АСР з нечітким регулятором, у який введено додатковий сигнал по швидкості зміни відхилення регульованої величини. Три-імпульсна АСР має недоліки. Основним недоліком вказаної АСР є той факт, що при зникненні будь-якого з трьох сигналів система припиняє роботу, а при наявності розбіжності в показаннях витратомірів по живильній воді та перегрітому пару регулятор починає підтримувати рівень води в барабані, який дорівнює сумі завдання і величини, пропорційній цій розбіжності (з'являється статична помилка регулювання).

Ключові слова: рівень живильної води,нечіткий регулятор,паровий котел, барабан,регульований параметр,автоматизована система регулювання.

Постановка проблеми

Рівень в барабані є одним з найважливіших регульованих параметрів правого котла, до якого виставляються жорсткі вимоги. Це обумовлено тим, що зниження або підвищенні рівня води в барабані парового котла суттєво знижує ефективність його роботи або може призвести до виходу з строю котлоагрегату в цілому [1, с.225]. При створенні сучасних систем автоматичного управління технічними об'єктами широке застосування знаходять нечіткі регулятори. Теорія нечітких множин дозволяє задавати алгоритми змінення налаштованих параметрів корегувальних пристроїв,враховуючи відхилення регульованої величини, а також швидкості змінення цього відхилення [2, с.295]. Тому досить важливим є завдання комплексного дослідження нечіткого регулятора, із застосуванням його на промислових котлах, що дозволяє виявити основні закономірності його функціонування при зміні тих чи інших налаштувань.

Аналіз останніх досліджень і публікацій

В роботі А.А. Коростельова [5], проводиться порівняння ПІ-регулятора з нечітким регулятором. Порівняльний аналіз якості регулювання проводився при збуреннях,

що йдуть по каналах завдання, регулювання і параметричного збурення. Якість регулювання визначалася за такими характеристиками: динамічна помилка, ступень гасіння, час регулювання. Отримані в роботі результати показали, що система з нечітким регулятором перевершує систему з ПІ-регулятором за швидкодією. Динамічна помилка системи з нечітким регулятором незначно відрізняється від динамічної помилки системи з ПІ-регулятором. Дослідження, проведені Куколевим А.А. та Пиотровским Д.Л. [2] показали, що нечітке регулювання може застосовуватися для управління судовим допоміжним котлоагрегатом і має більшу швидкодію, порівняно з регулюванням по ПІ-закону.

Викладення основного матеріалу

Регулювання живлення парового котла є дуже важливим, оскільки відхилення рівню води в барабані може стати причиною важких механічних пошкоджень екранних труб,а також ротора і лопаток парової турбіни. [3, с.163].

Якість регулювання живлення парового котла визначається не лише точністю підтримки рівня на заданому значенні, але і рівномірністю подачі живильної води. [4, с.15; 5, с.221].

Для проведення аналізу взято 3-імпусльну АСР рівня, яка є найбільш розповсюдженою на енергетичних котлах середньої потужності, яким є барабанний котел Е-50. Принципова схема даної АСР наведена на рис. 1.

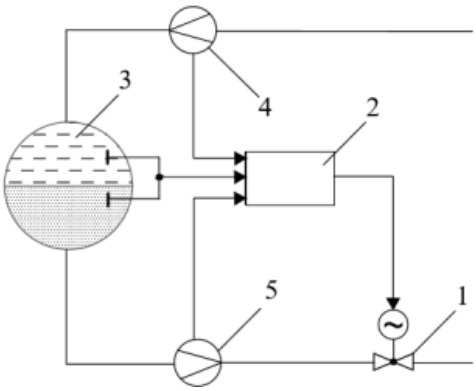

Рис. 1. Принципова схема 3-імпульсної АСР рівню води в барабані: 1 – регулюючий клапан живильної води; 2 – регулятор живлення; 3 – барабан; 4 – сигнал по витраті пара; 5 – сигнал по витраті живильної води.

Принцип роботи 3-імпульсної автоматичної системи регулювання полягає у наступному. Сигнали за витратою пари та живильної води вводяться в регулятор з протилежними знаками. У сталому режимі ці сигнали дорівнюють один одному, протилежні за знаком і, відповідно, компенсують один одного. Сигнал за рівнем води в барабані компенсується сигналом завдання [3]. Основною перевагою даної АСР, яка обумовила її розповсюдження, є той факт, що при зміні витрати пари регулятор дуже швидко змінює витрату живильної води не дочікуючись зміни рівня. Ця перевага дозволяє нейтралізувати так зване явище «набухання» рівню води.

Однак на зважаючи на вказану перевагу, 3-імпульсна АСР має і недоліки. Основним недоліком вказаної АСР є той факт, що при зникненні будь-якого з трьох сигналів система припиняє роботу, а при наявності розбіжності в показаннях витратомірів по живильній воді та перегрітому пару регулятор починає підтримувати рівень води в барабані, який дорівнює сумі завдання і величини, пропорційній цій розбіжності (з'являється статична помилка регулювання).

Схему нечіткого регулятора розроблено на основі [2]. Однак за основу взято одноконтурну АСР рівня, принципова схема якої представлена на рис. 2.

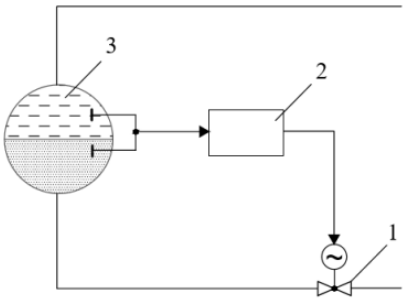

Рис. 2. Принципова схема одноконтурної АСР рівня води у барабані: 1 – регулюючий клапан живильної води; 2 – регулятор живлення; 3 – барабан

В наведеній схемі на вхід регулятора рівня 2 надходить лише сигнал від датчику вимірювання рівня в барабані 3. Після чого регулятор здійснює вплив на регулюючий клапан 1 і змінює витрату живильної води [3]. Однак в енергетичних котлах середньої потужності, які мають невеликий запас живильної води, використання даної АСР є неможливим в наслідок статичної похибки регулювання і неможливість забезпечення сталого регулювання в наслідок явища «набухання» рівню.

Моделювання перехідних процесів здійснювалося за допомогою середовища MatLab, функцію нечіткого регулятора виконує об'єкт FIS Editor (Рис.3), який в основі завантажених в нього даних регулятора розраховує керуючий вплив.

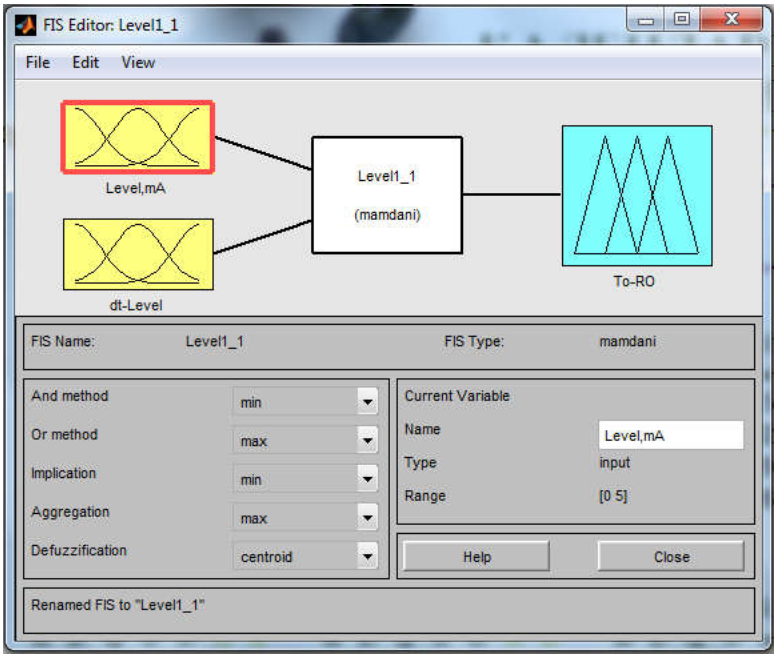

Рис. 3. Редактор систем нечіткого виводу FIS

Функції приналежності обрано дві: це зміна похибки регулювання та швидкість зміни похибки регулювання. Таким чином, кількість і характер функцій приналежності для регулятора пропорційного ланки приймають такий вигляд, рис. 4.

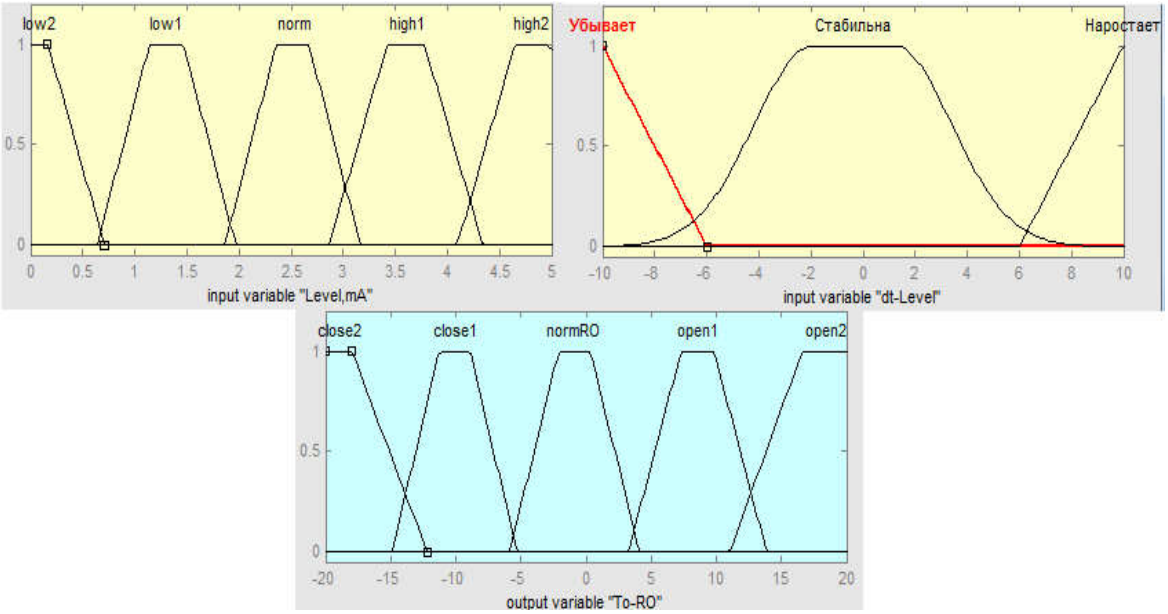

Рис. 4. Лінгвістичні змінні нечіткого регулятора системи автоматичної підтримки рівня води в барабані парового котла Е-50.

Перелік евристичних правил, які встановлюють співвідношення лінгвістичних змінних, наведено на рис. 5.

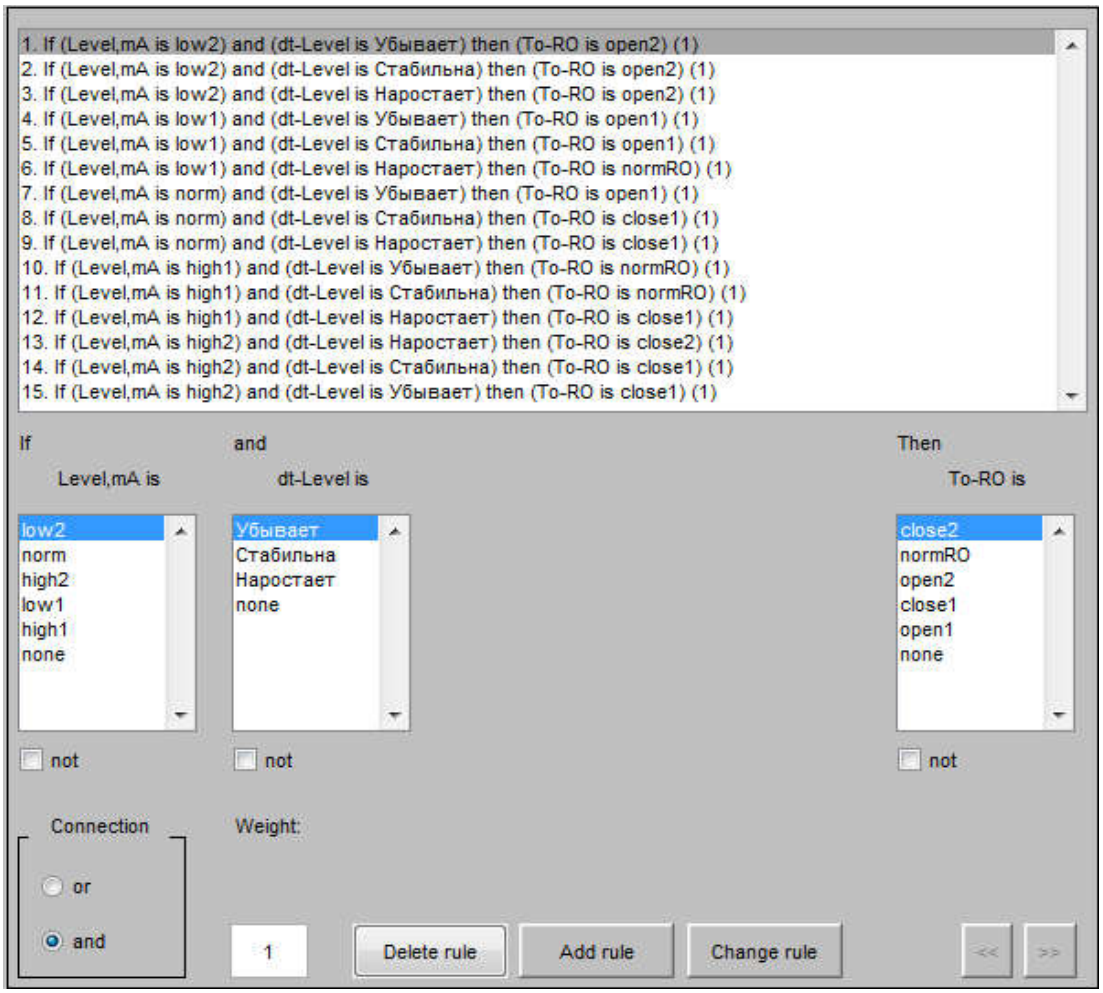

Рис. 5. Перелік правил для лінгвістичних змінних

Після визначення всіх параметрів нечіткого регулятора, промоделюємо його роботу у середовищі MatLab, а також порівняємо його із звичайним 3-імпульсним ПІ-регулятором.

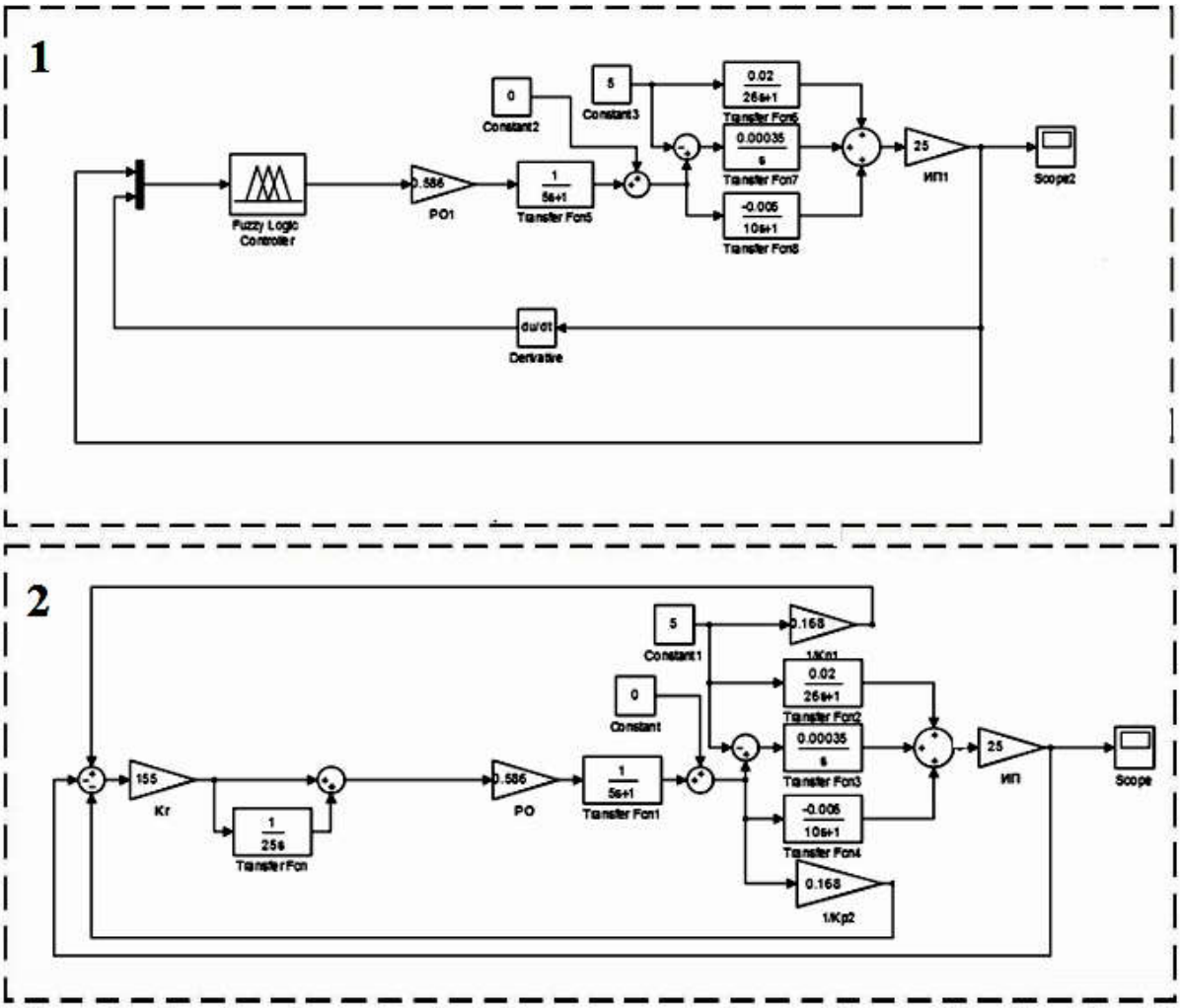

Рис. 6. Схема моделювання одноконтуроної АСР із застосуванням нечіткого регулятора (1) та 3-імпульсної АСР із застосуванням класичного ПІ-регулятора (2)

Нечіткий логічний регулятор був впроваджений в існуючу систему, замінивши класичний ПІ-регулятор, давши можливість спростити схему до одноконтурної. Графіки перехідних процесів зображенні на рис. 8.

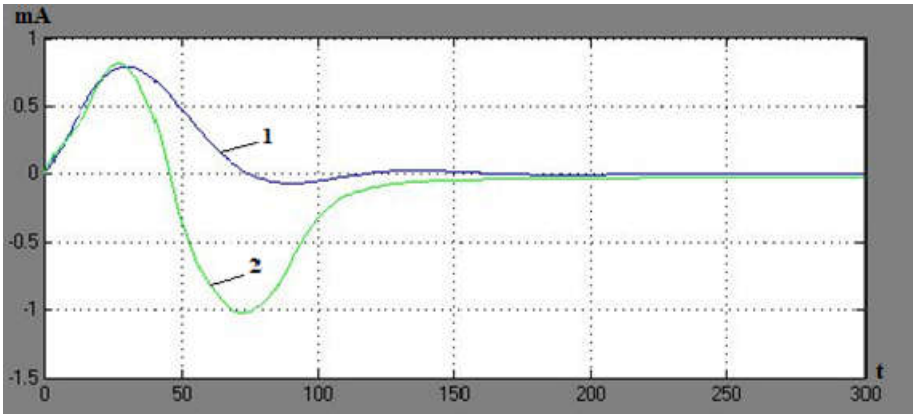

Рис. 7. Перехідні характеристики для класичного 3-імпульсного ПІ-регулятора (1) та одноконтурної АСР з нечітким регулятором (2)

Порівнюючи класичний і нечіткий ПІ-регулятор, ми можемо помітити, що в останнього, якість регулювання є нижчою, а ніж у класичного ПІ – регулятора за рахунок більшого відхилення регульованої величини, але час регулювання є однаковим. Слід пам'ятати, що з нечітким регулятором показана робота 1-контурної АСР рівня, яка має нижчу якість регулювання за 3-імпульсну. Однак, не зважаючи на це відхилення рівняння перевищують допустимих значень(± 1.25 мА).

Висновок

Нечіткий регулятор в складі одноконтурної АСР з додатковим імпульсом за швидкістю зміни регульованої величини може використовуватися для регулювання рівню води в барабані парового котла Е-50. Якість перехідних процесів є задовільною: час регулювання не збільшився, відхилення рівня не виходять за допустимі значення. Значною перевагою АСР з нечітким регулятором є спрощення схеми регулювання до одноконтурної. Таким чином, можна зробити висновок, що нечіткі логічні системи управління мають хороші перспективи для впровадження їх в автоматизації промислових котлоагрегатів.

Список літератури

1. Фам В.Д., Коновалов В.И. Исследование вариантов построения САР уровня в барабане парового котла. *Сборник трудов XI МНПК студентов, аспирантов и молодых учащихся.* 2013. С. 225 – 227.
2. Куколев А.А., Пиотровский Д.Л. О применении нечеткого адаптивного регулятора в системе управления уровнем воды в судовом вспомогательном котле. *Научные труды Куб ГТУ.* 2018. № 3. С. 295 –303.
3. Рура А.С., Тарахтій О.С. Аналіз існуючих схем регулювання рівня в барабані парового котла. *Молодий вчений*. 2019. № 11(75). С. 163 – 166.
4. Плетнев Г.П. Автоматизация технологических процессов и производств в теплоэнергетике. Москва, 2007. 352 с.
5. Коростелёв А.А. Сравнительный анализ функциональных возможностей интеллектуальных нечетких и ПИ-регуляторов. *Первый открытый конкурс молодых специалистов ЗАО «Сиб КОЭС». 2008.*

DEVELOPMENT OF A FUZZY CONTROLLER OF THE WATER LEVEL IN THE DRUM STEAM BOILER E-50

A.S. Rura, O.S. Tarakhtiy

Odessa National Polytechnic University
Shevchenko Avenue, 1, Odessa, 65044, Ukraine;
e-mail: rurandrew@gmail.com, tarakhtij@opu.ua

The water level in the drum of a steam boiler is one of the most important parameters characterizing the reliability of the boiler unit operation. Currently, fuzzy controllers are becoming more and more widespread, which implement in practice fuzzy algorithms for controlling units, mechanisms, as well as technological processes. The use of fuzzy logic technology, focused on processing logical-linguistic models of knowledge representation, opens up broad prospects for creating intelligent control systems for complex dynamic objects operating in conditions of incomplete information content, predicting the behavior of the system, generating many alternative actions, and performing a formal description of fuzzy de-

cision-making rules. Operational change of the tuning parameters of the regulator makes it possible to qualitatively move to a higher level of control over technological processes accompanying human activity. The purpose of this work is to analyze the quality of stabilization of the water level in the drum of a steam boiler subject to the introduction of a fuzzy regulator, as well as to simplify the structure of the control system. The article proposes a comparative analysis of the model of a classic 3-pulse automatic control system (ACS) with a PI-controller with a single-loop ACS with a fuzzy controller, into which an additional signal is introduced for the rate of change of the deviation of the controlled value. Three-pulse ACS has disadvantages. The main disadvantage of this ACP is the fact that the disappearance of any of the three signals, the system stops working, and in the presence of discrepancies in the readings of flow meters for feed water and superheated steam, the regulator begins to maintain the water level in the drum, which is equal to the sum of the task and value, proportional to this discrepancy (there is a static adjustment error).
Keywords: feed water level, fuzzy regulator, steam boiler, drum, adjustable parameter, automated control system.

DOI 10.15276/imms.v10.no 3-4.197
УДК 004.056.53

Informatics and Mathematical Methods in Simulation
Vol. 10 (2020), No. 3-4, pp. 197-207

РОЗРОБКА СИСТЕМИ БЕЗПЕКИ КЛІЄНТ-СЕРВЕРНОГО ЗАСТОСУНКУ НА БАЗІ ОПЕРАЦІЙНОЇ СИСТЕМИ ANDROID

А.Ю. Судаков, А.В. Соколов

Одеський національний політехнічний університет,
Україна, Одеса, 65044, пр. Шевченка, 1, e-mail: radiosquid@gmail.com

В сучасному світі неможливо обійтися без використання різного роду систем комунікації. Вони стали невід'ємною частиною нашого життя. Майже кожна сучасна людина користується тою чи іншою системою обміну інформації з іншими людьми. Частіше всього для обміну інформацією використовуються мобільні платформи. В переважній більшості це такі платформи як Android, iOS та Windows Phone. Інформація, яка передається від одного користувача до іншого, часто може бути конфіденційною або з обмеженим доступом. Для цього мають використовуватися відповідні методи захисту інформації. Сьогодні увага дослідників інформаційної безпеки зосереджена на покращенні роботи криптографічних алгоритмів та примітивів, на яких вони засновані. Тим не менш, питання побудови комплексних систем захисту в системах обміну миттєвими повідомленнями залишаються розглянутими недостатньо. Дана стаття присвячена розробці комплексної системи захисту застосунку для обміну миттєвими повідомленнями. Будь який застосунок для роботи з миттєвими повідомленнями складається з трьох основних частин. Першою складовою частиною є програмний код, виконуваний на мобільній платформі. Другою частиною є канал зв'язку. Останньою частиною є програмний код, виконуваний на стороні серверу. В даній статті розглянуто кожну з основних частин для побудови комплексної системи захисту застосунку для обміну миттєвими повідомленнями. Обґрунтовано вибір тих чи інших компонентів для побудови системи захисту, приведено схеми роботи програмного коду виконуваного на мобільній платформі Android, обґрунтовано вибір форм передачі користувацької інформації через канал зв'язку. Надано рекомендації по вибору каналу зв'язку та забезпеченню його безпеки. Також приведено схеми роботи серверної сторони застосунку. Обґрунтовано вибір тих чи інших хеш-функцій, функцій перевірок вхідної інформації, підходів до реалізації системи захисту, системи зберігання і обробки користувацької інформації на стороні серверу. У застосунку також продемонстровано деякі недоліки поточної версії мобільної платформи Android з точки зору інформаційної безпеки. Показано, як зловмисники можуть використати ці недоліки, та надано поради по уникненню їх експлуатації зловмисником. Результати роботи можуть бути використані для захисту інформації у подібних застосунках.

Ключові слова: системи обміну миттєвими повідомленнями, захист інформації, мобільний застосунок.

Вступ і постановка задачі

З кожним днем кількість користувачів мобільних пристроїв зростає. Більшість пристроїв, які використовують користувачі, — це смартфони та планшети на базі операційної системи Android та iOS. Нові способи взаємодії з пристроєм та його мобільність — це нові фактори, через які з'являються нові проблеми з інформаційною безпекою користувача. При розробці мобільного застосунку необхідно брати до уваги те, що дані, які використовуються застосунком, можуть представляти певну цінність для зловмисників. Те, наскільки цінною буде інформація, залежить від багатьох факторів, проте навіть найпростіша інформація, наприклад, особистий пароль від облікового запису користувача потребує опрацювання його за допомогою системи захисту. На сьогоднішній день мобільні застосунки зайняли місце у всіх сферах електронних послуг, включаючи фінансові, банківські операції, зберігання і передачу

особистих даних, що робить завдання підвищення їх безпеки особливо важливим [1]. Сьогодні в літературі чимало уваги дослідники приділяють основним блокам для побудови систем захисту інформації — криптографічним алгоритмам, хеш-функціям, тощо [2, 3]. Однак питання побудови комплексних систем захисту інформації для конкретних програмних продуктів, зокрема, систем обміну миттєвими повідомленнями освітлені в літературі недостатньо. Існуючі представлені системи [4…6] є специфічними і при цьому деталі технічної реалізації їх систем захисту інформації на клієнтській та серверній частині розкрито не повністю. При цьому системи безпеки реально працюючих програмних продуктів зазвичай, в більшій своїй частині, залишаються комерційною таємницею компаній, що розроблюють та підтримують свої програмні продукти, та є недоступними для світової наукової спільноти. У цій роботі розглядається питання побудови комплексної системи безпеки реального застосунку для обміну миттєвими повідомленнями на базі операційної системи Android.

Метою роботи є розробка системи захисту інформації застосунку для обміну миттєвими повідомленнями.

Основна частина

Більшість сучасних застосунків є клієнт-серверними, тобто частина логіки застосунку, а також частина інформації користувача зберігається та обробляється на стороні серверу [7]. Для отримання якісної моделі системи захисту клієнт-серверного Android застосунку, а також для кращого її розуміння розділимо її на три основні частини. Кожна частина системи безпеки буде розглянута окремо для кращого її розуміння та більш детального опису. Розглянемо три основні частини захисту клієнт-серверного застосунку.

Перша частина, це власне сам застосунок, точніше його код, який буде виконуватися на пристрої користувача, всі маніпуляції з інформацією та її захистом на пристрої. Друга частина — канал передачі інформації між пристроєм та сервером. Остання частина системи безпеки — серверна сторона застосунку — код, який обробляє запити та надсилає відповіді на них, а також сам сервер і база даних, в якій зберігається інформація користувачів. Основні частини клієнт-серверного застосунку показані на рис. 1.

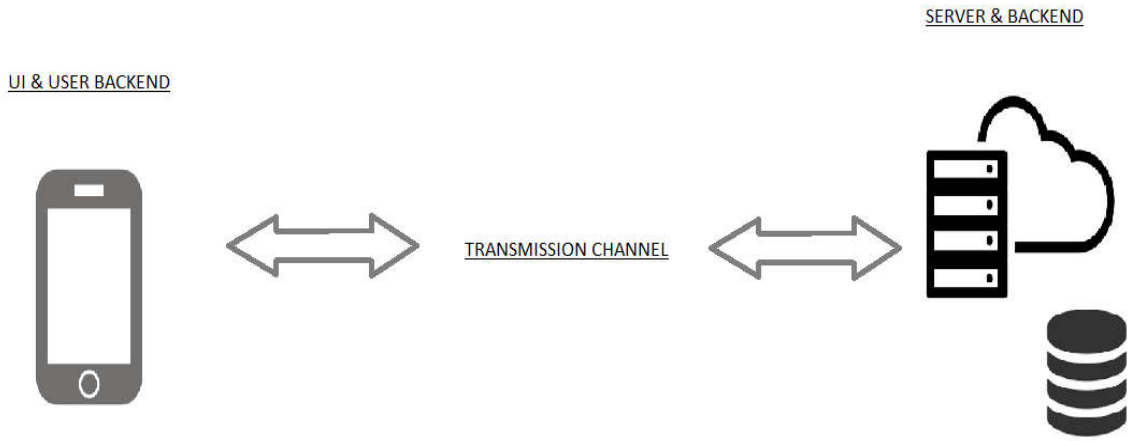

Рис. 1. Основні частини клієнт-серверного застосунку

Далі ми окремо розглядаємо аспекти системи захисту інформації у кожній частині клієнт-серверного застосунку.

1. Захист на стороні клієнта

Розглянемо більш детально клієнтську частину системи захисту клієнт-серверного застосунку. Вона складається з двох основних частин. Перша частина — те, що бачить користувач на дисплеї свого екрану — UI (UserInterface), друга частина — код, який виконується на пристрої — backend, тобто сторона застосунку, яка прихована від користувача.

Кожен користувач клієнт-серверного застосунку має бути авторизованим [8]. Частіше всього в якості ідентифікатора в сучасних застосунках виступає обліковий запис користувача певного пристрою. Проте є застосунки, які надають доступ до інформації тільки після вводу певних даних для авторизації і знищують всю інформацію після виходу з облікового запису. Саме такими є два основних підходи до створення систем захисту. Перевагою першого є те, що користувачу достатньо знати пароль та логін і, маючи ці дані, він в будь-який час може отримати доступ до своєї інформації. З точки зору користувача, така система є доволі комфортною. Проте в ній є певні недоліки. Наприклад, небажано, щоб хтось інший міг отримати доступ до інформації користувача. Уявимо ситуацію, коли така інформація не видаляється, а зберігається в певному місці. Дані для входу в обліковий запис можуть бути викрадені і зловмисник отримає доступ до інформації користувача. Проте, якби така інформація була видалена відразу після виходу із облікового запису, навіть отримавши доступ до нього, було б неможливим отримання такої інформації, адже вона була видалена. В свою чергу, недоліком другого підходу є те, що користувачеві необхідно кожного разу вводити одну і ту ж саму інформацію, що викликає дискомфорт у користувачів. Також без збереження даних користувачів складно відрізнити одного користувача від іншого, або і зовсім неможливо. Це несе ризик того, що один користувач зможе використовувати ресурси, розподілені на інших користувачів і як наслідок, перенавантажувати систему.

Для системи обміну миттєвими повідомленнями найкращим вибором системи авторизації є перший підхід. Даними для отримання доступу до інформації виступає логін та пароль. Розглянемо систему захисту застосунку на етапі входу в обліковий запис.

Тут слід наголосити, що вся інформація в застосунку може бути змінена користувачем. Завдання захисту інформації в застосунку в частині UI & USER BACKEND — захистити персональну інформацію користувача від інших застосунків та від витоку на сторонні сервісу, запобігти передачі некоректної інформації на сервер, для запобігання виникнення помилок в застосунку та позитивного досвіду користування у користувача. Слід розуміти, що вся інформація, яку користувач передає на сервер, повинна перевірятися на сервері. Інформація, яку застосунок передає на сервер може бути змінена як системою так і іншими застосунками, тому в самому застосунку перевірка інформації більше потрібна для зручності користувача.

Ще одним важливим моментом є безпека критично важливої інформації, яка зберігається на пристрої. До такої інформації можна віднести паролі, ключі, персональну інформацію.

В табл. 1, ми наводимо перелік основних вразливостей критично важливої інформації безпосередньо в самому застосунку, характеризуючи їх рівень небезпеки, а також наводимо методи захисту інформації, які було імплементовано у розробленій системі для протидії наведеній вразливості.

Почнемо з запуску застосунку. Під час запуску, система повинна перевірити, чи пройшов користувач процедуру входу в обліковий запис, а також перевіряти статус входу під час кожної дії користувача. Для цього використовується функція *is Authed ()*. Вона викликається застосунком при кожній дії користувача. Така функція звертається до внутрішньої бази даних для перевірки наявності даних для авторизації користувача на сервері. Якщо така інформація наявна, функція повертає true, інакше — false.

Якщо функція повернула true — виконується запуск activity, яка містить основну частину застосунку, проте, якщо функція повернула false — виконується запуск activity, яка містить поля для вводу інформації для авторизації на сервері. В нашому випадку, це поля *e-mail* та *password*.

Далі, інформація відправляється на сервер через протокол https. Коли відповідь від сервера отримана, створюється таблиця в локальній БД (Базі Даних), в якій зберігається хеш-значення паролю та e-mail, які будуть відправлятися на сервер з кожним запитом. В нашому випадку використовується хеш-функція sha-256, яка є досить стійкою на даний момент. Не рекомендується використовувати хеш-функції, довжина дайджесту яких менше ніж 256 символів. Такою застарілою функцією є md5. В найкращому випадку рекомендується використовувати хеш-функцію з третього покоління sha. Такою функцією є sha-512. Може здатися дивним те, що хеш-функція з довжиною дайджесту в 512 символів працює швидше ніж та ж сама функція, з довжиною дайджесту в 256 символів. Проте це доведений факт. В нашому застосунку використовується sha-256 для кращого сприйняття, адже вона давно відома і широко використовується.

Таблиця 1.

Перелік основних вразливостей критично важливої інформації безпосередньо в самому застосунку

№	Вразливість	Рівень ризику	Використане рішення захисту
1	Використання незахищених локальних сховищ	Дуже висока	Зберігати критично важливу інформацію тільки в захищених сховищах платформи Android
2	Зберігання інформації в захищених сховищах, але у відкритому вигляді	Середня	Критично важлива інформація не повинна використовуватися в застосунку без додаткового шифрування. Як тільки потреба в такій інформації відпала — вона негайно повинна бути або зашифрована, або знищена
3	Зберігання критично важливої інформації в коді	Висока	Не зберігати критично важливу інформацію в коді або ресурсах застосунку
4	Використання асиметричного алгоритму з приватним ключем, відомим для сервера	Залежить від ступеня захищеності сервера	Не зберігати приватний ключ на сервері, він повинен бути доступний тільки користувачу
5	Використання самописних алгоритмів шифрування та захисту	Середня	Слід підбирати відповідний алгоритм тільки з налагоджених і актуальних загальновідомих криптографічних алгоритмів
6	Передача критично важливої інформації у відкритому вигляді	Середня	Будь-яка інформація, перед виходом за межі застосунку повинна бути зашифрована
7	Ігнорування пристроїв з правами суперкористувача	Середня	Перевіряти на права суперкористувача систему і в разі їх наявності інформувати користувача і, по можливості, не продовжувати роботу застосунку без інформування користувача

Пароль обов'язково хешується ще до відправки на сервер. По каналу зв'язку передається тільки хеш-значення цього паролю. В локальній БД також зберігається тільки хеш-значення пароля. Як було вказано раніше в табл. 1 — не можна зберігати критично важливу інформацію в захищених сховищах у відкритому вигляді. При цьому e-mail зберігається у відкритому вигляді, оскільки в даному контексті він не відноситься до критично важливої інформації.

Коли застосунок отримав інформацію про успішний вхід до облікового запису і створив таблиці з даними користувача в локальній БД, ініціюється запуск основної activity в якій реалізовано основну частину логіки застосунку.

Схожим чином реалізується і «відновлення паролю». Після натискання на «відновити пароль» завантажується activity в якій є поля для вводу логіна та кнопка підтвердження дії. Перевірка логіна (e-mail) працює таким же чином як і при «вході» в застосунок. Для кращого розуміння на рис. 2 представлена схема логіки UI &BACKEND застосунку.

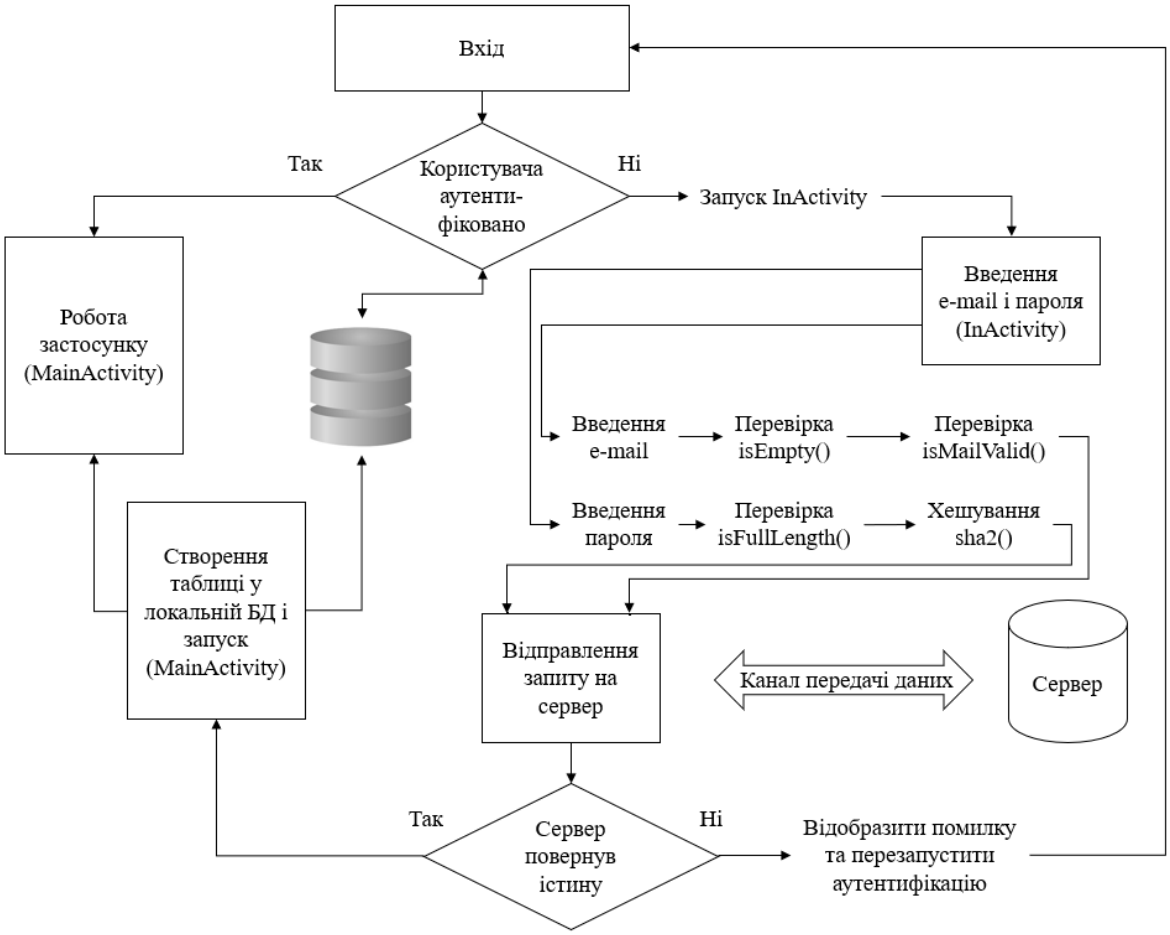

Рис. 2. Схема логіки входу та перетворення даних в UI &BACKEND частині

2. Захист інформації при її передаванні на сервер

Перейдемо до частини «TRANSMISSION CHANNEL». В застосунку використовується сучасний захищений протокол передачі https, який забезпечує безпеку інформації при її передаванні. Також для передачі даних на сервер використовується неявна передача методом POST замість стандартного GET, адже критично важливу інформацію слід передавати неявним методом. Інформація передається в вигляді «key –>value» без кодування JSON. Файли передаються як multipart/form-data.

3. Захист інформації на серверній частині

Перейдемо до останньої частини — Server & BACKEND. Розглянемо, як сервер опрацьовує запити та відповідає на них. Для кращого розуміння розглянемо можливість реєстрації нових користувачів у застосунку. Реєстрація на пристрої працює схожим способом як і «Вхід», дані обробляються тими ж функціями і так само відправляються на сервер. Різниця між «входом» і «реєстрацією» більше всього відчувається на стороні Server & BACKEND. Розглянемо більш детально.

Коли дані користувача потрапляють до серверу їх потрібно обробити. Не можна забувати, що дані могли прийти не від користувача і що в них може міститися шкідливий код або щось інше. Основні атаки на сервер — це DDoS, SQL-injection, XSS та OWASP [9]. Оскільки розглядається саме сторона захисту в коді, який опрацьовує запити (файл, який виконується після перевірки на безпеку запиту системою захисту сервера) то найактуальнішою, в даному контексті, атакою є атака типу injection та інші способи викликати помилку на сервері.

Для найкращого захисту від різних атак на сервері потрібно вимкнути відображення помилок користувачу і відображати мінімум інформації. Для цього, у випадку невірних параметрів або їх відсутності просто потрібно повернути помилку. Наприклад: `{"err":"wrongparam(s)"}`. Такий результат дає мало інформації і зловмисник не має можливості перевірити чи спрацював його метод, чи ні. Наступним кроком захисту є перевірка наявності всіх необхідних параметрів. Якщо кількість або імена параметрів не збігаються з потрібними — повертаємо помилку. Щоб перевірити наявність параметрів частіше всього використовують php код, наприклад, такий:

```
if(isset($_POST['app']) &&isset($_POST['mail']) &&
isset($_POST['userName']){doSomething();}else{exitWithStatus("wrong
param(s)");}
```

Такий спосіб перевірки не дасть зловмиснику вибрати інший метод передачі даних або додати свої параметри. В цьому випадку зловмиснику залишається тільки намагатися підмінити значення цих параметрів. Щоб захиститися від цього використовуються наступні функції:

– trim(data) — зрізає пробіли на початку і в кінці рядка, запобігає внесеннювідправки пустого поля;

– stripslashes(data) — видаляє екрануючіслеши, які можуть привести до виконання переданого коду;

– htmlspecialchars(data) — перетворює спеціальні символи в html сутності, таким чином можна запобігти будь-яким спробам виконати код.

Таким чином перевіряються всі параметри. Далі потрібно перевірити, що передано і яка в цього значення довжина. Це робиться за допомогою наступного коду:

```
if(strlen($data) <someLength){
exitWithStatus("err: wrongparam(s)");}
```

Так як ми розглядаємо процедуру реєстрації, після вказаних вище перевірок, необхідно перевірити, чи наданий e-mail вже зареєстровано. Якщо такий e-mail вже зареєстрований, але не підтверджений, потрібно видалити всю інформацію пов'язану з ним і надіслати код підтвердження на e-mail. Якщо користувач все ж таки не зареєстрований, потрібно згенерувати пароль, який буде зберігатись в БД. Перед тим, як вносити хеш-значення пароля в БД необхідно згенерувати для нього модифікатор входу хеш-функції. Модифікатор входу хеш-функції — певний рядок інформації, який передається хеш-функції разом з вхідним масивом інформації для вираховування хеш-значення. Модифікатор входу хеш-функції використовується для ускладнення визначення прообразу хеш-функції методом перебору по словнику можливих вхідних значень, включаючи атаки з використанням райдужних таблиць. Головною функцією є приховання факту використання однакових вхідних даних, наприклад, — паролів. Тобто, однакові паролі, після обробки хеш-функцією з додаванням модифікатора входу хеш-функції будуть виглядати по різному.

Модифікатор входу хеш-функції повинен бути максимально випадковим. Тому нами був обраний наступний підхід до формування модифікатора входу хеш-функції: для її генерації використовується хеш-значення пароля від користувача, до нього додається хеш-значення часу запиту з точністю до мілісекунди, ім'я користувача, а також хеш-значення e-mail адреси, яка була використана при реєстрації.

Отриманий рядок обробляється алгоритмом sha2(data) [10]. Отриманий модифікатор входу хеш-функції змішується з хеш-значенням пароля користувача і вноситься в БД. Тобто в розробленій нами системі у БД зберігається модифікатор входу хеш-функції і хеш-значення пароля користувача, яке було змішане з модифікатором входу хеш-функції. Таким чином, навіть однакові паролі в БД виглядають абсолютно по різному.

Одним з ризиків підсистеми реєстрації у системах парольного захисту інформації є атака за допомогою множинної реєстрації фейкових користувачів. Для цього нами були прийняті наступні засоби захисту: для підтвердження реєстрації генерується 4-х значний код, який відправляється на e-mail адресу, яка вказана при реєстрації. Для його генерації використовується функція «стандартний генератор псевдовипадкових чисел» за рівномірним законом у діапазоні від 1000 до 9999, після чого код зберігається в БД. Разом з ним генерується timeHash, який є унікальним ідентифікатором коду. Також, в БД зберігається кількість спроб ввести код. Якщо кількість спроб більше 3, код генерується знову, відправляється на e-mail.

Після того як код буде підтверджено, вноситься запис в БД про те, що користувач підтвердив e-mail і йому може бути надано доступ до інформації та можливостей. Нижче показана схема взаємодії даних від користувача та сервера (рис. 3).

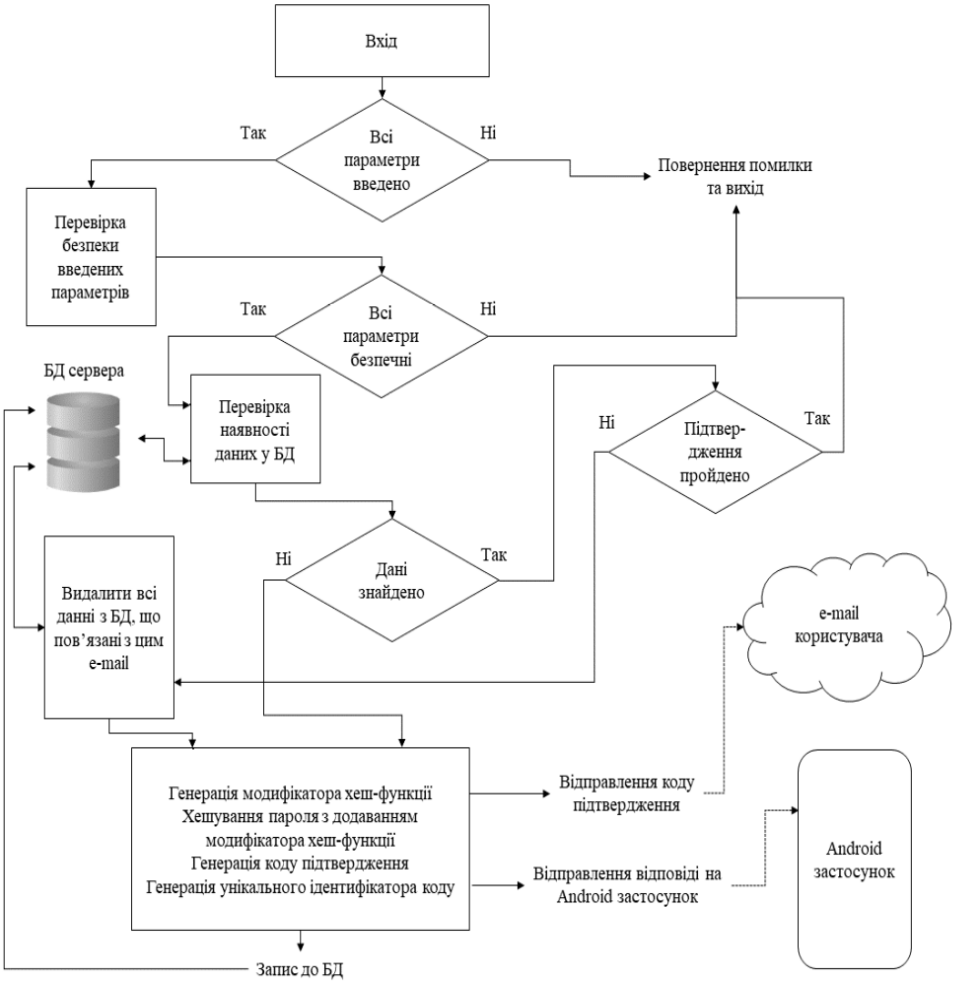

Рис. 3. Схема серверної логіки можливості «Реєстрація»

Після відправки коду підтвердження, сервер повідомляє про це застосунок. Застосунок, отримавши таку відповідь, завантажує activity для передачі коду підтвердження на сервер із застосунку. Система перевірки інформації та її захист виконується подібно до можливості «Реєстрація», як на сервері так і в самому застосунку.

Зовнішній вигляд застосунку представлено на рис.4.

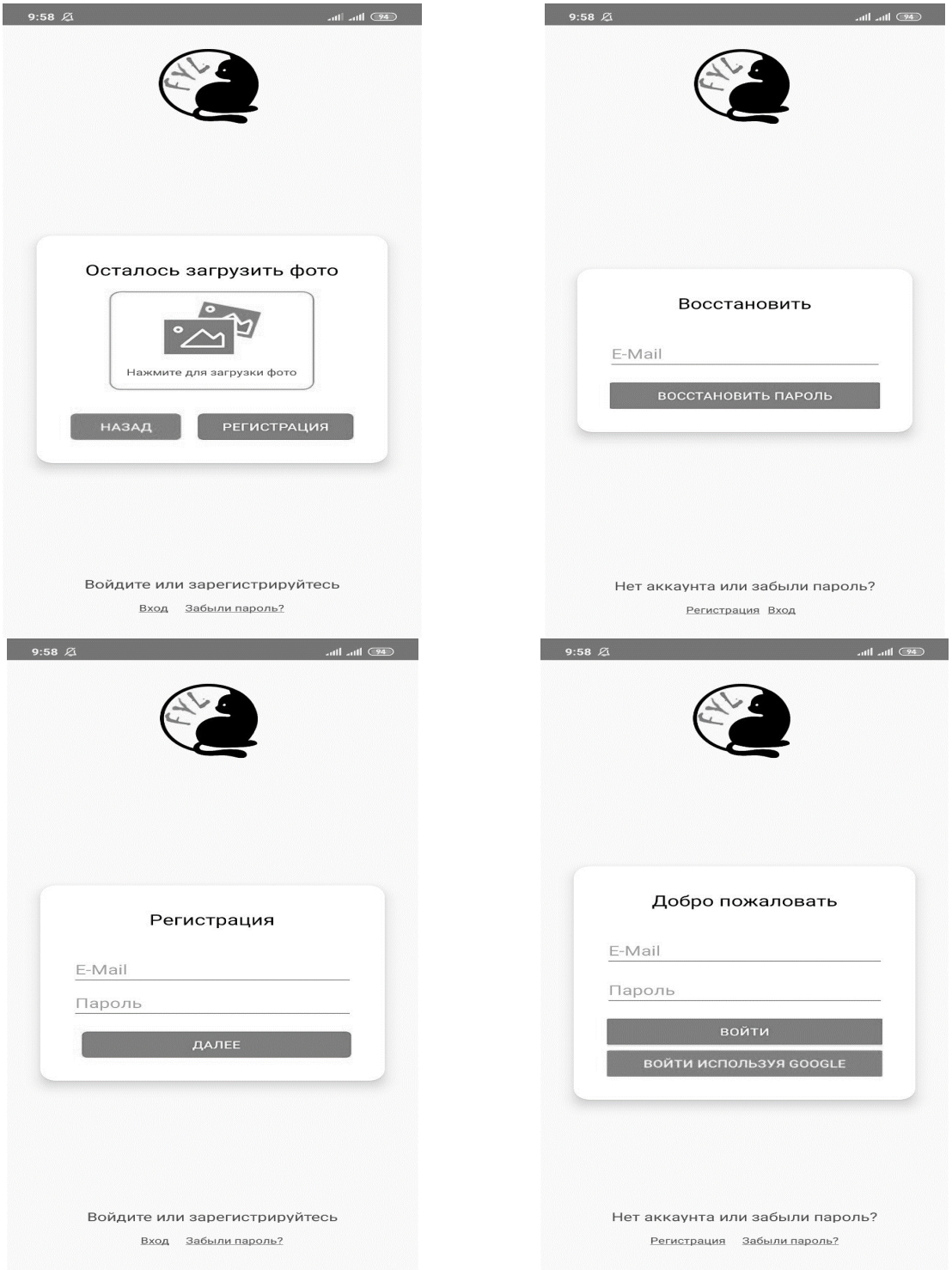

Рис. 4. Зовнішній вигляд розробленого застосунку

Код застосунку можна переглянути на GitHub за наступним посиланням [11].

Висновки

Відзначимо основні результати проведеного синтезу системи безпеки клієнт-серверного застосунку для обміну миттєвими повідомленнями:

1. При розробці клієнт-серверного застосунку мають окремо розглядатися заходи захисту інформації у трьох його основних частинах: на стороні клієнта, у каналі передачі даних та на серверній стороні. При цьому, зважаючи на існування надійного на цей час протоколу https, найголовнішими завданнями є розробка системи захисту у клієнтській та серверній частині.

2. В клієнтській частині застосунку було розроблено систему захисту, яка перевіряє всі введені користувачем дані. Перевіряється довжина введеної інформації в поля вводу, її формат, виконується перевірка на пустоту та допустимі символи. Також вся інформація в клієнтській частині зберігається в захищеному внутрішньому сховищі платформи у вигляді бази даних. Внутрішнє захищене сховище використовується для зберігання користувацьких фото. Критичні користувацькі дані, такі як пароль, не зберігаються у відкритому вигляді. Дані користувача про його місцезнаходження є менш критичними, тому зберігаються у відкритому вигляді, проте всього на протязі 24-х годин.

3. Серверна частина застосунку є більш захищеною ніж клієнтська сторона. Це зумовлено тим, що на серверній стороні обслуговуються запити від багатьох користувачів і перевірка на стороні сервера повинна бути якомога більш жорсткою та надійною. На стороні сервера, крім тих же перевірок, що і на клієнтській стороні, також виконується перевірка на кількість вхідних параметрів, екранується вхідна інформація для запобігання різного роду ін’єкцій в передану інформацію. В базі даних зберігаються певні мітки про користувачів, завдяки яким можна надати чи не надати доступ до ресурсу. Також зберігається кількість спроб вводу коду підтвердження та виконується ще ряд додаткових перевірок користувацької інформації. При виникненні помилки обробки запиту, сервер повертає відповідь з мінімальною кількістю інформації для запобігання вивчення системи безпеки на серверній стороні.

Було запропоновано нові підходи до реалізації:

— вводу та зберігання пароля в локальному сховищі;

— передачі пароля через канал зв’язку;

— генерації унікального хеш-значення з використанням унікальної користувацької інформації;

— перезавантаження сервісів після їх знищення системою;

— використання пасивних менеджерів для отримання геолокації з інших застосунків;

— пошукових запитів, які відображають збіги в користувацькому місцезнаходженні по даним геолокації та часу;

— зберігання користувацької інформації обмежений час, як в самому застосунку так і на сервері.

Таким чином, була розроблена система безпеки клієнт-серверного застосунку, яка показує як потрібно перетворювати, зберігати, передавати та обробляти інформацію користувача на пристрої, в каналі зв’язку та на сервері. Показано основні методи захисту від вводу некоректної інформації на пристрої, а також коректної обробки такої інформації на сервері. Розроблено конкретні схеми комунікації Androidзастосунку з сервером.

Список літератури

1. Внукова З.А., Буханцов А.Д., Путивцева Н.П., Кулешов С.И. Оценка безопасности систем мгновенного обмела сообщениями методом анализа иерархий. *Научные ведомости. Серия Экономика. Информатика*. 2016. №23(244). Вып. 40. С. 165–169.
2. Zhdanov O.N., Sokolov A.V. Block symmetric cryptographic algorithm based on principles of variable block length and many-valued logic. *Far East Journal of Electronics and Communications*. 2016. V.16, No. 3. P. 573–589.
3. Deng S., Li Y., Xiao D. Analysis and improvement of a chaos-based Hash function construction. *Communications in Nonlinear Science and Numerical Simulation*, 2010. V. 15, No. 5. P. 1338–1347.
4. Yang C.H., Kuo T.Y., Ahn T.N. et al. Design and Implementation of a Secure Instant Messaging Service based on Elliptic-Curve Cryptography. *International Symposium on Computer Science and Computational Technology*, 2008, 20–22 December 2008, Shanghai, China. P. 31–38.
5. Z. Wang, Z. Ma, S. Luo et. al. Enhanced Instant Message Security and Privacy Protection Schemed or Mobile Social Network Systems. *IEEE Access*. 2018. V.6. P. 13706–13715.
6. Bonesa E., Hasvolda P., Henriksena E. et al. Risk analysis of information security in a mobile in stant messaging and presence system for healthcare. *International Journal of Medical Informatics*. 2006. No. 76(9). P.677–687.
7. Чернобровкин С.В., Мялкин М.П. Архитектура клиент-серверного взаимодействия с мобильным приложением. *Молодежный научно-технический вестник*. 2015. №. 8.С. 25.
8. Шибанов С.В., Карпушин Д.А. Сравнительный аналіз современных методов аутентификации пользователя. *Информационное обеспечение систем*. 2015. №1(6). С. 33–37.
9. Al-Khurafi O.B., Al-Ahmad M.A. Survey of web application vulnerability attacks. *4th International Conference on Advanced Computer Science Applications and Technologies*.2015. P. 154–158.
10. Mendel F., Nad T., Schaffer M. Finding SHA-2 characteristics: searching through a minefield of contradictions. *International Conference on the Theory and Application of Cryptology and Information Security*., Berlin, Heidelberg : Springer, 2011. P. 288–307.
11. Sudakov A.Yu. Код застосунку FYL URL: https://github.com/ArtemSudakov/FylApp.

DEVELOPMENT OF CLIENT-SERVER APPLICATION SECURITY SYSTEM BASED ON ANDROID OPERATING SYSTEM

A.Yu. Sudakov, A.V. Sokolov

Odesa National Polytechnic University,
Ukraine, Odessa, 65044, 1 Shevchenko Ave. radiosquid@gmail.com

In today's world it is impossible to do without the use of various communication systems. They are now the integral part of our lives. Almost every modern person uses one or another system of information exchange with other people. Mobile platforms are most often used for information exchange. The vast majority are platforms such as Android, iOS and Windows Phone. Information transmitted from one user to another can often be confidential or restricted. So, the appropriate methods of information protection should be used for this purpose. Today, information security researchers focus on improving the performance of cryptographic algorithms and the primitives on which they are based. Nevertheless, the issues of building of integrated security systems for instant messaging systems remain insufficiently considered. This paper is devoted to the development of a comprehensive application protection system for instant messaging. Any IM application consists of three main parts. The first component is the program code executed on a mobile platform. The second part is the communication channel. The last part is the program code executed on the server side. This paper discusses each of the main parts for building a comprehensive application protection system for instant messaging. The choice of certain components for building a security system is substantiated, the schemes of operation of the program code executed on the Android mobile platform are given, the choice of forms of transmission of user information through the communication channel is substantiated. Recommendations for choosing a communication channel and ensuring its security are given. The schemes of the server side of the application are also given. The choice of certain hashes functions, functions of input information checks, approaches to the implementation of the protection system, storage system and processing of user information on the server side is substantiated. The developed application also shows some shortcomings of the mobile platform Android in terms of information security. It is shown how attackers can take advantage of these shortcomings, and suggestions to prevent their use are provided. The results of the work can be used to protect information in practical systems.

Keywords: instant messaging systems, information security, mobile application.

DOI 10.15276/imms.v10.no 3-4.208
УДК 681.51

Informatics and Mathematical Methods in Simulation
Vol. 10 (2020), No. 3-4, pp. 208-221

СИНТЕЗ РЕГУЛЯТОРА В ДИСКРЕТНОМУ ЧАСІ З ЗАДАНИМ ЧАСОМ ВСТАНОВЛЕННЯ ПЕРЕХІДНОГО ПРОЦЕСУ

А.О. Стопакевич, О.А. Стопакевич

Одеська національна академія зв'язку , 14, Кузнечна, Одеса, 65029, stopakevich@gmail.com
Одеський національний політехнічний університет 1, пр. Шевченка, Одеса, 65044, stopakevich@opu.ua

Фактичним стандартом для промислових технологічних процесів та багатьох інших галузей автоматизації є регулятор ПІД-типу. Проблема синтезу таких регуляторів достатньо докладно вивчена в літературі. Перевагою такого регулятора, що значною мірою вплинуло на його популярність, є те, що це регулятор, в якому наладчик системи автоматизації при незадовільних перехідних процесах в системі автоматичного керування може емпірично змінити числові коефіцієнти (від 1 до 4 в залежності від типу регулятора), базуючись на прямих критеріях якості перехідного процесу: максимальному відхиленні, перерегулюванні, часі встановлення, а також ознак нестійкої роботи. Проблему оптимального синтезу регулятора ПІД-типу за типовими моделями можна вважати у цілому розв'язаною. З розвитком комп'ютерної техніки й інженерних математичних пакетів задача синтезу оптимального регулятора ПІД-типу для довільного об'єкта керування розв'язується шляхом поєднання частотних критеріїв й оптимізаційних алгоритмів. Застосовуються також й інші підходи, які переважно призначені для багатовимірних об'єктів керування. В роботі розв'язується задача синтезу дискретного одновимірного регулятора для стійкої лінійної моделі довільного порядку з запізненням з застосуванням інженерних математичних пакетів чи іншого спеціалізованого програмного забезпечення. Основна ідея методу – це модифікація класичного регулятора Даліна. Запропонований регулятор має наступні переваги: простота програмної реалізації, відсутність необхідності розв'язку оптимізаційної задачі, висока робастність, можливість врахування усієї динаміки, нескладна процедура налаштування. Проведено дослідження роботи регулятора для типових форм моделей й приділена увага проблемі нейтралізації стрибкоподібних збурень при керуванні об'єктами без самовирівнювання.

Ключові слова: дискретна система автоматичного керування, регулятор Даліна, прямий синтез, робастність, одновимірна, модель високого порядку, запізнення.

Вступ

Проблема синтезу промислових систем керування може бути розв'язана багатьма методами, вибір яких обґрунтовується характером моделі технологічного процесу, технологічними вимогами, ступенем простоти застосування й технічної реалізації, та просто традиціями. Більшість застосувань розглядають керування одновимірними об'єктами керування (ОК) першого чи другого порядку з запізненням за допомогою регуляторів ПІД-типу, чи керування модальними регуляторами ОК високого порядку без запізнення.

З розвитком теорії керування проблема синтезу регуляторів для ОК високого порядку з запізненням стала розв'язуватись за допомогою синтезу багатовимірних регуляторів, що є більш складними з точки зору програмно-технічного реалізації в цифрових системах, ніж регулятори ПІД-типу. В роботі запропоновано метод синтезу одновимірного цифрового регулятора для ОК з запізненням (в т. ч. високого порядку й з домінантним запізненням), який є простим з точку зору програмно-технічної реалізації.

Аналіз літературних джерел

При реалізації ПІД регуляторів в цифровій техніці з'являються додаткові фактори, які методи налаштування, що ставлять задачу в аналоговій формі, як правило не враховують. В роботах [1, 2]проілюстровані основні з них. Це проблеми вибору алгоритму дискретизації складових регулятора, впливу кроку дискретності на якість та стійкість САК, реалізації реального диференціатора та ін. Так, наприклад, для аналогових ПІД-регуляторів І-складова знижує запас стійкості, а Д – збільшує. Для дискретного регулятора при достатньо великому кроку дискретності ситуація може бути прямо протилежною.

Задача синтезу одновимірних САК (як і багатьох інших) – це багатоцільова задача, для якої було розроблено багато критеріїв якості, які частково дублюють один одного. Спрощено їх можливо розбити на дві категорії: швидкість – час наростання (це час, за який вихідна величина ОК зміниться від 10% до 90% сталого значення),процент перерегулювання, час регулювання, інтегральні критерії, та робастність – запас по фазі й по амплітуді, кореневе розташування.

В монографії [3] вперше запропоновано зручний критерій, який оснований на функції чутливості $M_s = \max\limits_{0 \pounds \omega < ¥} \left| \frac{1}{1 + P(j\omega) \times C(j\omega)} \right|$, де P – передаточна функція (ПФ) об'єкта керування, C – ПФ регулятора (оператор s для зручності опустимо).В результаті отримується число, що має бути для ОК з самовирівнюванням в діапазоні від 1.3 до 2 (2.5 в деяких випадках) Чим більше число – тим нижча робастність, оскільки розімкнена система наближується до критичної точки на графіку Найквіста. Також можна наближено отримати величину запасів по фазі й амплітуді. Критерій показує, що в межах стійкої системи швидкість й робастність є базовою дихотомією синтезу САК.

Метод прямого синтезу – один з класичних методів розрахунку. Нехай задано ПФ замкненої одновимірної системи по завданню, тоді регулятор можна описати залежністю.

$$C = \frac{1}{P} \cdot \frac{W}{1 - W}. \tag{1}$$

З першого погляду, виходячи з того, що динаміка багатьох ОК може бути описана лінійним рівнянням високого порядку, то W– це звичайно рівняння високого порядку. І з нього можливо отримати регулятор високого порядку.

Але, якщо ми хочемо отримати ПІ чи ПІД регулятор, то треба спростити задачу до рівняння ОК в вигляді першого порядку. Так, для ОК, що заданий ПФ

$$P = \frac{k_o}{T_o \cdot s + 1}$$

при заданій еталонній ПФ W

$$W = \frac{1}{\lambda \cdot s + 1} \tag{2}$$

виводиться регулятор виду $C = \frac{T_o \cdot s + 1}{k_o} \cdot \frac{1}{\lambda \cdot s} = \frac{T_o}{k_o \cdot \lambda} \cdot \left(1 + \frac{1}{T_o \cdot s}\right)$ що й є ПІ-регулятором $C = k_r \cdot (1 + \frac{1}{T_i \cdot s})$, де $k_r = \frac{T_o}{k_o \cdot \lambda}$, $T_i = T_o$.

Аналогічно, для ОК, що заданий ПФ (FOPDT модель)

$$P = \frac{k_o}{T_o \cdot s + 1} \cdot e^{\tau o \cdot s}$$

можна вивести ПІД-регулятор послідовної форми з реальним диференціатором

$$C = \left(\frac{T_o}{k_o\left(T_r + \tau_o\right)}\right)\left(1 + \frac{1}{T_o \cdot s}\right)\left(\frac{1 + \frac{\tau_o}{2} s}{1 + \left(\frac{T_r}{T_r + \tau_o}\right)\frac{\tau_o}{2} s}\right) \tag{3}$$

Як бачимо, в такій постановці розв'язується задача оптимальності з точки зору категорії «швидкість». Ідеальний перехідний процес при такій постановці має аперіодичний характер й час регулювання, 63.2% якого дорівнює λ. Якщо λ замала, то виникає перерегулювання, а якщо завелика – то САК по якості наближається до ручного управління. Для більшості процесів величина оптимальної λ знаходиться в інтервалі $[T_o, 3 \cdot T_o]$. Справедливим є твердження, що приблизно в цьому діапазоні чим менша швидкість, тим більша робастність (тобто він є певним відображенням M_s).

Тема синтезу регуляторів ПІД-типу найбільш докладно викладена в монографії [4]. Методи налаштування таких регуляторів можливо розділити на 2 класи: інженерні (вимагають в гіршому випадку калькулятора) й комп'ютерні.

Більшість популярних інженерних методів налаштування регуляторів ПІД-типу за моделлю створювались двома способами:

– розв'язок оптимізаційної задачі на комп'ютері за заданим критерієм, побудова номограми, її апроксимація рівняннями (частіше простими);

– модифікація методу прямого синтезу зі зведенням процедури налаштування до простих рівнянь.

Інженерні методи як правило розглядають задачу вибору налаштувань регулятора ПІД-типу за FOPDT моделлю, рідше за SOPDT моделлю (2-го порядку з запізненням).

Оскільки це важливо для огляду, викладемо основні надбання в методах,заснованих на прямому синтезі. Ці методи відрізняються обраним підходом до редукції моделі. В основному є проблема з запізненням: треба розкласти його у ряд Тейлора чи Паде, а також скоротити полюси (якщо це необхідно).

Першим прийнятим промисловим виробництвом методом модифікованого прямого синтезу став IMC-PID, оригінальна версія якого викладена в [5]. Цей метод використовує розкладення в ряд Паде і для FOPDT моделі має два варіанти: для ПІ і ПІД регулятора. Перша версія мала правило $T_i = T_o$, виявилось поганим при керуванні за збуренням. Покращена версія правил розглянута в роботі [6].

$$ПІ: k_p = \frac{T_o + \frac{\lambda}{2}}{k_o \cdot \lambda}, T_i = T_o + \frac{\tau_o}{2}, \lambda = 1.5 \cdot \tau_o (\text{якщо } \tau_o > T_0)$$

$$ПІД: k_p = \frac{T_o}{k_o\left(\lambda \cdot + \frac{\tau_o}{2}\right)}, T_i = T_o + \frac{\tau_o}{2}, T_d = \frac{T_o \cdot \frac{\tau_o}{2}}{T_o + \frac{\tau_o}{2}}, \lambda = 0.7 \cdot \tau_o$$

В цьому, навіть модифікованому, методі виникає різке зниження якості керування для важкокерованих ОК, яке спостерігається й у методів, що побудовані за першим способом [6]. Як показано в роботі [7] застосування апроксимації Паде першого порядку для FOPDT з $\tau_o > T_o$ в методах прямого синтезу призводить до зниження якості керування.

Подальшим розвитком методу IMC-PID став метод SIMC [8] . В цьому методі використовується апроксимація запізнення рядом Тейлора першого порядку. Для FOPDT моделі цей метод дозволяє отримати ПІ-регулятор. Введення обмеження на інтегральну складову виду $T_i = \min(T_o, 4 \cdot (\lambda \cdot + T_0))$ дозволяє значно покращити якість керування за збуренням й важкокерованими ОК, що показано в роботі [6]. Крім того, в порівнянні з IMC-PID розширюється кількість типів ОК внаслідок використання в методі SIMC авторського методу редукції. Метод й надалі покращується, наприклад в роботі [9] запропоновано правило для врахування оригінального, а не апроксимованого при перетворенні SOPDT в FOPDT запізнення, правило для інтегратора 2 порядку з запізнення, фільтр для сигналу завдання.

Серед комп'ютерних методів розглянемо коротко тільки метод, який реалізовано в функції pidtune в Matlab, та запатентовано Math Works [10]. Це частотний метод, який може бути застосований для довільних ОК, в том числі для деяких нестійких. Регулятор задається в вигляді

$$C(s) = \frac{\omega_c}{s}\left(\frac{\sin\phi_z s + \omega_c \cos\phi_z}{\omega_c}\right)\left(\frac{\sin\beta s + \omega_c \cos\beta}{\sin\alpha s + \omega_c \cos\alpha}\right),$$

де ω_c - частота зрізу, яка обирається автоматично чи користувачем, а інші параметри знаходяться шляхом розв'язку оптимізаційної задачі, що включає умови стійкості й намагається досягти величини запасу по фазі в 60°С. Крім того, можливо задати параметр пошуку оптимального регулятора по завданню, збуренню чи компромісного.

Як показано в роботі [6]комп'ютерний метод, реалізований в функції pidtune для FOPDT моделі в цілому не кращій інженерного методу SIMC. Але його істотною перевагою є можливість отримати налаштування для ОК високого порядку. З іншої сторони, якщо модель не може бути з достатньою точністю редукована до FOPDT, то далеко не факт, що цей регулятор буде оптимальним. Це виходить з того, що ПІД – це регулятор обмеженої структури, що не може врахувати динаміку ОК високого порядку. Крім того, при застосуванні частотних критеріїв будуть виникати складності з ОК високого порядку, що мають декілька частот зрізу і, відповідно, декілька запасів по фазі.

Проблему синтезу одновимірних систем для FOPDT моделі з великим запізненням також можна розв'язати з використанням предіктора Сміта (чи однієї з його модифікацій), що досліджено в роботі [6]. В цьому випадку поведінка системи й

процедура її синтезу майже не буде залежати від відношення τ_o / T_o. Але для більшості модифікацій предіктора ОК має бути з самовирівнюванням.

Також регулятор з FOPDT може бути виведено з використанням других методів. Наприклад, в роботі [11] запропонований інженерний метод отримання дискретного регулятора стану з наглядачем для FOPDT моделі. При використанні методу параметри оптимального регулятора стану не залежать від запізнення, а визначаються виключно постійною часу й обраним кроком дискретності. Регулятор дозволяє отримати кращі перехідні процеси за інтегральним квадратичним критерієм і прямими показниками якості у порівнянні з pidtune.

Метод прямого синтезу може бути застосований й для моделей в дискретному часі. Найбільш відомим серед дискретних регуляторів є цифровий аперіодичний регулятор (ЦАР). Для ЦАР бажана z-ПФ замкненої системи дорівнює

$$W = z^{-dk}, dk \geq 1$$

А регулятор отримується за правилом

$$C = \frac{1}{P} \cdot \frac{W}{1-W} = \frac{1}{P} \cdot \frac{z^{-dk}}{1-z^{-dk}} = \frac{1}{P} \cdot \frac{1}{z^{-dk}-1}$$

Для ОК з запізненням величина dk має бути більшою за кількість станів, які виділені для зберігання запізнення в ОК на одиницю. ЦАР розв'язує задачу керування за перший крок, в який подає достатньо великий керуючий вплив, всі інші кроки подається керуючий вплив, що відповідає статиці ОК. По причині значної агресивності керування такі регулятори мають невелику сферу застосування.

Серед модифікацій ЦАР найбільш відомим й придатним для використання є регулятор Даліна [12]. Використовуючи таблиці z-перетворень він виводиться наступним чином. Модель FOPDT представляється наступним рівнянням:

$$P(z) = \frac{k_o \cdot \left(c_1 + c_2 \cdot z^{-1}\right)}{1 - a_p \cdot z^{-1}} \cdot z^{-(k+1)},$$

де $a_p = e^{\left(\frac{-\Delta t}{T_o}\right)}, a = 1 - \left(\tau_o - k_o \cdot \Delta t\right), \quad c_1 = 1 - e^{\left(\frac{-a \cdot \Delta t}{T_o}\right)}, c_2 = e^{\left(\frac{-a \cdot \Delta t}{T_o}\right)} - e^{\left(\frac{-\Delta t}{T_o}\right)}$

Модель еталонної z-ПФ отримується наступним чином і є еквівалентом (2)

$$W(z) = \frac{1 - e^{\left(\frac{-T_o}{\lambda}\right)}}{1 - e^{\left(\frac{-T_o}{\lambda}\right)} z^{-1}} \cdot z^{-\left(\frac{\tau_o}{\Delta t}+1\right)},$$

Тоді регулятор Даліна буде мати вигляд:

$$C(z) = \frac{1}{P(z)} \cdot \frac{W(z)}{1-W(z)} = \frac{(1-a_3) \cdot (1-a_p) \cdot z^{-1}}{k_o[1 - a_3 z^{-1} - (1-a_3) z^{-(k+1)}] \cdot (c_1 + c_2 \cdot z^{-1})}.$$

З першого погляду це регулятор еквівалентний (3), оскільки отримується таким же чином, але не при всіх умовах. Докладний аналіз регулятора Даліна й декількох інших дискретних регуляторів наданий в монографії[13]. Головною проблемою регулятора Даліна, що була розглянута ще її автором [12], є пульсація керуючого впливу, приклад якої показаний на рис. 1.

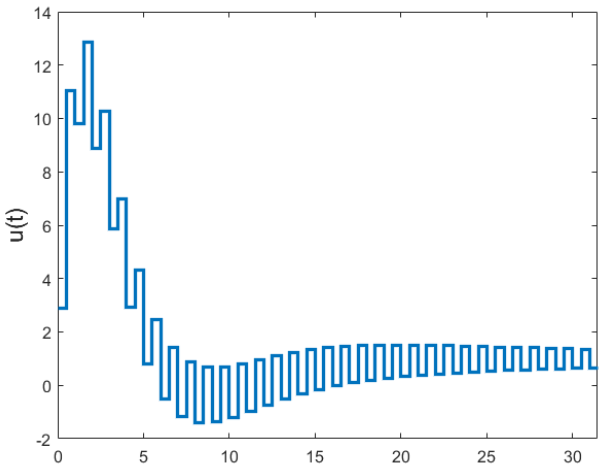

Рис. 1. Приклад пульсації керуючого впливу

Фактична її причина – близькість розміщення полюсів ПФ регулятора до z=-1 в колі з радіусом |z|=1. Далін запропонував вручну підставляти корені z=1 в множники знаменників z-ПФ регулятора, які викликають коливальність. Необхідність застосування такої процедури знижує зручність використання регулятора, хоча якість керування при цьому звичайно не знижується. Аналіз причин пульсації регулятора Даліна проведений в роботі [14], показав, що пульсація не залежить від величини λ.

Подібність регуляторів ПІД-типу, предіктора Сміта й регулятора Даліна доцільно аналізувати тільки для FOPDT моделей. Для об'єктів, що не належать до класу важкокерованих можна говорити про те що, ці регулятори є подібними. В монографії [8] показано, що при застосуванні апроксимації запізнення виду $1-s\cdot\tau_o$, регулятор Даліна можна звести до регулятора (3) без диференційної складової. В роботі [15] вказується, що оскільки в методі прямого синтезу ПІД-регулятора запізнення не може бути враховано без апроксимації, то для ОК, з запізненням, особливо з великим, оптимального керування досягти неможливо. Більш якісне керування буде досягнуто з предіктором Сміта. А якщо предіктор реалізувати в дискретному часі, то він буде аналогічним до регулятора Даліна.

Мета й задачі дослідження

Метою роботи є розробка методу синтезу лінійного дискретного регулятора для одновимірних лінійних ОК довільного порядку й величини запізнення з застосуванням модифікованої еталонної ПФ замкненої системи. Крім того, в роботі розглянута проблема компенсації стрибкоподібних збурень при керуванні за допомогою дискретного регулятора об'єктами без самовирівнювання.

Задача дослідження наступні.

1) Розробити алгоритм синтезу дискретного цифрового одновимірного регулятора для лінійного ОК з запізненням довільного порядку

2) Перевірити працездатність алгоритму для різних типових об'єктів при відхиленні параметрів ОК, різних типах збурень й при обмеженому керуванні.

3) Розв’язати проблему наявності статичної похибки при керуванні за збуренням ОК без самовирівнювання.

Основна частина

Алгоритм, що показаний на рис. . **2**, рекомендовано для синтезу регулятора одновимірного лінійного ОКз запізненням (особливо високого порядку чи/та з великим запізненням) та з самовирівнюванням. Реалізація алгоритму доволі проста в сучасних інженерних математичних пакетах, таких як Matlab.

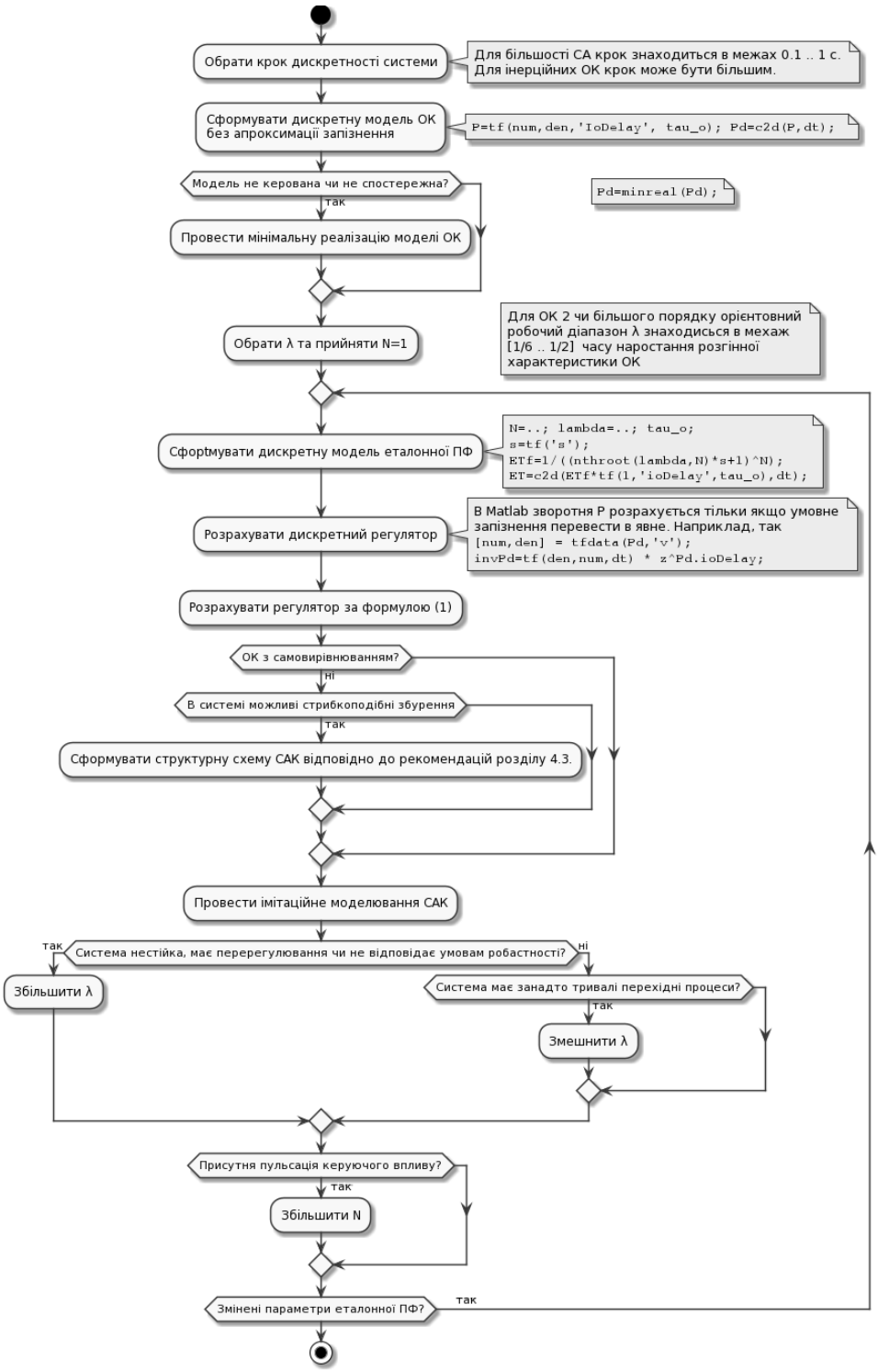

Рис. 2. Алгоритм синтезу дискретного регулятора

В якості еталонної ПФ приймається функція виду

$$W = \left(\frac{1}{\sqrt[N]{\lambda} \cdot s + 1} \right)^N \cdot e^{-\tau_o \cdot s},$$

де N – це цілий коефіцієнт, що компенсує пульсацію керуючого впливу.

Необхідні коментарі показані на рис. **2**.

Спочатку дослідимо якість керування за завданням для типових моделей ОК й ступінь відповідності λ 0.632 часу регулювання САК, а також величину перерегулювання при істотній зміні параметрів ОК;

Дослідимо робастність систем керування з розробленим регулятором.

Перший експеримент проведемо з моделлю FOPDT $P = k_o / (T_o \cdot s + 1) e^{-tau \cdot s} = 1/(10 \cdot s + 1) \cdot e^{-5 \cdot s}$ з номінальним відношенням $\tau / T_o = 0.5$, $\Delta t = 0.5$, N=1, λ=3. Коефіцієнти моделі належать наступним діапазонам $k_o \in [0.5, 1, 1.5], T_o \in [5, 10, 15], \text{tau} \in [2.5, 5, 7.5]$ Результати експерименту при зміні завдання показані на рис. . **3**. Бачимо, що регулятор робастний. Бажаний час (відмічений зіркою) приблизно досягається у всіх випадках. При збільшенні k_o і зменшенні T_o процес перестає бути аперіодичним, хоча перерегулювання не більше 20-30%. Цікаво також, що при відхиленні параметрів ОК величина максимального керуючого впливу майже не змінюється.

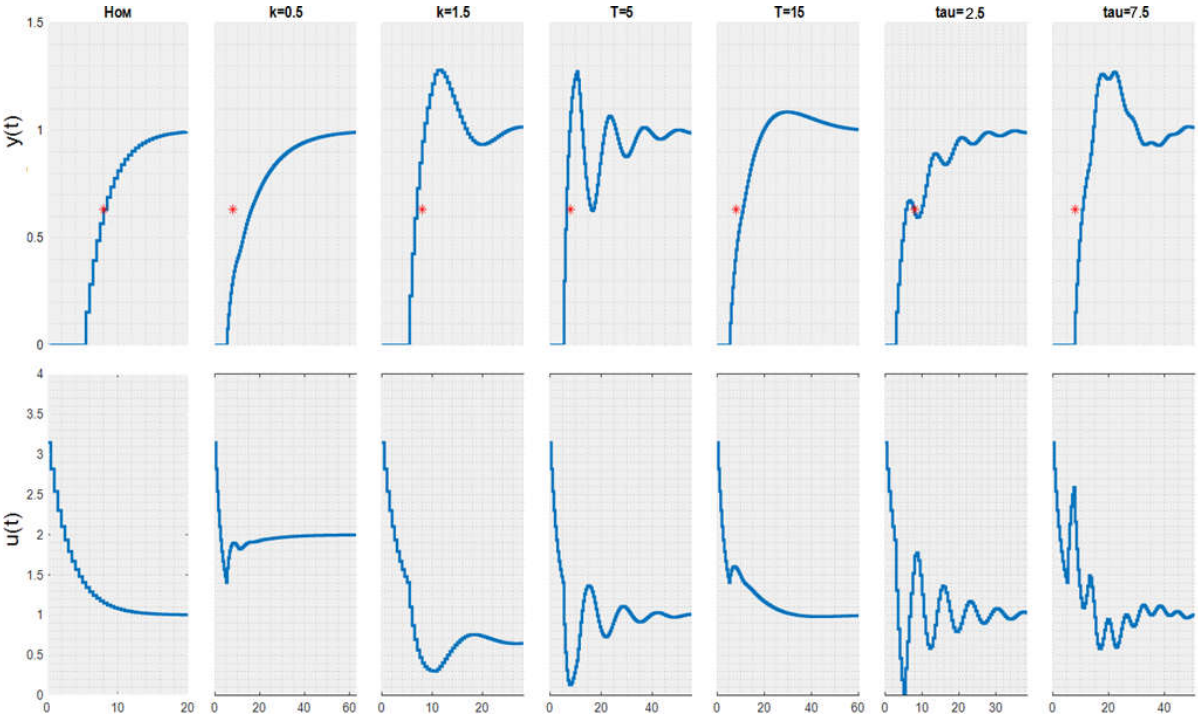

Рис. 3. Дослідження робастності САК з номінальною моделлю $P = 1/(10 \cdot s + 1) \cdot e^{-5 \cdot s}$

Другий експеримент проведемо з моделлю FOPDT $P = 1/(10 \cdot s + 1) \cdot e^{-20 \cdot s}$ з відношенням $\tau / T_o = 2$, $\Delta t = 0.5$, N=1, λ=3. В цьому випадку регулятор дає на першому кроці агресивне керування (починає працювати подібно ЦАР). При відхиленні k_o і T_o на $\pm 50\%$ ПП встановлюється за бажаний час, але з перерегулюванням до 50%. При відхиленні τ_o на ± 10 САК втрачає стійкість. Причина цього в тому, що λ встановлена за межами рекомендації, яка наведена в блок-схемі алгоритму. Час

наростання ОК складає 47.2, тобто λ має бути між 23.6 і 7.87. Отже треба встановити значення λ в рекомендованому діапазоні. Встановимо $\lambda = 15$ й проведемо ще один експеримент.

Третій експеримент проведено для моделі другого експерименту при встановленні λ=15. Результати його показані на рис. . **4**. Коефіцієнти моделі належать наступним діапазонам $k_o \in [0.5,1,1.5]$, $T_o \in [5,10,15]$, $\text{tau} \in [10,20,30]$. Бачимо, що якість ПП процесів за критерієм швидкості висока й робастність САК достатньо висока.

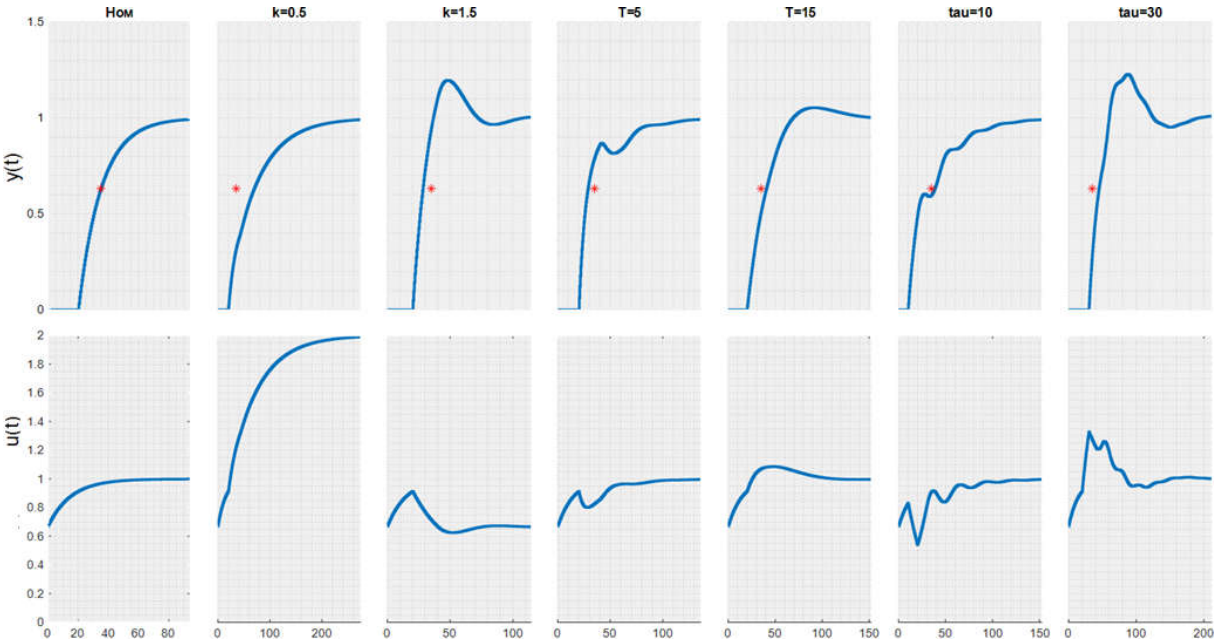

Рис. 4. Дослідження робастності САК з номінальною моделлю $P = 1/(10 \cdot s + 1) \cdot e^{-20 \cdot s}$

Четвертий експеримент проведемо з моделлю SOPDT $P = 1/\left((20 \cdot s + 1)(10 \cdot s + 1)\right) \cdot e^{-10 \cdot s}$ з умовою $\Delta t = 0.5$, N=3, λ=10 (час наростання моделі 51.8). В цьому випадку виникає пульсація керуючого впливу, що для ОК з номінальними параметрами показана на рис. **1**. Тому треба збільшити значення N з 3 до 4 і провести ще один експеримент.

П'ятий експеримент проведений з тією ж самою моделлю, однак при N=4. В цьому випадку пульсація зникає при всіх відхиленнях параметрів ОК. Регулятор дає значний керуючий вплив на початку ПП й швидко досягає бажаного часу. Для зниження величини керуючого впливу треба збільшити λ.

Шостий експеримент проведений з моделлю виду $P = \frac{1}{s} \cdot \frac{1}{10 \cdot s + 1} \cdot e^{-5 \cdot s}$. В цьому випадку регулятор реалізується при умовах $\Delta t = 0.5$, N=4 (менше – виникає пульсація), λ=10. В цілому регулятор працює аналогічно рис. . **3** і . **4**. Максимальний керуючий вплив – біля 0.5.

Сьомий експеримент проведений з моделлю виду $P = \frac{1}{s} \cdot \frac{20 \cdot s + 1}{10 \cdot s + 1} \cdot e^{-10 \cdot s}$. В цьому випадку регулятор реалізується при умовах $\Delta t = 0.5$, N=3 (менше - виникає пульсація), λ=10. В цілому регулятор також працює аналогічно рис. . **3** і . **4**. Максимальний керуючий вплив дорівнює 0.07.

Таким чином, бачимо, що з модифікованою еталонною ПФ процесу можливо спростити синтез регулятора. Якість керування при цьому для розглянутих об'єктів при керуванні за завданням є задовільною. Крім того, на відміну від регуляторів ПІД-типу, в системі з розглянутим регулятором не присутня проблема насичення інтегратора. В той самий час інтегратор може й не компенсувати статичну похибку, що проявляється при збуренні стрибком по входу ОК в експериментах №6 і №7 (рис. . **5**). Ця похибка не компенсується інтегратором, тому ПП встановлюються на близьких значеннях керованих змінних як при наявності обмеження керування, так і без нього.

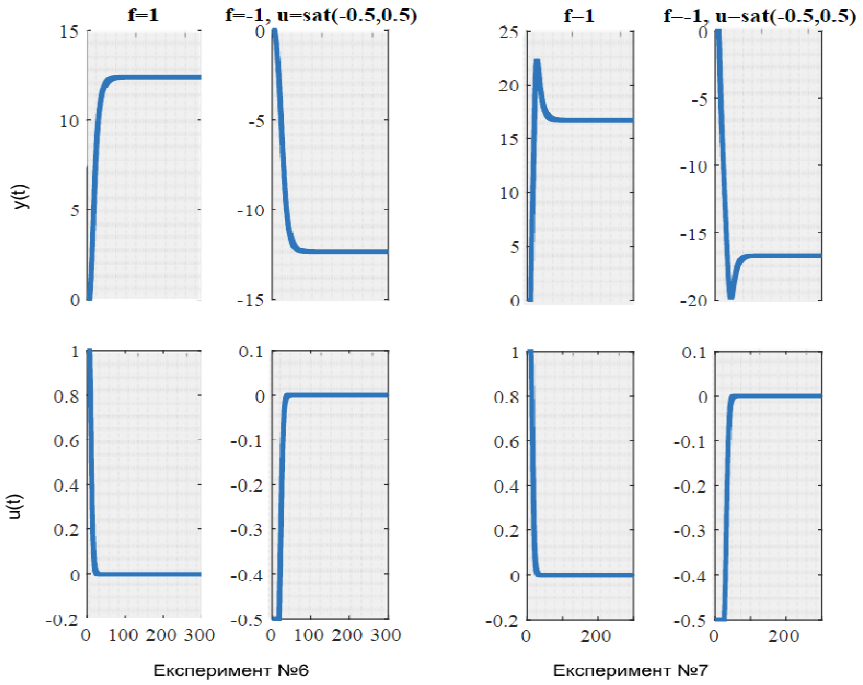

Рис. 5. Статична похибка в ПП при збуренні стрибком

Для подолання невідомого стрибкоподібного збурення на вході пропонується схема САК, що показана на рис. . **6**.

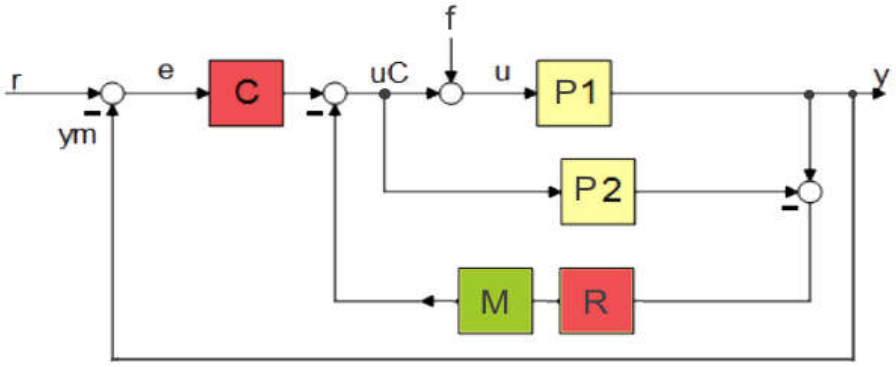

Рис. 6. Структурна схема САК для подолання стрибкоподібних збурень для ОК без самовирівнювання

На схемі P_1 – реальний об'єкт керування (для моделювання – його точна модель), P_2 – теоретична модель ОК. В випадку збурення стрибком по входу запропонованій схемі робиться спроба звести сигнал, що йде на суматор після регулятора до постійного. Сигнал P_1–P_2 є інтегральним, тому щоб його перетворити до

стрибкоподібного він проходить через диференціатор виду $R = \dfrac{s}{3 \cdot \tau_o \cdot s + 1}$. Параметр блоку М обирається за правилом $M = \dfrac{1}{k_o}$.

Математична модель в Simulink САК для ОК з сьомого експерименту показана на рис. 7 і 8.

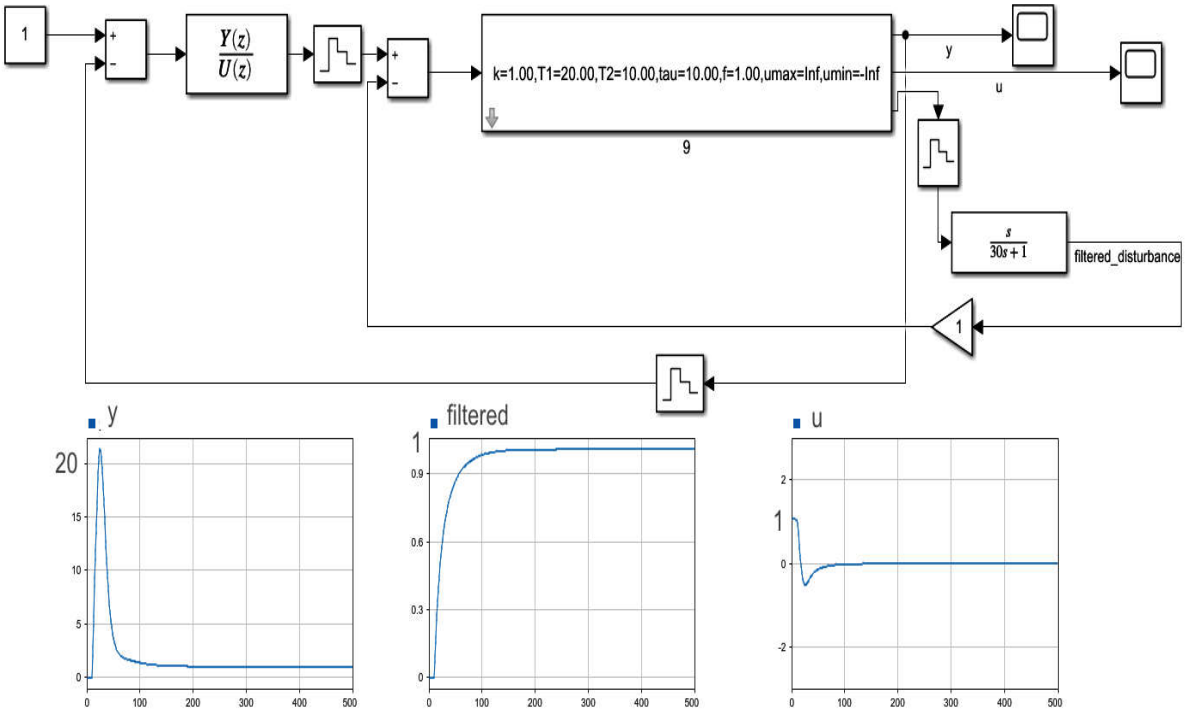

Рис. 7. Simulink модель САК для подолання стрибкоподібних збурень для ОК без самовирівнювання

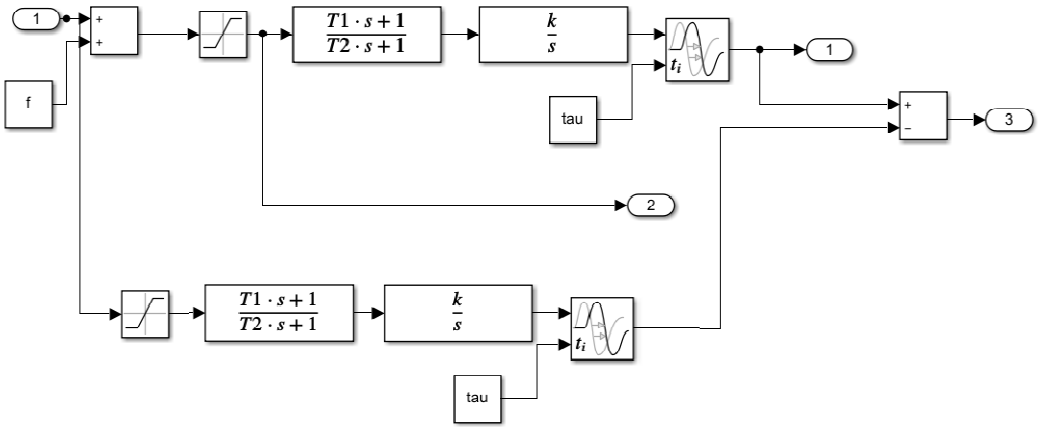

Рис. 8. Simulink модель блоку підсистеми моделі, показаної на рис. 7

Основою моделі є блок підсистеми, що має один вхід й три виходи. 1-й вхід – керуючий вплив регулятора, 1-й вихід - керована змінна з "реального" ОК, 2-й вихід – обмежений керуючий вплив зі збуренням по входу (при наявності), 3-й вихід – різниця

між виходом "реального" ОК й його теоретичної моделі. На рис. **7** показано, що при такій структурі регулятор подолав збурення й статична похибка відсутня.

Перехідний процес по завданню при зміні τ_o «реального об'єкту» з10на 15(рис. . **9**) показує, що регулятор діє також як й регулятор в звичайній замкненій САК при відхиленні параметру моделі. Компенсаційний сигнал фільтра в цьому випадку знаходиться в зоні ± 0.01.

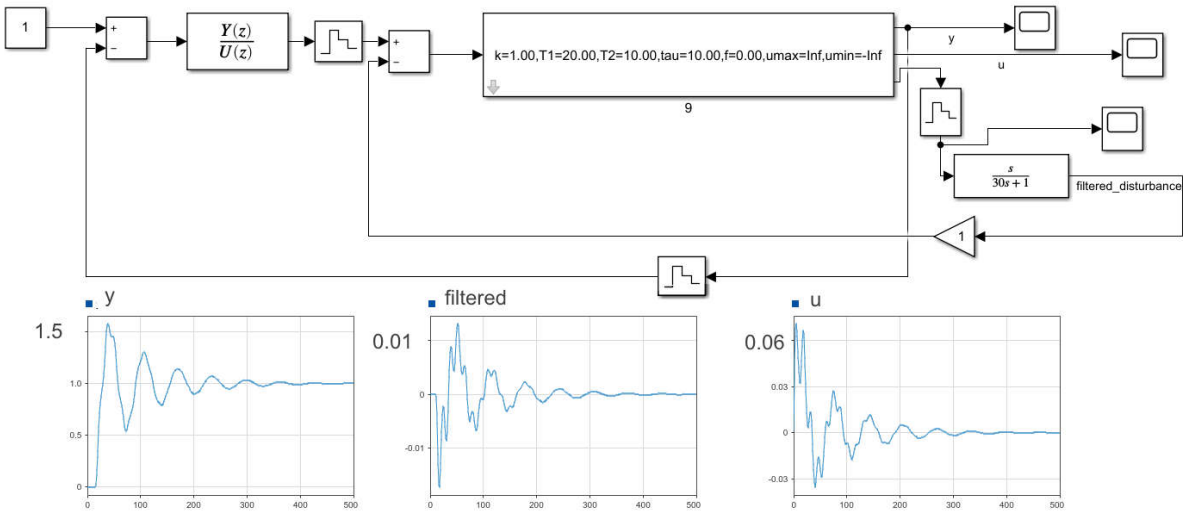

Рис. 9. Simulink модель САК для подолання стрибкоподібних збурень для ОК без самовирівнювання й перехідні процеси по завданню при невідповідності часу запізнення реального об'єкту часу запізнення, що закладено в модель дискретного регулятора.

Висновки

Розроблено алгоритм синтезу дискретного регулятора, оптимального за часом перехідного процесу за завданням, який включає:

- модифіковану передатну функцію еталонного перехідного процесу;
- рекомендацію по інтервалу пошуку бажаного часу перехідного процесу;
- структуру САК й методи налаштування додаткових елементів в ній для розв'язку проблеми виникнення статичної похибки в об'єктах керування без самовирівнювання.

Для наладчика системи автоматизації алгоритм може бути зручним при його програмній реалізації не тільки в межах інженерного математичного пакета, а й, наприклад мовою Python [16], яка містить всі необхідні бібліотеки. Така програма дозволить користувачу задавати бажаний час ПП й модель об'єкту керування. Коефіцієнт N може бути знайдений автоматичним пошуковим алгоритмом.

Список літератури

1. Laskawski M., Wcislik M. Influence of sampling on the tuning of PID controller parameters. *IFAC-Papers On Line.* 2015. №48-4. P. 430 – 435.
2. Tomov L., Garipov E. Choice of sample time in digital PID controllers. Recent. 2007. №2(20). V. 8. P. 169 –178.
3. Aström K., Hägglund T. PID Controllers: Theory, Design, and Tuning (2nd Edition). Research Triangle Park, NC: Instrument Society of America. 1995. (16)

4. O'Dwyer A. Handbook of PI and PID controller tuning rules (3rd edition). London: Imperial Colledge Press, 2009.
5. Rivera D.E., Morari M., Skogestad S. *Ind. Eng. Chem. Process Des. Dev*. 1986.№25, P. 252-265.
6. Стопакевич А.А. Проектирование робастных регуляторов объектами с большим запаздыванием. *Восточно-европейский журнал передовых технологий.* №2 (79). Т. 1, 2016. С. 48-56.
7. Pathiran A., Prakash J. A Comparative Study on the Well-Known Feedback Controller Design Methods. *2017 Trends in Industrial Measurement and Automation (TIMA)*. Chennai*, 6-8Jan 2017*.
8. R. Vilanova, A. Visioli (eds.). PID Control in the Third Millennium, Advances in Industrial Control. London: Springer-Verlag, 2012.
9. Lee J., Cho W., Edgar T. Simple Analytic PID Controller Tuning Rules Revisited *Ind. Eng. Chem. Res.* 2014, №53, V. 13, P. 5038–5047.
10. Eryilmaz P., Automated PID controller design, pat. US8467888B2, 2013. URL: https://patents.google.com/patent/US8467888.
11. Stopakevych A., Stopakevych O., Tigariev A., Tigarieva T. A simple method for a precise solution of the digital optimal controllers design problem for SISO objects with delay. Наукові праці ОНАЗ ім. О. С. Попова, 2019, №2. P. 104-114.
12. Dahlin E.B. Designing and tuning digital controllers. *Instruments and control systems.* 1968, №41 (6). P. 77-84.
13. Кваско М., Піргач М. Аверіна Т. Проектування і дослідження дискретних систем автоматичного керування технологічними процесами. Київ: Політехніка, 2003.
14. Zhang W., Sun Y., Xu X. Robust digital controller design for processes with dead times: New results. *IEE Proc.-Control Theory Appl.* Vol. 145. No. 2, March 1998. C. 159-164.
15. Weidong Z. Xing X., Xiaoming X. Comparison of several well-known controllers used in process control. *ISA Transactions*. 2003, № 42. P. 317–325.
16. Стопакевич А. О., Стопакевич О. А., Тігарєв А. М., Тігарєва Т. Г. Розробка автономних web-сервисів для імітаційного моделювання динамічних систем в реальному часі на базі моделей MATLABSimulink. *Автоматизація технологічних і бізнес-процесів*, 2020. №12(4), С. 21-29.

DISCRETE TIME CONTROLLER SYNTHESIS WITH THE DESIRED SYSTEM TRANSIENT TIME

A. O. Stopakevych, O.A. Stopakevych

Odessa National Academy of Telecommunications, 14, Kuznechna,
Odessa, 65029, stopakevich@gmail.com
Odessa National Polytechnic University, 1, Shevchenko Ave.,
Odessa, 65044, stopakevich@opu.ua

The actual standard for industrial technological processes and many other branches of automation is the PID-type controller. The problem of synthesis of such controllers has been studied in the literature in sufficient detail. The advantage of such controllers, which influenced on its wide popularity, is that it is a controller in which the automation system tuner can empirically change the numerical coefficients (from 1 to 4 depending on the controller type), based on the direct criteria of transient quality: the maximum deviation, overshoot, setting time, as well as on signs of instability. The problem of optimal synthesis of the PID-type controller based on typical models can be generally considered as solved. With the development of computer techniques and engineering mathematical software, the problem of synthesis of the optimal PID-type controller for any control object is solved by combining frequency criteria and optimization algorithms. Other approaches are also used, which are mainly designed for multivariable control objects. This paper solves the problem of synthesis of a discrete SISO (Single Input and Single Output) controller for a stable linear model of arbitrary order with dead time using engineering mathematical software. The main idea of the method is a modification of the classical Dahlin controller. The proposed controller has the following advantages: simple software implementation, no necessity to solve the optimization problem, high robustness, possibility to take into account all dynamics, and simple tuning procedure. A study of the controller's operation for typical forms of models was carried out and attention was paid to the problem of neutralization of stepwise disturbances when controlling integrating plants.

Keywords: Discrete automatic control system, Dahlin controller, direct synthesis, robustness, SISO controller, high-order model, dead time, delay.

DOI 10.15276/imms.v10.no 3-4.222
УДК 004.946.5:519.81

Informatics and Mathematical Methods in Simulation
Vol. 10 (2020), No. 3-4, pp. 222-229

ВИКОРИСТАННЯ ТЕОРІЇ ІГОР ПРИ АНАЛІЗІ ГІБРІДНИХ ВІЙН

В.О.Хорошко[1], М.М. Браіловський[2]

[1]Національний авіаційний університет, пр. Любомира Гузера, 1, Київ, 03058, Україна;
e-mail: professor_va@ukr.net
[2]Київський національний університет імені Тараса Шевченка, вул. Богдана Гаврилишина, 24, Київ, 04116
Україна, e-mail: bk1972@ukr.net

Проблеми зміни геополітичної обстановки в світі, бажання провідних країн отримати нові або зміцнити наявні сфери впливу, а інших країн зберегти або повернути свої колишні позиції призводить до застосування більш нових методів гібридної війни. Одна з методик оцінки ризику для інформаційного простору (мережевої системи) – це ймовірність атаки на неї. Оцінка безпеки інформаційного простору визначається величинами взаємодії атакуючих і оборонних сторін. Виникає запитання необхідності оцінки та прогнозу дій як оборонної сторони, так і атакуючої. Процес взаємодії між атакуючою та оборонною сторонами можна розглядати як ігровий процес. Розуміючи під грою - процес стратегічної взаємодії між ворогуючими або співпрацюючими гравцями в умовах певних обмежень і плану їх дій. Виходячи з такої інтерпретації гри, пропонується засновані на теорії ігор рішення проблем гібридної війни, прогнозування дій атакуючої сторони, визначення рішень оборонної сторони. Як і в будь-якої теорії в галузі прикладної математики, теорія ігор задає деяку формальну структуру. Приймається, що всі можливі дії кожного гравця можуть бути точно встановлені і що для кожної комбінації таких дій очікуваний результат змагання може бути визначений чисельно. Метою кожного гравця є максимізація свого очікування виграшу. Гравець може припускати, що кожен з його суперників зайнятий аналогійною оптимізацією. В роботі розглянуті різні можливі ситуації взаємодії між атакуючою та стороною, що захищається. Наведені функціональні вирази, дозволяють визначити оптимальні стратегії протиборчих сторін і знайти гарантований максимальний рівень вартості атаки. Запропоновано методи вирішення цих виразів. Зокрема, до них відносяться: методи зведення матричних і безперервних ігор до задач лінійного програмування, методи відомості безперервних ігор до матричних ігор, алгоритми наближеного рішення безперервних ігор методом випадкового пошуку, а також методи моделювання ігор.

Ключові слова: гібридна війна, теорія ігор, прогноз дій, оптимізація дій.

Вступ

Безпека інформаційного протиборства стає все більш складною темою, оскільки численні нові мережеві атаки, що набувають характеру гібридності, стають все більш витонченими і призводять до величезних втрат. Сформувалися такі області злочинів, як кіберзлочинність та кібервпливу, які вимагають найпильнішої уваги через поширення комп'ютерів як інструменту життєзабезпечення в різних областях людської діяльності.

При цьому, слід зазначити таке. З одного боку, слабкість традиційних рішень для мережевої безпеки, в умовах гібридної війни, полягає у відсутності в них системи кількісних рішень [1].

З іншого боку, оцінка безпеки [2], є важливим аспектом безпеки інформаційного простору: це оцінка конфіденційності, цілісності, доступності, уразливості і ризиків безпеки. Оцінка просторової безпеки - це категорія, яка включає визначення кожного аспекту просторової і мережевої безпеки. Оцінка ризику [3] є однією з таких заходів. Оцінка безпеки інформаційного простору і мережі включає взаємодії атакуючих і оборонних сторін на результати оцінки і визначення впливу оцінки на їх взаємодії. Наприклад, одна з методик оцінка ризику для інформаційного простору (мережевих

систем) - це ймовірність її атаки. Необхідно оцінити і передбачити дії як оборонної сторони, так і атакуючої. Процес взаємодії між атакуючою та стороною, що обороняється можна розглядати як ігровий процес. Розуміючи під грою - процес стратегічної взаємодії між ворогуючими або співпрацюючими гравцями в умовах певних обмежень і плану їх дій. Виходячи з такої інтерпретації гри, досить часто пропонується засновані на теорії ігор вирішення проблем гібридної війни, прогнозування дій атакуючої сторони, визначення рішень оборонної стороною.

Як і в будь-якій теорії в галузі прикладної математики, теорія ігор задає деяку формальну структуру. Приймається, що всі можливі дії кожного гравця можуть бути точно встановлені і що для кожної комбінації таких дій очікуваний результат змагання може бути визначений чисельно. Метою кожного гравця є максимізація свого очікування виграшу. Гравець може припускати, що кожен з його суперників зайнятий аналогійною оптимізацією [4].

Основна частина

Розглянемо наступну багатокрокову конфліктну ситуацію між атакуючою стороною C_1 і стороною, що обороняється C_2 [1]. Сторона C_1 має n_2 типів атакуючих засобів і може використовувати їх будь-яким з наявних у її розпорядженні n1 способів. Вибір типів атакуючих засобів і тактичних прийомів здійснюється незалежно на кожному кроці атаки. Сторона C_2 має життєво важливі об'єкти оборони (мета), M засобів оборони і Ц центрів управління обороною, кожен з яких здатний одночасно керувати діями не більше ρ засобів оборони. Оборонні акції сторона C_2 робить на кожному кроці атаки боку C_1 шляхом виділення m1 і m_2 оборонних засобів, взаємодіючих із засобами атаки до і після нанесення ними удару об'єкта боку C_2.

Об'єктами атаки є цілі і керуючі центри. Атака складається з послідовних кроків, що закінчуються, або в момент виснаження засобів нападу, або, коли сторона C_2 знищена. На кожному кроці атаки сторона C_1 може використовувати тільки один атакуючий засіб. Сторона C_2 для захисту цілей та керуючих центрів виділяє m1 оборонних засобів, а для знищення повернутих методів атаки виділяє m2 оборонних методів. З урахуванням керуючої здатності центрів Ц маємо такі обмеження на m_1 і m_2

$$m_1 = 0,1,2,...,\min\left[M, \sum_{t\in Ц} \rho_i\right],$$

$$m_2 = 0,1,2,...,\min\left[M - m_1, \sum_{t\in Ц} \rho_i\right].$$

Припустимо, що атакуючий пристрій *i*-го типу вартістю $a_к$ при використанні *j*-го методу атаки не досягає мети з ймовірністю $\rho_{jk}(m_1)$ і не повертається в бік C_1 з ймовірністю $\rho^*_{jk}(m_2)$. Нехай ймовірність того, що атакуючий метод знищить *min (I,S$_{jk}$)* цілей буде дорівнювати τ_{jk}, а ймовірність знищення *min (Ц,S'$_{jk}$)* керуючих центрів дорівнює τ'_{jk}.

Мета сторін C_1 і C_2 полягає у тому, щоб мінімізувати і максимізувати очікувану вартість атаки. Нехай $f_I(I, Ц, M)$ та $f_Ц(I, Ц, M)$ є очікування значення вартості атаки на одному кроці для мети і керуючих центрів відповідно. Тоді, використовуючи принцип оптимальності [6], отримаємо наступний вираз:

$$f_I\left(I,Ц,M\right)=\min_{j,k}\max_{m_1m_2}\{a_k\left[\rho_{jk}\left(m_1\right)+q_{jk}\left(m_1\right)\cdot\rho^*_{jk}\left(m_2\right)\right]+f\left(I,Ц,M-m_1\right)\rho_{jk}\left(m_1\right)+$$
$$+f\left(I,Ц,M-m_1-m_2\right)q_{jk}\left(m_1\right)\left(1-\tau_{jk}\right)+f\left[I-\min\left(I,S_{jk}\right),C,M-m_1-m_2\right]q_{jk}\left(m_1\right)\tau_{jk}\}; \quad (1)$$

$$f_Ц\left(I,Ц,M\right)=\min_{j,k}\max_{m_1m_2}\{a_k\left[\rho_{jk}\left(m_1\right)+q_{jk}\left(m_1\right)\cdot\rho^*_{jk}\left(m_2\right)\right]+f\left(I,Ц,M-m_1\right)\rho_{jk}\left(m_1\right)+$$
$$+f\left(I,Ц,M-m_1-m_2\right)q_{jk}\left(m_1\right)\left(1-\tau_{jk}\right)+f\left[I,Ц-\min\left(Ц,S_{jk}\right),M-m_1-m_2\right]q_{jk}\left(m_1\right)\tau'_{jk}\}; \quad (2)$$

де $f(I,Ц,M)=\min\left\{f_I(\mathrm{I},Ц,\mathrm{M}),f_Ц(\mathrm{I},Ц,\mathrm{M})\right\}$,
$q_{jk}(m_1)=1-\rho_{jk}(m_1)$.

Функціональний вираз (1) та (2) дозволяють визначити оптимальні стратегії сторін C_1 і C_2 і знайти гарантований максимальний рівень вартості атаки. При цьому необхідно враховувати очевидні умови:

$$f(0,Ц,M)=0, \quad (3)$$

$$f_I(\mathrm{I},Ц,M)=f(\mathrm{I},\mathrm{C},0)=0. \quad (4)$$

Насправді, якщо I = 0, то сторона C_2 вже знищена, стороні C_1 не потрібно витрачати кошти нападу. При M = 0 сторона C_2 може використовувати лише одну наявну в її розпорядженні стратегію оборони $m_1 = m_2 = 0$, а тому сторона C_1 може атакувати сторону C_2 тільки спеціальними засобами. Якщо ж сторона C_1 має засіб нападу тільки одноразового використання, то при M = 0, опираючись на вираз (1) $\rho_{jk}=0,\ \rho^*_{jk}=1$, маємо:

$$f(\mathrm{I},Ц,0)=\min\left\{a_k+f(I,Ц,0)(1-\tau_{jk})+f\left[I-\min(I,S_{jk}),Ц,0\right]\tau_{jk}\right\}. \quad (5)$$

Рівняння (5) не залежить від Ц і може бути вирішено з урахуванням умови (3).

І нарешті, при Ц = 0 сторона C_2 втрачає здатність керувати обороною, що еквівалентно нагоди M = 0. Аналогічно (5) маємо:

$$f(\mathrm{I},Ц,0)=\begin{cases}0,\ \textit{при атаці засобами багаторазового використання}\\ \min\left\{a_k+f(I,Ц,0)(1-\tau_{jk})+f\left[I-\min(I,S_{jk}),Ц,0\right]\tau_{jk}\right\},\ \textit{при атаці}\\ \textit{засобами одноразового використання}\end{cases} \quad (6)$$

У деяких випадках загальні функціональні вирази (1) і (2) можна спростити. Зокрема, якщо напад сторони C_1 на сторону C_2 здійснюється тільки системами разового використання або багаторазового використання, а сторона C_2 може оборонятися тільки перед атакою, то, опираючись на вираз (1) і (2) $m_2=0$, отримуємо такі функціональні рівняння.

При нападі засобами багаторазового використання маємо:

$$f_I\left(I,Ц,M\right)=\min_{j,k}\max_{m_1}\{a_k\rho_{jk}\left(m_1\right)+f\left(I,Ц,M-m_1\right)\left[1-q_{jk}\left(m_1\right)\tau_{jk}\right]+$$
$$+f\left[I-\min\left(I,S_{jk}\right),C,M-m_1\right]q_{jk}\left(m_1\right)\tau_{jk}\},$$

$$f_Ц\left(I,Ц,M\right)=\min_{j,k}\max_{m_1}\{a_k\rho_{jk}\left(m_1\right)+f\left(I,Ц,M-m_1\right)\left[1-q_{jk}\left(m_1\right)\tau'_{jk}\right]+$$
$$+f\left[I,Ц-\min\left(I,S'_{jk}\right),M-m_1\right]q_{jk}\left(m_1\right)\tau'_{jk}\}.$$

Для застосування засобів разового використання:

$$f_I\left(I,Ц,M\right)=\min_{j,k}\max_{m_1}\{a_k\rho_{jk}\left(m_1\right)+f\left(I,Ц,M-m_1\right)\left[1-q_{jk}\left(m_1\right)\tau_{jk}\right]+$$
$$+f\left[I-\min\left(I,S_{jk}\right),\text{Ц},M-m_1\right]q_{jk}\left(m_1\right)\tau_{jk}\},$$

$$f_Ц\left(I,Ц,M\right)=\min_{j,k}\max_{m_1}\{a_k+f\left(I,Ц,M-m_1\right)\left[1-q_{jk}\left(m_1\right)\tau^{є}_{jk}\right]+$$
$$+f\left[I,Ц-\min\left(I,S'_{jk}\right),M-m_1\right]q_{jk}\left(m_1\right)\tau'_{jk}\}.$$

Початкові умови (3) – (6) залишаються при цьому без змін.

Питання вирішення виразів (1) і (2) пов'язані з використанням різних методів. Зокрема, до них відносяться: методи зведення матричних і безперервних ігор до задач лінійного програмування [7,8], методи відомості безперервних ігор до матричних ігор [9], алгоритми наближеного рішення безперервних ігор методом випадкового пошуку [10], а також методи моделювання ігор [11].

Між матричними і безперервними іграми та завданнями лінійного програмування існує найтісніший зв'язок [7,12]. Останні можуть бути вирішені одним з добре відомих методів [12,13,14]: симплекс-методом, методом послідовного поліпшення плану, методом послідовного уточнення оцінок або методом послідовного скорочення неоднозначностей.

У тих випадках, коли для даного класу гри не існує регулярного методу визначення оптимальних стратегій і вартості гри, можна скористатися методом моделювання ігор. Серед різних підходів до моделювання ігор найбільш перспективними є: імітування гри шляхом використання імітуючих моделей ігор, побудова штучних стохастичних моделей гри (метод Монте-Карло) і безпосереднє розігрування партій гри з метою отримання переваги.

Використання сучасних засобів обчислювальної техніки дозволяє без особливих труднощів визначити оптимальні стратегії поведінки сторін в ситуації «напад-оборона».

Для практичних застосувань теорії ігор характерним є наявність ситуації не суворого антагоністичного характеру. Ігрові моделі таких ситуацій вивчаються теорією біометричних і коаліційних ігор. При цьому виникають завдання вимірювання та обліку характеру взаємовідносин сторін [15].

Розглянемо нормальну форму гри: G(I): сторона $i \in I = (1,2,..,n)$у дискретні моменти часу t=0,1,2… вибирає стратегії $\chi_s^{(i)}$ у просторі $X_i = \left\{\chi_s^{(i)}; 1 \le S \le m_i\right\}$, у випадку вибору точки сторона *i* отримує виграш, який оцінюється функцією $M^{(i)}(\chi, t)$.

$$\chi = \left(\chi^{(1)}, \chi^{(2)}, ...\chi^{(n)}\right) \hat{I} X = \prod_{i\hat{I}I} X_i$$

Через те, що функції сторін залежать від часу, то взаємини сторін з часом можуть змінюватися. Отже, в кожний момент часу коаліційна структура гри *G(I)* буде характеризуватися певними взаємовідносинами сторін. Для вимірювання цих взаємин в роботі [15] було введено поняття шкали напруженості конфлікту *H(t),* а також поняття ступеня, кооперування b_{ij} сторони *i* зі стороною *j*. При цьому негативні значення $b_{ij}(t)$ розуміються як ступінь конфлікту.

В результаті відношення боку *i* до всіх інших сторін безлічі I можна визначити вектором $b_i = \{b_{i1}, b_{i2}, \dots, b_{in}\}$, який буде називатися стратегією переваги сторони *i*. Таким чином, вся гра характеризується матрицею

$$B_t = \left\| b_{ij}(t) \right\| \tag{7}$$

де $b_{ij}(t)$ – є характеристика відносин сторони $i_к$ власним інтересам.

Абсолютні значення b_{ij} характеризують ступінь симпатій або ворожнечі боку *i* до сторони *j*. У загальному випадку $b_{ij} \neq b_{ji}$, тобто, відносини сторін можуть не відрізнятися повною взаємністю, а прагнення до об'єднання зусиль може бути неоднаково сильним. Іншими словами, відносини конфлікту або кооперація не обов'язково симетричні: сторона *i* може конфліктувати зі стороною *j*, в той час як сторона *j* кооперується зі стороною *i*. Такі ситуації особливо характерні для соціальних систем.

Нехай $A_t^{(i)} = \{j: b_{ij} > 0\}$ и $B_t^{(i)} = \{j: b_{ji} > 0\}$, тоді коаліція N_t, в яку хотіла б в момент *t* входити сторона *i*, може бути визначена умовою:

$$N_t^{(i)} = A_t^{(i)} \bigcap B_t^{(i)}. \tag{8}$$

Можливість же освіти цієї коаліції визначається виконанням співвідношення

$$\bigcap_{S \in N_t^{(i)}} N_t^{(i)} \bigcap A_t^{(S)} = N_t^{(i)}. \tag{9}$$

Розглянемо випадок, коли в якості шкали напруженості обрана упорядкована сукупність {H} станів гри G (I). Причому, припустимо, що задані ймовірності переходу $p_{ij}(B)$ зі стану H_i до стану H_j. Завдання полягає в тому, щоб стороні *i* вибрати таку стратегію переваги b_i, яка б максимізувала ймовірність:

$$P_i(b_1, b_2, ..., b_n) = P\left\{H \in \Theta_i = \bigcup_{j \in G_i} H_i / G_i\right\} = \left\{j : M^{(i)}(H_j, t) \ge M^{(i)}(H_l, t),\ (l = 1, 2, ..., \tau)\right\},$$

де τ – число можливого стану гри G(I): $M^{(i)}(H_l, t) = \sum_{\chi \in H_l} M^{(i)}(\chi, t)$.

Отже, стійка стратегія переваги b_i^0 боку *i* буде визначатися рівністю:

$$P_i(b_i^0) = \max_{b_i} \min_{\{b_i\}_{j\neq i}} P_i(b_1, b_2, \ldots, b_n)$$

де – мінімум береться по всім сторонам матриці B, за винятком *i*-й сторони, по якій шукаємо мінімум. Очевидно, що якщо хоча б одна зі сторін безлічі I не є противником боку *i*, то значення $P_i(b_i^0)$ може тільки збільшуватися, тобто .$P_i(b_i^0)$ є нижня оцінка ймовірності $P_i(b_1, b_2, \ldots, b_n)$ для сторони *i*.

Отже, справедлива наступна теорема.

Теорема. Гра G(I) в момент часу *t=k* в інтервалі$0 \leq t \leq m$ має оптимальну структуру $\tau_k = \left\{N_t^{(i)}\right\}$, де коаліція $N_t^{(i)}$визначаєтьсяумовою (8) та (9), а матриця B визначається з розв'язку рівняння:

$$P_j^0(k,s) = \max_{b_i(t)} \min_{\{b_j(t)\}_{j\neq i}} \sum_{j=1}^{\tau} P_{sj}(B) P_i^0(k+1, j) \tag{10}$$

де $P_{s_j}(B) = P_{s_j}[b_1(k), b_2(k), \ldots, b_n(k)]$ - ймовірність переходу зі стану H_s до стану H_j в момент *i=k*, залежної від стратегій переваги сторони з безлічі I.

Розв'язання рівняння (10) знаходиться при початковій умові

$$P_i^0(\mathrm{m}, s) = \begin{cases} 1 \ \textit{при}\ H_s \in \Theta_i \\ 0 \ \textit{при}\ H_s \notin \Theta_i \end{cases}$$

Нехай$P_i(k,s,B)$єймовірність того, що при потраплянні на *k*–м кроків перейде в стан H_s гра за решту *m-k* кроків перейде у стан Θ_i, бажано для сторони *i*:

$$P_i(\mathrm{k,s,B}) = P\left\{H(m) \in \Theta_i / H(k) \in H_S\right\}$$

За формулою повної ймовірності маємо

$$P_i(\mathrm{k,s,B}) = \sum_{j=1}^{\tau} P_{sj}(B) P_i(k+1, j, B). \tag{11}$$

При *k=m-1*отримаємо

$$P_i(\mathrm{m,j,B}) = \begin{cases} 1 \ \textit{при}\ H_j \in \Theta_i \\ 0 \ \textit{при}\ H_j \notin \Theta_i \end{cases}$$

Отже

$$P_i(m-1, s, B) = \sum_{j: H_j \in \Theta_i} P_{sj}(B) \tag{12}$$

З виразу (10) и (12) маємо

$$P_i^0(m-1, s) = P_i(m-1, s, \mathrm{B}^0) = \max_{b_i(t)} \min_{\{b_j(t)\}_{j\neq i}} P_i(m-1, s, \mathrm{B}) \tag{13}$$

Маючи на увазі (11) *k=m-2,* с врахуванням формули (12) маємо

$$P_i(m-2,s,B)=\sum_{j=1}^{\tau}P_{sj}(B)P_i(m-1,j,B)=\sum_{j=1}^{\tau}P_{sj}(B)\sum_{j:H_l\in\Theta_i}P_{sl}(B)=\sum_{j=1}\sum_{l:H_j\in\Theta_i}P_{sj}(B)P_{sl}(B) \qquad (14)$$

Нехай в (14) до функції матриця B вибрана з умови (13). Тоді ймовірність $P_i(m-2,s,B)$ буде найменшою, а тому можна записати рівність:

$$P_i(m-2,s,B)=\sum_{j=1}^{\tau}P_{sj}(B)P_i^0(m-1,j)\,.$$

Аналогічно отримаємо $P_i^0(m-2,s)=\max\limits_{b_i(t)}\min\limits_{\{b_j(t)\}_{j\neq i}}\sum\limits_{j=1}^{\tau}P_{sj}(\mathrm{B})\,\mathrm{P}_i^0(m-1,j)$.

Продовжуючи ці міркування, отримаємо функціональне рівняння (10) для визначення стійких стратегій переваги. Цим теорема доведена.

Висновки

В роботі запропоновано підхід до оцінки безпеки інформаційного простору в інформаційному протиборстві сторін в гібридній війні. Наведено методику оцінки безпеки інформаційного простору, яка визначається величинами взаємодії і передбачення дій атакуючих і оборонних сторін. Процес взаємодії між атакують і обороняються сторонами розглянуто як ігровий процес. Сформульовано і доведено теорему, що дозволяє знайти рішення гри G(I), оптимальне в розумінні гарантування мінімуму виграшу для кожної сторони безлічі I.

При цьому, збільшення оцінок виграшів може бути досягнуто за рахунок урахування додаткової функції про взаємини сторін.

Список літератури

1. Alpcan T., Baser T. An intrusion detection game with limited observation, Proc. 12th Int. Symp. On Dynamic Games and Applications, 2006. URL: http://www.tansu.alpean.org/papers/isdg06.pdf.
2. Security measurement – white paper, URL: http://www.psmsc.com/Downloads/ Technology Papers/Security White Paper-v. 3.0. pdf.
3. He W., X: Ac., Wang H., Zheng C., J.Y. A game theoretical attack-defense model oriented to network security risk assessment, *International Conference on Computer Science and Soft ware Engineering*, 2008, P. 498-504.
4. Горяшко А.П. Теория игр: от анализа к синтезу. Обзор результатов. *Электронный журнал Cloud of Science*, 2014, Т.1, №1. с. 47-55. URL: http://cloud of science.ru
5. Gohen N. An attack defense game with matrix strategies, “Naval Res. Logist. Quart.”, 1996, V 13, №4 – p. 234-246.
6. Беллман Р. Динамическое программирование. М.: Иностр. лит., 2005. 308 с.
7. Дрешер М. Стратегические игры: Теория и приложения. М.: Сов. радио, 2014. 304 с.
8. Forgo F. Relationship between continuous zero-sum two-person game sand linear programming. *Dep. Math. K. Marx. Univ. Econ. Budapest.* 2009. №1. P. 98-110.

9. Блекуэлл Д., Гришик М.А. Теория игр и статистических решений. М.: Иностр. лит., 2001. 363 с.
10. Мак-Кинет Дж. Введение в теорию игр. М: Физмат. 2000. 502 с.
11. Blackman N. Communication as a game. *IRE Wescon Convention record.* 2001. V.2.P. 176-189.
12. Волконский В.А. Модель оптимального планирования и взаимосвязи экономических показателей. М.: Наука, 2007. 286 с.
13. Поспелов Д.А. Игры и автоматы. М.: Энергия, 2006. 284 с.
14. Юдин Д.Б., Гольштеин Е.Г. Задачи и модели линейного программирования М: Сов. радио, 1991. 408 с.
15. Sisson R.I., Ackoff R.L. Toward a theory of the dynamics of conflict. *Peace Res. Soc. (Int.) Papers*. 2006. V. 5. P. 1011– 1032.

THE USE OF GAME THEORY FOR THE ANALYSIS OF HYBRID WARS

V.O. Horoshko[1], M.M. Brailovskyi[2]

National Aviation University, Lubomyr Guzar Ave, 1, Kyiv, 03058, Ukraine; e-mail: professor_va@ukr.net
Taras Shevchenko National University of Kyiv, Bohdana Havrylyshyna Street, 24, Kyiv, 04116, Ukraine; e-mail: bk1972@ukr.net

The issues of constantly changing geopolitical situation in the world and the desire of leading powers to obtain or strengthen the new and existing spheres of influence, as well as the urge of other countries to maintain or regain their former positions, leads to the use of new methods of hybrid warfare. One of the methods employed for information environment (i.e. network system) risk assessment is the probability of an attack on it. Information Security Assessment is determined by the values of the interaction between the attacking and defensive sides. This raises the challenge of the need to assess and predict the actions of both the defensive and the attacking sides. The process of interaction between attackers and defenders can be viewed as a game play, understood as the process of strategic interaction between the opposing or cooperating players under certain constraints and their plans of action. Deriving from this interpretation of the game, resolving the issues of hybrid war on the basis of the theory of games, predicting the actions of the attacking side, and determining the decisions by the defensive side is proposed. As in any theory of applied mathematics, game theory provides some formal structure. It is assumed that all possible actions of each player can be accurately established and for each combination of such actions the expected outcome of the competition can be quantified. The goal of each player is to maximize their expectation of winning. The player can assume that each of his opponents is busy with a similar optimization. The paper considers various possible situations of interaction between the attacking and defending sides. Functional expressions are given to determine the optimal strategies of the opposing sides and to find the guaranteed maximum level of the cost of an attack. Methods for solving these expressions are proposed. In particular, these include the following: methods for reducing matrix and continuous games to linear programming problems, methods for reducing continuous games to matrix games, algorithms for the approximate solution of continuous games by the random search method, and methods for modeling games.
Keywords: hybrid warfare, game theory, action prediction, action optimization.

DOI 10.15276/imms.v10.no 3-4.230
УДК 004.056:621.391

Informatics and Mathematical Methods in Simulation
Vol. 10 (2020), No. 3-4, pp. 230-242

КОНЦЕПЦІЯ КІБЕРБЕЗПЕКИ ТА МОДЕЛЮВАННЯ ПРОЦЕСІВ ОПТИМАЛЬНОГО УПРАВЛІННЯ СИСТЕМОЮ КІБЕРЗАХИСТУ ДЕРЖАВИ

В.О. Хорошко, Ю.Є. Хохлачова, І.В. Кібальчич

Національний авіаційний університет,
пр. Любомира Гузара, 1, Київ, 03058, Україна; e-mail: post@nau.edu.ua

Система організації безпеки держави та її об'єктів в кожному випадку повинна бути індивідуальною. Як завжди, коли наявні ресурси малі (а їх ніколи не буває в надлишку), намагаємося визначити способи, як найкраще їх використовувати, щоб максимально ефективно захиститися від потенціальних загроз, як уникнути їх. Попередження злочину – це передбачення кримінальних ризиків, їхнє виявлення й оцінка, а також дії, спрямовані на їхнє усунення чи знищення. Виявлення особливостей конкретного об'єкта держави, у якому слід забезпечити належний захист інформації, є першим важливим еталоном досягнення поставленої мети. Реалізація оптимального управління засобами обчислювальної техніки в реальному або прискореному часі не є складною. Для цього використовуються математичні моделі, які дозволяють описувати процеси оптимального управління системою кіберзахисту держави. Ці моделі дозволяють на стадії проектування або експлуатації системи контролювати або здійснювати управління процесами оптимізації в аналітичному вигляді.

Запропоновано метод моделювання процесів оптимального управління розподіленими системами (якою і є система кібербезпеки держави) на основі системи одномірних диференціальних перетворень, які описують управління хвильовим процесом. Він дозволяє постійно контролювати та коригувати процес управління системою кібербезпеки держави, що дуже важливо щодо забезпечення загальної безпеки держави.

Ключові слова: кібербезпека, кіберзахист, безпека держави, система кібербезпеки держави, процес оптимального управління, моделювання процесів.

Вступ

При побудові системи кібербезпеки держави (СКБД) дуже важливо розуміти особливості кожного об'єкта держави, захист яких треба забезпечити. Саме звідси треба починати аналіз ризиків, на які може наражатися досліджувана структура. Причому треба врахувати те, що деякі особливості носять тимчасовий характер, а з цього випливає, що їх можна виявити тільки в тому випадку, якщо досліджувати об'єкт (держави та її елементів) не тільки в цілодобовому режимі роботи, але й, протягом повного робочого циклу.

Однак особливості держави та її елементів, що захищаються, залежить не тільки від часу, але й від виду діяльності об'єктів та їх місця розташування.

А звідси напрошується очевидний висновок – система організації безпеки держави та її об'єктів, причому в кожному випадку повинна бути індивідуальною. Як завжди, коли наявні ресурси малі (а їх ніколи не буває в надлишку), намагаємося визначити способи, як найкраще їх використовувати, щоб максимально ефективно захиститися від потенціальних загроз, як уникнути їх. Попередження злочину – це передбачення кримінальних ризиків, їхнє виявлення й оцінка, а також дії, спрямовані на їхнє усунення чи знищення.

Таким чином, виявлення особливостей конкретного об'єкта держави, у якому слід забезпечити належний захист інформації, є першим важливим еталоном досягнення поставленої *мети*. [1 С.127].

Основна частина

Комплексна система безпеки повинна містити у собі:

– механічні засоби захисту, іншими словами фізичні перешкоди, що можуть використовуватися для відлякування потенційних порушників і для уповільнення швидкості їхнього проникнення на об'єкти, що охороняються;

– електронні засоби виявлення чи охоронні сигналізації, які повинні задовольняти чотирьом основним вимогам:

1) надійно виявляти присутність зловмисника;
2) надійно виявляти проникнення крізь фізичні охоронні бар'єри;
3) вчасно пускати в хід сили та засоби відповідного реагування;
4) не допускати помилкових спрацьовувань;

– електротехнічні засоби запобігання витоку інформації (різні генератори шуму, детектори, нелінійні локатори, аналізатори, виявлювачі і т.д.);

– програмі та криптографічні методи захисту, що забезпечують цілісність даних, досяжність даних конфіденційність даних і таємність;

– організаційні міри. Навіть самий захищений об'єкт, при охороні якого дотриманні високі стандарти, не може зберегти інформацію та обладнання у безпеці, якщо його користувачі не будуть дотримуватися елементарних запобіжних заходів. Тому важливо забезпечити управлінські процедури, дотримання яких дозволить створювати єдину та надійну систему безпеки об'єкта та держави в цілому.

Забезпечення безпеки інформації, яка має конфіденційний характер, у даний час набуває особливу актуальність. Крім цього, необхідно вирішувати задачі оптимального управління системи КБД, які є розподільними системами. При чому, розв'язування задачі управління в реальному часі вимагає моделювання процесів оптимального управління в прискореному часі з метою формування на основі моделювання управляючого впливу на розподілену систему КБД.

У сформульованих сучасних умовах задача забезпечення безпеки об'єктів та держави в цілому вимагає комплексного наукового підходу. Її вирішення для конкретного об'єкту доцільно починати з розробки концепції забезпечення безпеки. Концепція безпеки виражає загальний задум організації та реалізацію заходів для забезпечення захисту об'єктів держави від можливих загроз. Суть концепції забезпечення комплексної безпеки будь-якого об'єкта держави (рис.1) наполягає в перетворенні в життя трьох принципів [1, С.125]:

1. визначення цілей захисту (кого і що захищати?);
2. визначення і оцінка загроз (від кого захищати?);
3. розробка та реалізація адекватних мір захисту (як захищати?).

На державному об'єкті, що охороняється, в принципі існують три мети захисту [2]:

– люди (персонал об'єкта);
– майно (обладнання, цінності, документи);
– інформація (конфіденційна, службова та комерційна).

Цілі захисту утворюють простір загроз. В узагальненому виді основними видами загроз безпеки об'єкта та самої держави є [1, 2]:

– природні катаклізми та надзвичайні ситуації;
– розкрадання (втрата) майна;
– несанкціонована зйомка інформації, що містить конфіденційну, службову чи комерційну таємницю.

Система забезпечення комплексної безпеки об'єкта чи держави повинна бути сформована таким чином, щоб за допомогою людей, електронних, програмно-

апаратних і технічних засобів ефективно протистояти перерахованим загрозам шляхом вживання адекватних заходів захисту [1,2].

Для цього повинні бути створенні та надійно функціонувати наступні підсистеми безпеки [2,С.195]:

- система захисту об’єкта при надзвичайних ситуаціях;
- система захисту об’єкта при випадкових помилках персоналу;
- система захисту об’єкта при несанкціонованих діях зловмисників.

Рис. 1. Концепція забезпечення захисту об’єкта

Одним з основних джерел (причин) виникнення надзвичайних ситуацій на об’єктах, крім природних і техногенних є злочинні несанкціоновані дії фізичних осіб (порушників). Слід зазначити, що в сучасних умовах несанкціоновані дії зловмисників становлять особливу небезпеку, тому що можуть привести до виникнення кожної із загроз, представлених на рис. 1.

Загрози, як можливі небезпеки здійснення будь-якої дії, спрямовані проти об’єкта захисту, виявляються не самі по собі, а через вразливості (фактори), що приводять до порушення безпеки інформації на об’єкті, що захищається.

Вразливості притаманні будь-якому об’єкту, що захищається, невіддільні від нього й обумовлюються недоліками експлуатації, розташування й процесу

функціонування систем, програмно-апаратними комплексами, які застосовуються в роботі системи захисту.

Існує загальна класифікація вразливостей [1,2]:

– об'єктивні вразливості залежать від особливості побудови та технічних характеристик обладнання, яке застосовується на об'єкті, що захищається. Повне усунення цих вразливостей неможливе, але вони можуть істотно послабитися технічними й інженерно-технічними методами захисту інформації;

– об'єктивні вразливості залежать від дії співробітників й усуваються організаційними та програмно-апаратними методами;

– випадкові вразливості залежать від особливостей навколишнього середовища об'єкту, що захищається, і непередбачених обставин.

Ці фактори, як правило, мало передбачувані й їхнє усунення можливе тільки при проведенні комплексу організаційних й інженерно-технічних заходів щодо протидії загрозам несанкціонованого отримання інформації.

На базі сформованої концепції змоделюємо процеси управління системою кібернетичної безпеки держави.

Так як математична модель процесів оптимального управління містить опис процесу, яким управляють, у вигляді диференціальних рівнянь з частинними похідними, початкові та граничні умови; обмеження та оптимізуючий функціонал. Обмежуємося розглядом задач оптимально управління, в яких СКБД знаходяться під дією розподіленого лише в часі управління. Місце впливу вважається заданим.

На даний час найбільше розповсюдження для моделювання фізичних процесів отримали інтегральні перетворення [3 с. 231]. Однак, застосування інтегральних перетворень обмежується моделюванням фізичних процесів, які описуються лінійними диференціальними рівняннями з частинними похідними. На відмінну від інтегральних, диференційні перетворення дозволяють моделювати фізичні процеси, які описуються як лінійними, так і нелінійними диференційними рівняннями з частинними похідними з лінійними та нелінійними крайовими умовами [45].

В роботах [6, 7] розглядались методи моделювання процесів оптимального управління в області диференціальних перетворень тільки з об'єктами із зосередженими параметрами. Нам же треба вирішувати загрозу управління СКБД.

Розглянемо фізичні процеси, що описуються функцією θ (x, t) двох незалежних змінних в області, що визначається обмеженнями [8 с. 151]:

$$0 \le x \le H_x;\ 0 \le t \le H_t, \tag{1}$$

де H_x, H_t – задані додаткові сталі.

Обмежимося розглядом розподілених систем (СКБД), математична модель, яких допускає опис фізичних процесів у вигляді диференціальних рівнянь з частинними похідними в одній з двох формі:

$$\frac{\partial^2\theta(x,t)}{\partial x^2} = \varphi_1\left(x,t,\theta,\frac{\partial\theta}{\partial x},\frac{\partial\theta}{\partial t},\frac{\partial^2\theta}{\partial x\partial t},\frac{\partial^2\theta}{\partial t^2}\right), \tag{2}$$

$$\frac{\partial^2\theta(x,t)}{\partial x^2} = \varphi_2\left(x,t,\theta,\frac{\partial\theta}{\partial x},\frac{\partial\theta}{\partial t},\frac{\partial^2\theta}{\partial x\partial t},\frac{\partial^2\theta}{\partial t^2}\right) \tag{3}$$

До вигляду (2) та (3) можна звести лінійні й квазілінійні рівняння.

Надалі розглядаємо такі рівняння вигляду (2), (3), для яких можна застосувати принцип суперпозиції [9 с.354].

В момент часу t=0 стан фізичного процесу задається початковими умовами вигляду:

$$\theta(x,0)=\varphi_1(x),\frac{\partial\theta}{\partial t}\Big|_{t=0}=\psi_2(x), \tag{4}$$

де φ_1, φ_2 задані неперервні функції. Будемо вважати, що управляючий вплив $u(t)$ зосереджено в граничних умовах:

$$\theta(0,\mathrm{t})=u(t),\theta(H_x,t)=0, \tag{5}$$

Задача оптимального управління полягає в синтезі такого керуючого впливу $u(t)$, якого на фіксованого інтервалі часу [0, H_t] переводить фізичний процес кіберзахисту з початкового стану (4) в заданий термінальний стан:

$$\theta(x,H_t)=0,\frac{\partial\theta}{\partial t}\Big|_{t=H_t}=0, \tag{6}$$

а функціонал

$$I(u)=\int_O^{H_t}u^2(t)dt, \tag{7}$$

повинен досягати мінімального значення.

Функціонал (7) характеризує витрати енергії на управління, яке переводить фізичний процес кіберзахисту в заданий термінальний стан (6).

Метод вирішення задачі оптимального управління полягає в реалізації наступних етапів:

1 етап. Управління кібербезпекою моделюємо функцією заданого вигляду:

$$u(t)=\theta(t,C), \tag{8}$$

де $C=(C_1,C_2,\dots,C_n)$– вектор вільних коефіцієнтів апроксимуючої функції або ряду.

2 етап. На основі принципу суперпозиції [9 с. 403] розв'язок рівнянь (2) або (3), які описують фізичний процес кіберзахисту, представимо у вигляді суми двох доданків:

$$\theta(x,t,C)=\theta_1(\mathrm{x},\mathrm{t})+\theta_2(x,t,C), \tag{9}$$

де функція $\theta_1(x,t)$ описує вільну складову роз'язку, що виникає від ненульових початкових умов u при $u(t)=0$, а функція $\theta_2(x,t,C)$ описує вимушену складову розв'язку, яка виникає під дією управління $u(t)$ при нульових початкових умовах

$$\theta(x,0)=\frac{\partial\theta}{\partial t}\Big|_{t=0}=0. \tag{10}$$

3 етап. Визначаємо вектори вільних коефіцієнтів управління СКБД (8) шляхом розв'язку задачі мінімізації функції:

$$I(C)=\int_0^{H_t}\theta^2(t,C)dt\,, \tag{11}$$

при виконання термінальних умов

$$\theta(x,\mathrm{H}_t,C)=0,\ \frac{\partial\theta}{\partial t}\Big|_{t=H_t}=0\,. \tag{12}$$

Метод (8) ÷ (12) реалізуємо в області диференціальних перетворень [4, 5] на основі двох одномірних перетворень вигляду:

$$\bar{\theta}(x,\mathrm{k}_1)=\frac{H_t^{k_1}}{k_1!}\left(\frac{\partial^{k_1}\theta(x,t)}{\partial t^{k_1}}\right)_{t=0},\ \theta(x,t)=\sum_{k_1=0}^{\infty}\left(\frac{t}{H_t}\right)\frac{k_1}{\theta(x,k_1)}\,; \tag{13}$$

$$\bar{\theta}(\mathrm{k}_2,\mathrm{t})=\frac{H_x^{k_2}}{k_2!}\left(\frac{\partial^{k_2}\theta(x,t)}{\partial t^{k_2}}\right)_{x=0},\ \theta(x,t)=\sum_{k_2=0}^{\infty}\left(\frac{x}{H_x}\right)\frac{k_2}{\theta(\mathrm{k}_2,\mathrm{t})}, \tag{14}$$

де цілочисельні аргументи k_1 і k_2 приймають значення 0, 1, 2, 3,…; $\bar{\theta}(x,k_1)$ і $\bar{\theta}(k_2,t)$ – зображення фізичного процесу кіберзахисту $\theta(x,t)$, який моделюється та $\bar{\theta}(x,k_1)$ і $\bar{\theta}(k_2,t)$ прийнято називати диференціальними спектрами.

При цьому слід враховувати, що на сьогоднішній день існування як інформаційно-обчислювальних систем, так і СКБД не можливо без дослідження й узагальнення світового досвіду їх побудови та їх складових підсистем, ключовим елементом яких є зокрема системи кіберзахисту. Математичним забезпеченням таких систем є моделі процесів оптимального управління. [7, 9]. Наявні математичні моделі та методи моделювання СКБД, на яких ґрунтуються концепції та процеси моделювання оптимального управління, не враховуючи динаміку зміни множини можливих управлінь і варіацій параметрів системи як у реальному або прискореному часі. Тому базисом таких моделей та процесів моделювання є математичний апарат, який базується на теорії оптимального управління хвильового процесу[9,С.318], а саме оптимального управління затуханням коливань.

Моделювання процесів оптимального управління розподіленими СКБД (1) ÷ (7) на основі реалізації методу (8) ÷ (12) в області диференціальних перетворень (13) ÷ (14) розглянемо на прикладі оптимального управління затуханням коливань [9 с.126]. Так як диференціальний процес описується хвильовим рівнянням:

$$\frac{\partial^2\theta^*}{\partial\tau^2}=a^2\frac{\partial^2\theta^*}{\partial y}$$

де $\theta^*(y,\tau)$ – відхилення точок коливального середовища від положення рівноваги в просторовій точці y на час τ, a– швидкість розповсюдження коливань в середовищі, що моделюється.

Розглянемо коливання середовища в межах просторового відрізку [0, π].

Перейдемо до нових змінних:

$$t=a\tau,\ x=y,\ \theta\frac{\theta^*}{\theta_{\max}}$$

де θ_{max} – максимально допустиме відхилення точок коливального середовища.

Хвильове рівняння в нових змінних набуває вигляду

$$\frac{\partial^2\theta(x,t)}{\partial\tau^2}=\frac{\partial^2\theta(x,t)}{\partial x^2}, \tag{15}$$

в області

$$0\le x\le\pi,\ 0\le t\le T\ . \tag{16}$$

В початковий момент часу $t=0$ маємо збурення фізичного процесу, яке описується початковими умовами:

$$\theta(x,0)=0,\ \frac{\partial\theta}{\partial t}\Big|_{t=0}=\cos\frac{x}{2}. \tag{17}$$

Задаємо граничні умови:

$$\theta(\pi,\mathrm{t})=0,\ \theta(0,t)=u(t). \tag{18}$$

З (18) випливає, що управління$u(t)$ зосередженно в точці $x=0$.

Потрібно знайти таке управління $u(t)$ на фіксованому інтервалі часу $[0,T]$, щоб фізичний процес за час $T=2\pi$ досяг термінального стану, заданою умовами:

$$\theta(x,\mathrm{T})=0,\ \frac{\partial\theta}{\partial t}\Big|_{t=T}=0\ , \tag{19}$$

причому функціонал (7) при $H_t=T$повинен досягти мінімального значення.

З теорії оптимального управління розподіленими коливальними системами [9 с.268], випливає що оптимальне управління можна апроксимувати відрізками ряду Фур'є:

$$u(t)=\begin{cases} u_1(t),\ 0\le \mathrm{t}\le\pi \\ u_2(t),\ \pi\le \mathrm{t}\le 2\pi, \end{cases} \tag{20}$$

де $u_i=C_{0i}+C_{1i}\sin C_{3i}t+C_{2i}\cos C_{3i}t$, $i=1,2, C_{0i}, C_{1i}, C_{2i}, C_{3i}$ – вільні коефіцієнти, які потрібно визначити.

Згідно другого пункту методу вільну складову $\theta_1(x,t)$розв'язку знаходимо як розв'язок рівняння (15) з початковими умовами (17) і нульовими граничними умовами (18). Розв'язок цієї задачі виконаємо в області диференціальних перетворень (13). Математична модель рівняння (15) в області зображень (13) має вигляд:

$$\overline{\theta_1}(x,k_1+2)=\frac{H_t^2}{(k_1+1)(k_2+2)}\cdot\frac{\partial^2\overline{\theta}(x,k_1)}{\partial x^2}, \tag{21}$$

Початкові дискрети диференціального спектру $\overline{\theta_1}(x,k)$ визначаються з початкових умов (17) і з першого виразу диференціальних перетворень (13):

$$\overline{\theta_1}(x,0)=0, \overline{\theta_1}(x,1)=H_t\cos\frac{x}{2}. \tag{22}$$

За рекурентним виразом (21), використовуючи початкові дискрети (22), розраховуємо диференціальний спектр при $k_1 = 0, 1, 2, 3, ...$

$$\overline{\theta_1}(x,0)=0; \overline{\theta_1}(x,1)=H_t\frac{x}{2}; \overline{\theta_1}(x,2)=0;$$

$$\overline{\theta_3}(x,3)=-\frac{1}{3!}\frac{H_t^3}{4}\cos\frac{x}{2}; \overline{\theta_1}(x,4)=0; \overline{\theta_1}(x,5)=\frac{1}{5!}\frac{H_t^5}{16}\cos\frac{x}{2}; \overline{\theta_1}(x,6)=0. \tag{23}$$

За другим виразом диференціальних перетворень (13) і диференціального спектру (23) відновимо оригінал вільної складової розв'язку рівняння (15).

$$\theta(x,t)=\sum_{k_1=0}^{\infty}\left(\frac{t}{H_t}\right)^{k_1}\overline{\theta_1}(x,k_1)=2\frac{t}{2}\cos\frac{x}{2}-\frac{2}{3!}\left(\frac{t}{2}\right)^3\cos\frac{x}{2}+\frac{2}{5!}\left(\frac{t}{2}\right)^5\cos\frac{x}{2}-...=$$

$$=2\left[\frac{t}{2}-\frac{1}{3!}\left(\frac{t}{2}\right)^3+\frac{1}{5!}\left(\frac{t}{2}\right)^5-...\right]\cos\frac{x}{2}=2\sin\frac{t}{2}\cos\frac{x}{2}. \tag{24}$$

Вимушену складову $\theta_2(x,t,C)$ розв'язку рівняння (15) знаходимо при нульових початкових умовах (10) з граничними умовами (18) і управління (20).

Розв'язок цієї задачі виконаємо в області диференціальних перетворень (14), в якій зображення рівняння (15) має вигляд:

$$\overline{\theta_2}(\mathrm{k}_2+2,\mathrm{t})=\frac{H_x^2}{(k_2+1)(k_2+2)}\frac{\partial^2\overline{\theta_2}(k_2,t)}{\partial t^2}. \tag{25}$$

Початкові дискрети диференціального спектра $\bar{\theta}(k_2,t)$ визначаються за другою граничною умовою (18):

$$\overline{\theta_2}(0,\mathrm{t})=u(t), \overline{\theta_2}(1,\mathrm{t})=0. \tag{26}$$

Дискрета $\theta_2(1,t)=0$ дорівнює нулю, бо управління затуханням коливань фіксована в точці $x=0$і не залежить від зміни змінної x. Тому $\left.\frac{\partial^2\theta_2}{\partial x}\right|_{x=0}=0$, а з першого виразу (14) слідує $\overline{\theta_2}(1,t)=0$.

Диференціальний спектр $\overline{\theta_2}(k_2,t)$ розраховується за рекурентним виразом (25) і початковими дискретами (26) шляхом послідовного надання цілочисельному аргументу значень $k_2 = 0, 1, 2, 3, ...$:

$$\overline{\theta_2}(0,\mathrm{t})=u(t); \overline{\theta_2}(1,\mathrm{t})=0; \overline{\theta_2}(2,\mathrm{t})=\frac{H_x^2}{2}u^{(2)}(t); \overline{\theta_2}(3,\mathrm{t})=0;$$

$$\overline{\theta_2}(4,\mathrm{t})=\frac{H_x^2}{4!}u^{(4)}(t); \overline{\theta_2}(5,\mathrm{t})=0; \tag{27}$$

де використано позначення $u^{(n)}(t) = \frac{d^n u(t)}{dt^n}$,n = 1, 2, 3, … .

За другим виразом обернених диференціальних перетворень (14) знаходимо вимушену складову $\theta_2(x,t,C)$ розв'язку рівняння (15) шляхом підстановки управління $u(t)$ (20) і його похідних $u^{(n)}(t)$ в (27):

$$\theta_2(x,t,\mathrm{C}) = \sum_{k_2=0}^{\infty}\left(\frac{x}{H_x}\right)^{k_2}\overline{\theta_2}(k_2,t) =$$

$$= C_{0i} + \left(C_{1i}\sin c_{3i}t + C_{2i}\cos C_{3i}t\right)\left[1 - \frac{(C_{3i}x)^2}{2!} + \frac{(C_{3i}x)^4}{4!} - \ldots\right] =$$

$$= C_{0i} + \left(C_{1i}\sin c_{3i}t + C_{2i}\cos C_{3i}t\right)\cos C_{3i}x.$$

Перша гранична умова (18) виконується, якщо у виразі (28) при$x = \pi$ коефіцієнтам надати значення $C_{0i} = 0,\ C_{3i} = \frac{1}{2}$. З врахуванням цих значень коефіцієнтів математична модель фізичного процесу (19) описується сумою вільної (24) і вимушеної (28) складових, що складають розв'язок рівняння (15):

$$\theta(x,t,C) = 2\sin\frac{1}{2}\cos\frac{x}{2} + \left(C_{1i}\sin\frac{1}{2} + C_{2i}\cos\frac{t}{2}\right)\cos\frac{x}{2}. \tag{29}$$

Вираз (29) описує процес затухання коливання на часовому проміжку $[0,\pi]$при $i = 1$. Як впливає в момент часу $t = \pi$управління має розрив, який має місце в результаті переходу від управління $u_1(t)$ до управління $u_2(t)$. В результаті в момент часу $t = \pi$ маємо збурення фізичного процесу, яке описується виразом (29) при $t = \pi$:

$$\theta(x,\pi) = (2 + C_{11})\cos\frac{x}{2}, \left.\frac{\partial\theta}{\partial t}\right|_{t=\pi} = -\frac{C_{21}}{2}\cos\frac{x}{2}. \tag{30}$$

Введемо новий часовий аргумент $\bar{t} = t - \pi$і розглянемо фізичний процес затухання коливань на часовому проміжку $\bar{t}\epsilon[0,2\pi]$ або $\bar{t}\epsilon[0,\pi]$. З врахування введення часового аргументу $\bar{t} = t - \pi$ зараз (30) задає початкові умови при $\bar{t} = 0$:

$$\theta(x,\bar{t} = 0) = (2 + C_{11})\cos\frac{x}{2}, \left.\frac{\partial\theta}{\partial t}\right|_{t=0} = -\frac{C_{21}}{2}\cos\frac{x}{2}. \tag{31}$$

Математична модель рівняння (15) в області зображень (21) не залежить від часового аргументу і тому може використовуватись для моделювання фізичного процесу на часовому проміжку $\bar{t}\epsilon[0,\pi]$. Послідовно надаючи цілочисельному аргументу значення $k_1 = 0,1,2,3,\ldots$ за рекурентним виразом (21) при початкових дискрета, заданих умовами (31):

$$\overline{\theta_1}(x,0) = (2 + C_{11})\cos\frac{x}{2}; \overline{\theta_1}(x,1) = H_t\frac{C_{21}}{2}\cos\frac{x}{2},$$

розрахуємо диференціальний спектр зображення вільної складової розв'язку рівняння (15) на часовому проміжку $\bar{t} = [0,\pi]$

$$\overline{\theta}_1(x,0)=(2+C_{11})\cos\frac{x}{2};\overline{\theta}_1(x,1)=-H_t\frac{C_{21}}{2}\cos\frac{x}{2};$$
$$\overline{\theta}_1(x,2)=-\frac{1}{4}(2+C_{11})\frac{H_t^2}{2}\cos\frac{x}{2};\overline{\theta}_1(x,3)=\frac{C_{21}}{8}\frac{H_t^3}{3!}\cos\frac{x}{2};$$
$$\overline{\theta}_1(x,4)=\frac{1}{16}(2+C_{11})\frac{H_t^4}{4!}\cos\frac{x}{2};\overline{\theta}_1(x,5)=\frac{C_{21}}{32}\frac{H_t^5}{5!}\cos\frac{x}{2}... \quad (32)$$

Оригінал вільної складової розв'язку рівняння (15) на часовому проміжку $\bar{t}\in[0,\pi]$ відновлюємо за другим виразом диференціальних перетворень (13) на основі диференціального спектру (22):

$$\theta_1(x,\bar{t})=\sum_{k_1=0}^{\infty}\left(\frac{\bar{t}}{H_t}\right)^{k_1}\overline{\theta}_1(x,k_1)=$$
$$=(2+C_{11})\left[1-\frac{1}{2}\left(\frac{\bar{t}}{2}\right)^2+\frac{1}{4!}\left(\frac{1}{2}\right)^4-...\right]-C_{21}\left[\frac{\bar{t}}{2}-\frac{1}{3!}\left(\frac{\bar{t}}{2}\right)^3+\frac{1}{5!}\left(\frac{\bar{t}}{2}\right)-...\right]\cos\frac{x}{2}=$$
$$=\left[(2+C_{11})\cos\frac{\bar{t}}{2}-C_{21}\sin\frac{\bar{t}}{2}\right]\cos\frac{x}{2}. \quad (33)$$

Вимушена складова розв'язку рівняння (15) на часовому проміжку $\bar{t}\epsilon[0,\pi]$ визначається виразом (28) при $i=2$, $C_{02}=0, C_{32}=\frac{1}{2}$, так як зображення (25) рівняння (15) і початкові дискрети (26) зберігають свій вигляд крім зміни управління $u_1(t)$ на управління $u_2(t)$. Отже,вимушена складова $\theta_2(x,\bar{t},z)$ (28) розв'язку рівняння (15) на часовому проміжку $\bar{t}\in[0,\pi]$ має вигляд:

$$\theta_2(x,\overline{t,C})=\left(C_{12}\sin\frac{\bar{t}}{2}+C_{22}\cos\frac{\bar{t}}{2}\right)\cos\frac{x}{2}. \quad (34)$$

Математична модель фізичного процесу затухання коливань на часовому проміжку $\bar{t}\in[0,\pi]$ визначається сумою вільної (33) і вимушеної (34) складових розв'язку рівняння (15):

$$\theta_2(x,\overline{t,C})=\left[(2+C_{11}+C_{22})\cos\frac{\bar{t}}{2}+(C_{12}-C_{21})\sin\frac{\bar{t}}{2}\right]\cos\frac{x}{2}. \quad (35)$$

Підстановка (35) в термінальні умови (19) при$t=T=2\pi$ або $\bar{t}=\pi$ дає наступні співвідношення між коефіцієнтами:

$$C_{12}-C_{21}=0;\ 2+C_{11}+C_{22}=0.$$

Перейдемо до реалізації третього пункту метода. Підставимо управління (20) при $C_{0i}=0, C_{31}=\frac{1}{2}$,$i=1,2$ в функціонал (7) дозволяє перетворити його в функцію вільних коефіцієнтів:

$$I(\mathrm{C})=\int_0^{\pi}U_1^2(t)dt+\int_{\pi}^{2\pi}U_2^2(t)dt=\frac{\pi}{2}\left(C_{11}^2+C_{21}^2+C_{12}^2+C_{22}^2\right). \quad (37)$$

Задача визначення вільних коефіцієнтів управління (20) звелась до задачі мінімізації функції (37) при виконанні умов у формі рівностей (36). Ця задача може бути розв'язана методом прямої підстановки або методом множників Лагранджа [3] . Розв'яжемо задачу умовної оптимізації (36) і (37) методом прямої підстановки.

З рівностей (36) випливає:

$$C_{11} = C_{21},\ C_{22} = -2 - C_{11}. \tag{38}$$

Підстановка (38) в (37) дозволяє звести оптимізаційну задачу (36) і (37) до задачі безумовної мінімізації функції двох змінних:

$$I\left(C_{11}, C_{12}\right) = \frac{\pi}{2}\left[C_{11}^2 + 2C_{12}^2 + \left(2 + C_{11}\right)^2\right]. \tag{39}$$

З необхідних умов екстремуму функції (39) отримаємо систему двох рівнянь для визначення C_{11} і C_{12}:

$$\frac{\partial I}{\partial C_{11}} = \pi\left(C_{11} + 2 + C_{11}\right) = 0,\ \frac{\partial I}{\partial C_{12}} = 2\pi C_{12} = 0. \tag{40}$$

З рівнянь (40) випливає $C_{11} = 1, C_{12} = 0$. Підстановка цих значень вільних коефіцієнтів в (39) визначає інші невідомі коефіцієнти:

$$C_{12} = C_{21} = 0,\ C_{11} = -1,\ C_{22} = -1. \tag{41}$$

Дослідження достатніх умов існування екстремуму в точці (41) показує, що функція (39) досягає в цій точці мінімуму.

До системи коефіцієнтів (41) слід добавити коефіцієнти, які були знайдені раніше з граничної умови (18):

$$C_{01} = C_{02} = 0,\ C_{31} = C_{32} = \frac{1}{2}. \tag{42}$$

Підстановка значень вільних коефіцієнтів (41) і (42) у вираз (20) дає оптимальне управління коливань пружного середовища в такому вигляді:

$$u(t) = \begin{cases} -\sin\dfrac{t}{2},\ 0 \le \mathrm{t} \le \pi \\ -\cos\dfrac{t}{2},\ \pi \le \mathrm{t} \le 2\pi. \end{cases} \tag{43}$$

Таким чином, моделювання процесів оптимального управління затуханням коливань, пружного середовища в області диференціальних перетворень дозволило отримати в прикладі, який розглянуто, оптимальне управління в аналітичному вигляді (43).

Висновки

Реалізація оптимального управління засобами обчислювальної техніки в реальному або прискореному часі не є складною. Для цього використовуються

математичні моделі, які дозволяють описувати процеси оптимального управління системою кіберзахисту держави. Ці моделі дозволяють на стадії проектування або експлуатації системи контролювати або здійснювати управління процесами оптимізації в аналітичному вигляді.

Запропонований метод моделювання процесів оптимального управління розподіленими системами (якою і є система кібербезпеки держави) на основі системи одномірних диференціальних перетворень, які описують управління хвильовим процесом. Він дозволяє постійно контролювати та коригувати процес управління системою кібербезпеки держави, що дуже важливо щодо забезпечення загальної безпеки держави.

Список літератури

1. Хорошко В.О., Хохлачова Ю.Є. Показатели для оценки живучести системы информационной безопасности государства. *Інформаційна безпека,* 2018, № 4 (32). С. 123-129.
2. Хорошко В.О., Хохлачова Ю.Є. Підхід до вибору засобів захисту з урахуванням їх оцінок. Інформаційні технології проблеми та перспективи: колективна монографія. Харків: Вид. Рожко Р.Г., 2017. С. 187-203.
3. Сейдж Э.П. Уайт Ч.С. Оптимальное управление системами. М.: Радио и связь, 1982. 392 с.
4. Пухов Г.Е. Дифференциальные преобразования и математическое моделирование физических процессов. К.: Наук. думка, 1986. 158с.
5. Пухов Г.Е. Дифференциальные спектры и модели. К.: Наук. думка, 1990. 184 с.
6. Баранов В.Л., Фролова Е.Г., Баранов Г.Л. Метод смещенных дифференциальных преобразований для решения многокритериальных задач управления. *Электроника и связь*. 2002, № 16. С.25 – 28.
7. Грищук Р.В. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень. Житомир: Рута, 2010. 280с.
8. Баранов В.Л. Капустен М.В., Костюченко Р.В., Хорошко В.О. Моделювання фізичних процесів в інформаційній безпеці. К.: ДУІКТ, 2010. 175 с.
9. Фельдбаум А.А., Бутковский А.Г. Методы теории автоматического управления. М.: Наука, 1971. 744 с.

THE CONCEPT OF CYBER SECURITY AND SIMULATION OF PROCESSES OF OPTIMAL CONTROL OF THE STATE CYBER PROTECTION SYSTEM

V.O. Khoroshko, Y.E. Khokhlachova, I.V. Kibalchich

National Aviation University,
Lubomyr Husar Ave., 1, Kyiv, 03058, Ukraine; e-mail: post@nau.edu.ua

The system of security organization of the state and its facilities in each case must be individual. As always, when available resources are small (and they are never in excess), we try to identify ways to best use them to best protect against potential threats, how to avoid them. Crime prevention is the anticipation of criminal risks, their detection and assessment, as well as actions aimed at their elimination or destruction. Identifying the specifics of a particular state object, in which the proper protection of information should be ensured, is the first important standard for achieving this goal. Implementation of optimal control of computer equipment in real or accelerated time is not difficult. For this purpose, mathematical models are used, which allow to describe the processes of optimal management of the state cyber defense system. These models allow at the stage of system design or operation to control or manage optimization processes in an analytical form.
A method for modeling the processes of optimal control of distributed systems (which is the system of cyber security of the state) based on a system of one-dimensional differential transformations that describe the control of the wave process is proposed. It allows you to constantly monitor and adjust the process of managing the state cyber security system, which is very important for ensuring the overall security of the state.
Keywords: cyber security, cyber defense, state security, state cyber security system, optimal management process, process modeling.

ІНФОРМАТИКА ТА МАТЕМАТИЧНІ МЕТОДИ В МОДЕЛЮВАННІ

Том 10, номер 3-4, 2020. Одеса – 124 с., іл.

ИНФОРМАТИКА И МАТЕМАТИЧЕСКИЕ МЕТОДЫ В МОДЕЛИРОВАНИИ

Том 10, номер 3-4, 2020. Одесса – 124 с., ил.

INFORMATICS AND MATHEMATICAL METHODS IN SIMULATION

Volume 10, No. 3-4, 2020. Odesa – 124 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 від 30.11.2020)

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, 2020