

Наукоємні технології

№ 3 (39) 2018

НАУКОВИЙ ЖУРНАЛ

Заснований у квітні 2009 р.

Science-Based Technologies

УДК 001:629.7(051)

ЗМІСТ

ГОЛОВНИЙ РЕДАКТОР

В. В. Козловський —
директор Навчально-наукового
інституту комп'ютерних
інформаційних технологій НАУ
доктор технічних наук, професор

ЗАСТУПНИК ГОЛОВНОГО РЕДАКТОРА

І. О. Мачалін — директор
Навчально-наукового інституту
аеронавігації, електроніки та
телекомунікацій НАУ,
доктор технічних наук, професор

ВІДПОВІДАЛЬНИЙ СЕКРЕТАР

А. С. Савченко — кандидат
технічних наук, доцент

РЕДАКЦІЙНА КОЛЕГІЯ

В. В. Бараннік, д-р тех. наук, проф., Україна
С. В. Бойченко, д-р тех. наук, проф., Україна
А. М. Грехов, д-р фіз.-мат. наук, проф., Україна
І. А. Жуков, д-р тех. наук, проф., Україна
О. І. Запорожець, д-р тех. наук, проф., Україна
Г. Ф. Коначович, д-р тех. наук, проф., Україна
О. Є. Литвиненко, д-р тех. наук, проф.,
Україна
О. М. Новіков, д-р тех. наук, проф., Україна
О. Г. Оксіюк, д-р тех. наук, проф., Україна
В. М. Опанасенко, д-р тех. наук, ст. наук.
співроб., Україна
О. В. Палагін, д-р тех. наук, проф., Україна
О. А. Тамаргазін, д-р тех. наук, проф., Україна
А. А. Тушнік, д-р тех. наук, проф., Україна
В. П. Харченко, д-р тех. наук, проф., Україна

Інформаційно-комунікаційні системи та мережі

**Savchenko A. S., Vasylenko V. A., Kolisnyk O. V.,
Holiavkina T. V.**

Computer networks monitoring and management methods.....281

Азаренко О. В., Кукліньський М. В., Клімова А. С.

Фактографічна інформаційна система
мультимедійної бази даних289

**Бараннік В. В., Бараннік Д. В., Сорокун А. Д.,
Дворський М. В.**

Вдосконалення методів компенсації руху динамічних
об'єктів у відеопотоці в системі відеоконференцзв'язку.....294

**Бараннік В. В., Гаврилов Д. С., Фустій, В. С.,
Бараннік В. В.**

Технологія багаторівневої селективної обробки
аерофотознімку для перспективних літальних
сенсорних мереж.....301

**Жуков І. А., Печурін М. К., Кондратова Л. П.,
Печуріна О. О.**

Способ оцінювання інтенсивностей первинних
інформаційних потоків, згенерованих абонентами
комп'ютерної мережі речей.....308

Козловський В. В., Глива В. А., Ходаковський О. В.

Захисні властивості електромагнітних екранів
на основі залізорудного пилу та їх застосування
для захисту інформації та людей.....314

Інформаційна безпека

Kozlovskii V. V., Ivanov O. V., Snizhko V. V.

Analysis and security management of telecommunication
systems based on predictive technologies.....321

В. І. Хаханов, д-р тех. наук, проф., Україна
Г. М. Юн, д-р тех. наук, проф., Україна
Ф. Й. Яновський, д-р тех. наук, проф., Україна
А. Смерлас, д-р тех. наук, Німеччина
В. Кук, д-р тех. наук, проф., Естонія
М. П. Карпінський, д-р тех. наук, проф., Польща
Л. Еріксон, д-р тех. наук, проф., США
О. С. Петров, д-р тех. наук, проф., Польща
П. Ексель, д-р тех. наук, проф., Велика Британія
П. Бейтс, д-р тех. наук, проф., Австралія
С. Е. Лішевський, д-р тех. наук, проф., США

ВІСНИК

НАУКОЄМНІ ТЕХНОЛОГІЇ

№ 3 (39), 2018

Свідоцтво про державну реєстрацію
друкованого засобу масової інформації
КВ № 13793-2767Р від 05.03.2008

Рекомендовано до друку Вченою радою
Національного авіаційного університету
(протокол № 6 від 28.09.2018)
Постановою Вищої атестаційної
Комісії України науковий журнал
«Наукоємні технології»
включено до переліку наукових видань,
публікації яких зараховуються
до результатів дисертаційних робіт з
технічних наук.
(Наказ Міністерства освіти і науки
України від 21.12.2015 р. № 1328
категорія «В»)

Адреса редакційної колегії:

03680, Київ-58, просп. Космонавта
Комарова, 1, тел. 406-70-08

Комп'ютерна верстка — Л. Т. Колодіної
Дизайн обкладинки — К. С. Лебеденко

Kozlovskii V. V., Kubiv S. I., Balanyuk Yu. V. Single-factor model of information security threats of the automated management system of production of high-speed telecommunication distributed data transfer systems.....	327
Бараннік В. В., Довбенко О. В., Белікова Т. В., Мусянко О. П. Методи виявлення прихованих сугестивних інформаційно-психологічних впливів в інформаційних ресурсів текстового змісту.....	331
Бойко Ю. П., Приходько Т. Ю., Басюк І. О. Огляд сучасних фільтруючих пристроїв НВЧ і їх методів побудови.....	338
Ільєнко А. В., Ільєнко С. С. Програмний модуль з використанням процедури формування та верифікації електронного цифрового підпису.....	345
Одарченко Р. С., Самойлик Є. О., Абакумова А. О. Метод побудови семантичного словника у складі досконало стійкої криптосистеми захисту текстової інформації.....	355

Експлуатація повітряного транспорту

Malikov E. Fluctuations of an airplane with aerodynamic wingtip «At winglets».....	362
Козлюк І. О. Коваленко Ю. Б. Методи оцінки показників надійності авіаційної техніки за результатами випробувань та технічної діагностики	367
Соломенцев О. В., Заліський М. Ю., Герасименко Т. С. Аналіз ефективності процедури виявлення розладнання в системах експлуатації наземних засобів аеронавігації.....	376

Екологія

Ремез Н. С., Бойко А. Г. Екологічна санітарія як засіб покращення ґрунтово- рослинного покриву.....	383
--	-----

Енергетика

Капітанчук К. І., Андрійшин М. П. Розрахунок подовження енергопоглинального елемента морської хвильової електростанції при трансформації спіралі у площину.....	387
---	-----

Підп. до друку 31.10.2018. Формат 60×84/8. Ум. друк. арк. 13,02. Обл.-вид.
арк. 14,0.

Тираж 100 пр. Замовлення № 485-1.

Видавець і виготівник Національний авіаційний університет
03680, Київ-58, проспект Космонавта Комарова, 1

Свідоцтво про внесення до Державного реєстру ДК № 977 від 05.07. 2002
© Національний авіаційний університет, 2018

A. S. Savchenko, cand. of techn. sciences, associate professor
National Aviation University
orcid.org/0000-0001-8205-8852
e-mail: alina@inet.ua

V. A. Vasylenko, cand. of techn. sciences, associate professor
National Aviation University
orcid.org/0000-0003-4733-2953
e-mail: lena_08@ukr.net

O. V. Kolisnyk, cand. of techn. sciences
National Aviation University
orcid.org/0000-0003-2955-1319
e-mail: kolisnuk1973@gmail.com

T. V. Holiavkina, cand. of techn. sciences, associate professor
National Aviation University
orcid.org/0000-0003-2595-9405
e-mail: holyavkina.t@gmail.com

COMPUTER NETWORKS MONITORING AND MANAGEMENT METHODS

Introduction

High-quality service of all types of traffic is important requirement for a computer network of any scale and purpose. One of the factors of meeting this requirement is effective resource management. Currently, monitoring and managing methods of computer networks are underdeveloped. The problem of large-scale networks is particularly relevant.

Thus, it is important to improve traditional, as well as development of new methods and approaches to network monitoring and management.

Definition of the issue

Managing a large and complex distributed structure of a large corporate computer network (CN) or data center (DC) is a non-trivial task even for an experienced system administrator. Monitoring and control systems allow you automate a process and increase efficiency of the CN [1].

Such systems have existed and improved for many years, however, they are clearly equipped not enough to manage homogeneous networks.

Such systems either have insufficient functionality or require significant modifications for a specific infrastructure, or they are expensive to implement and operate, cumbersome and difficult to set up [2, 3].

In addition, the presence of standard types of control information bases such as MIB-1, MIB-2, or RMON MIB and more than a thousand of MIB's proprietary databases, with its object structure reflecting some non-standard equipment and complicating the process of implementation of monitoring systems. And the continuous release on the market of new models and even new families of models of communication equipment and the lack of unified standards for monitoring and control protocols does not allow the development of a universal monitoring system.

The optimal monitoring/control system of the CS should ensure ease of implementation, operation and modernization.

The maximum degree of automation of processes, the presence of a friendly human-machine interface, and the tolerance of the system to errors, which the network administrator could possibly make, ensure ease of maintenance of computer network [1].

An equally important fundamental requirement for a monitoring system and managing network of any scale is the ease of implementation and modernization.

Simplicity of implementation could be achieved by providing management with minimal interference into the existing network infrastructure.

Consequently, monitoring and management systems should be developed based on existing and well-proven technologies and network management protocols. The obvious way out of this situation is the modular structure. Each module must solve its tasks for a particular technology and the corresponding control protocol, and be able to adapt when embedded in the system. It is significant to ensure interchangeability of modules with each other.

Thus, the study of common tasks, principles and methods of monitoring modern computer networks is the task of the current interest.

Computer networks monitoring tasks

The objectives of monitoring and managing computer networks in accordance with the quality of communication standards are to ensure the quality of service of traffic QoS (Quality of Services) as a total service performance effect that determines the level of customer satisfaction with this service.

The key monitored indicators of quality of service are:

- network performance or transmission speed (bit/s);
- amount of loss of packets transmitted (%);
- delay and jitter (random variances) delay (ms);
- reliability of network elements (probability of failure, average time of failure to work);
- viability of the network — the possibility of maintaining operational characteristics in case of failure of individual elements (redundancy of equipment under the schemes of cold or hot replacement).

First three parameters characterize the traffic parameters (logical level of connection), and the latter two relate to network equipment (ie, physical layer of the network), therefore, both monitoring of traffic parameters and monitoring of the state of network elements is required.

Among the network equipment parameters, it is most appropriate to monitor the availability and state of the ports, the state of the processor and the memory of the device.

Monitoring itself is not able to provide the required QoS level. To do this, they use methods and tools for managing the network, including:

- increase bandwidth network due to hardware capabilities;
- methods for reducing the load on the network (assigning traffic priorities and arranging queues, balancing the load, reserving resources, etc.).

Distributed monitoring and management of computer network

Classical distributed monitoring and control systems for the computer network are implemented in accordance with the concept of “manager-agent” [2; 3]. This architecture is distributed because there

may be several managers. On managed objects, agents are installed and an object model is created. It represents all the characteristics of the object that are necessary for its control. For example, a router model typically includes characteristics such as the number of ports, their type, routing table, the number of frames, and packet protocols for channel, network, and transport levels passed through these ports. Models of network objects are used by the manager as a source of knowledge about which set of characteristics has one or another object.

The object model coincides with the logical diagram of the database (DB) of the stored object with values of its characteristics. This database is stored on the device and is constantly replenished by the results of measurements of the characteristics carried out by the agent.

The agent can perform the following functions:

- store, extract and transmit on request information about the technical and configuration parameters of the device, including the device model, number of ports, type of ports, OS type, connections with other devices, etc.;
- perform, store and transmit on request the measurements (calculations) of the characteristics of the operation of the device, such as the number of received packets, the number of dropped packets, the degree of filling the buffer, the state of the port (working or not working);
- modify the configuration parameters from commands received from the outside.

The manager does not have direct access to the database, in order to obtain the specific values of the object characteristics; he has to contact his agent over the network. Thus, the agent is an intermediary between the managed object and the manager. The manager and agent interact according to the standard protocol. This protocol allows the manager to request the values of the parameters stored in the database, and the agent - to transmit the information based on which the manager must control the object.

A manager with a certain frequency produces farrowing agents on managed devices and receives information about their current characteristics. The manager consolidates and visualizes the information received in the form of tables or graphs. In complex control systems, the CS also analyzes the information received and predicts the state for detecting the abnormal operation of the network elements. The system provides a warning about the critical state of resources, which allows you to immediately take measures to maintain the work of these resources.

The exchange of information during monitoring and control can be carried out on the same channel, in which the transmission of user traffic — in-band.

Such an approach is more economical, since it does not require the creation of a separate control data transmission infrastructure and is more reliable, since for user traffic, Level 2 and 3 protocols create backup paths when a primary failure occurs. Out-band control on a separate channel, that is, carried out outside of the user data transmission channel, also has high reliability due to the fact that the corresponding equipment can perform its functions even when some network elements fail and the main transmission channels are inaccessible. Mixed approaches are often used.

The most commonly used classical monitoring system is SNMP (Simple Network Management Protocol), which implements the concept of “manager-agent”. SNMP is an application layer protocol, simplicity of which is determined by the simplicity of the Management Information Base (MIB) and the minimum requirements for the standardization of monitoring systems built on this protocol. The following items are standardized: protocol of interaction between agent and manager, MIB model description language and SNMP messages, several specific MIB models whose object names are logged in the ISO tree.

The protocol defines the format of the data, and their processing and interpretation remains at the discretion of the control stations or the network manager. SNMP messages do not have a fixed format and fixed fields.

Using the SetRequest command, the actual monitoring and management of the device takes place. The agent must "understand" the meaning of the variable that is used to control the device and, based on these values, carry out a real control action: turn off the port, assign the port of a specific VLAN line, expand the bandwidth, reserve resources, etc.

For example, the state of the network equipment can be tracked via the server agent SNMP requests: GetRequest and the agent server: Trap, specifying the desired object ID (OID) in the MIB database.

Centralized monitoring and management

Modern computer networks also use monitoring and management systems based on a centralized architecture. An example of this is software-configured networks SDN (Software Defined Networks), a technology for building communication network architectures based on the centralization of monitoring and control functions in a single point [4]. Centralization is achieved by separating network control functions (control plane) and data transmission functions (forwarding plane) in network equipment.

In traditional routers and switches, these functions are inseparable from each other, and each

element makes decisions independently and relatively independently (Fig. 1).



Fig. 1. Traditional network management

In accordance with the concept of SDN [6], it is taken out to transfer the management functions to a separate device - a controller, and to the switches leave only the function of traffic transfer. The entire logic of monitoring and managing network devices in SDN is implemented programmatically, which allows developers to create their own applications for monitoring and managing the network through the program interfaces (APIs) of the controller.

In the case of an abstract representation of the network topology in SDN (Fig. 2), the administrator should only write the rule “route from A to B = packet discard” in the management software platform, and it will always work, and changes in network topology will be automatically tracked in the network operating system (Network Operating System – NOS).

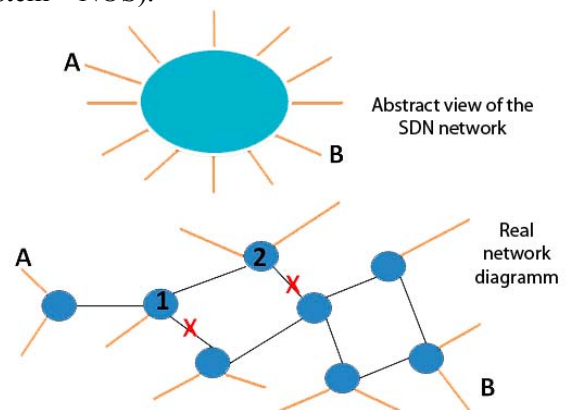


Fig. 2. SDN network management

The interaction between the controller and the switches is carried out through a protocol. NetFlow protocol is standardized for monitoring, and OpenFlow for network management.

In this case, monitoring and management are carried out at the level of flows, rather than individual packages. The rules in the switch are set up with the controller only for the first packet, then all subsequent packets of the flow use it.

The SDN architecture includes [5; 6]: SDN applications, SDN controller, control agents, whose functions are incorporated in OpenFlow switches, VflowVisor or the interface responsible for transferring control information, management and administration components (Fig. 3).

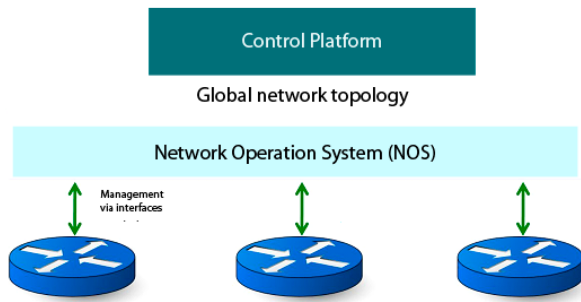


Fig. 3. SDN architecture

Applications contain requirements for the state and behavior of the network infrastructure, which are taken into account when monitoring and managing. The controller is a single centralized control point that monitors and controls the physical devices of the network through an open interface - the OpenFlow protocol. OpenFlow switches provide direct interaction between the network infrastructure and the management layer. The switchboard contains one or several redirection tables (flowtable), which contain all data about the streams of transmitted information. Records in the forwarding tables contain a set of fields with information about each packet (the number of the input and output port, the priority of the transmitted data, the counter and the types of actions that must be performed after the packet is processed (redirection, modification or reset). FlowVisor is responsible for distributing control information between data streams. By its nature, FlowVisor is a transparent proxy server between the switches and the controller. At the same time, FlowVisor determines which sets of flows belong to a particular network (switch) and, therefore, transfer control information to a specific controller. FlowVisor provides virtualization of control flow into separate network slices, each of these flows has its own control and transmission logic.

The management and administration components are static data sets that include external tasks: coordination of policies and rules established during the design of the SDN architecture, initial equipment configuration, and network resource allocation rules.

Based on the above description, SDN is a complex system of interaction of elements of both logical and physical nature, with a single intellectual point of control. The OpenFlow controller architecture consists of several levels, each of which responds to the charge of the necessary functionality. The controller acts as an element of response: it receives messages from the switches through control channels and generates responses that change the contents of the switching tables. The switch collects statistical data on the structure, state and characteristics of the data transfer level, creates

labels in the redirection tables and redirects them to the controller for making further decisions.

The interaction between the control level and the data transfer level is based on two protocols: OF-CONFIG, which allows you to configure separate ones to create a high-quality control information transmission channel and the OpenFlow protocol itself, which allows you to control packet forwarding and modification.

Selection the optimal structure of the computer network monitoring and management system

The advantage of centralized monitoring and control is the ability to form a holistic view of the network status, respectively, to calculate the global optimum control and load balancing.

Among the disadvantages of a centralized approach to monitoring and network management are:

1. Low survivability of the network, because in case of failure of the central controller, the network ceases to function. When reserving controllers, there are no clear instructions on how they are communicating and deciding on the primacy/transfer of functions.

2. It is not indicated on which communication channels the controller(s) and switches interact, according to the basic data transfer structure or parallel, and what happens when there are problems on the communication line.

3. A centralized monitoring and management system is a complex system, for the optimal management of which there is not enough information and resources. In such a system, in essence, it is necessary to solve a quadratic assignment problem (Quadratic Assignment Problem, QAP) — this is a well-known problem of discrete optimization, which is one of the most difficult tasks in this field [7].

The computational load on the central controller will be equal to K^m , where m is the number of end nodes and k is the number of switching nodes in the serviced segment. Solutions for managing such a complex system can be:

1. Decentralization (i.e., management of an autonomous network segment, which corresponds to the classical distributed approach according to the manager-agent scheme).

2. Creating a hierarchical structure. This reduces the computational load on the central node, and the degree of reduction will correspond to the ratio $\text{Log}_2(k + m)$. However, in such a case, the global optimum control [8]. The comparative degree of conformity of the selected models is characterized by a matrix of improvement factors.

$$\mathbf{R} = \left\| r_{ij} \right\|, \quad 1 \leq i \leq n, \quad 1 \leq j \leq m.$$

3. Application of heuristic or metaheuristic methods for optimizing large systems [9], in particular methods of taboo — search.

The optimization procedure is divided into several stages.

At the first stage — preliminary planning — the most common properties of the network are determined, in particular, the number and specifics of mobile services, network configuration parameters, etc.

At the second stage, an overview of the possible location of the switches is made, binding to the real network, the choice of methods for calculating transmission losses, the calculation of network resources. Based on this data and the selected transmission model, the switch parameters are planned — the size of the coverage area and the bandwidth resource. Some important parameters have a significant effect on the required channel resource, for example, the sensitivity and gain of transmitters of an SDN switch and SDN controller, cable losses and distribution medium, fading threshold, etc. Based on the geography of the network and the resource of the channel, it is possible to evaluate the various possibilities of creating a network segment using the optimization algorithm. The objective function is a combination of the achievable area of operation with a QoS of at least a given, optimal throughput with restrictions on costs. Geometric characteristics and capacity planning play a large role in network planning. When planning the geometric characteristics, the size of the network is determined, while the results of capacity planning determine the number of SDN switches used in the future and, accordingly, their capacity.

At the third stage, the adjustment and coordination of the parameters and structure of the network is made according to the results of testing each switch. According to the results of experimental studies carried out (if necessary) correction of the previous stages of the plan.

The goal of the network operator is to minimize costs (for example, by increasing the radius of the cells) so that the QoS values expressed in terms of the maximum allowed loss P_0^* and the GoS (GoS — Grade of Service) class indicators, denoted as P_b^* and P_d^* , meet the requirements. We formalize the objective function as follows:

$$\max_s R, \quad P_0 \leq P_0^*, \quad P_b \leq P_b^*, \quad P_d \leq P_d^*,$$

$S = \{RRR, CAC, R\}$ — Variety of optimization parameters

The basis of the integer combinatorial programming model used for the uplink is the classical minimization problem

$$\min \left(\sum_{j=1}^m c_j y_j + \mu \sum_{i=1}^n \sum_{j=1}^m u_i \frac{1}{r_{ij}} x_{ij} \right) \quad (1)$$

subject to normalization

$$\sum_{j=1}^m x_{ij} = 1, \quad i \in I \quad (2)$$

and additional restrictions

$$x_{ij} \leq y_j; \quad x_{ij}, y_j \in \{0;1\}; \quad i \in I, \quad j \in M \quad (3)$$

The first term in the objective function corresponds to the total normalized cost, where c_j is the resource consumption of the j -th switch.

Since $1/r_{ij}$ is proportional to the signal power from the i -th control point (CP) associated with the j -th switch, the second term describes the desired CP for which the total resource consumption is minimal. Since the criteria for finding a minimum for both terms are contradictory, a certain compromise coefficient is introduced. Condition (3) is a guarantee that each st CT is associated with a single switching node. Limiting condition (4) means that QDs are specified only for those points where switches are installed. Note that since the variables are binary, in each valid solution, all active connections can be assigned to only one switch.

It is proposed a sliding posteriori optimization algorithm. The concept of a balance between detailed search in the field of promising solutions and going to neighboring areas to find solutions of even better quality (lower value of the objective function) is implemented. However, such a search may require a lot of computation time. By searching in some promising area of solution space, you can miss other, perhaps even more promising areas. On the other hand, without an in-depth study of the neighborhoods of good solutions, we will only find low-quality solutions. The balance between an in-depth search in the vicinity of good solutions and the study of the entire solution space for finding other promising areas shifts in one direction or another according to the results of the previous analysis.

It can be seen that in the second case, local extremes are almost completely excluded from consideration.

In Fig. 4 shows graphs of the change in the integral component of the objective function — the total delay of routing to ensure data delivery with the required quality of service — when searching for the optimal placement of one of the switching nodes (SDN switches). Function 1 is calculated without regard to additional delay components, disconnections. Function 2 is calculated with these

components in mind. The smoothness of curve 1 is due to the connection and disconnection of users in the mode of independent transmission.

Curve 2 is smoother due to the summation of the components of the transmitted signal, which are random in nature and do not depend on each other. More importantly, when these components are taken

into account, the resulting required power of switching nodes decreases on average by about 4 – 5 %.

After optimizing the placement (Fig. 5), saving of the resource of switching nodes considering component packets during parallelization is more noticeable.

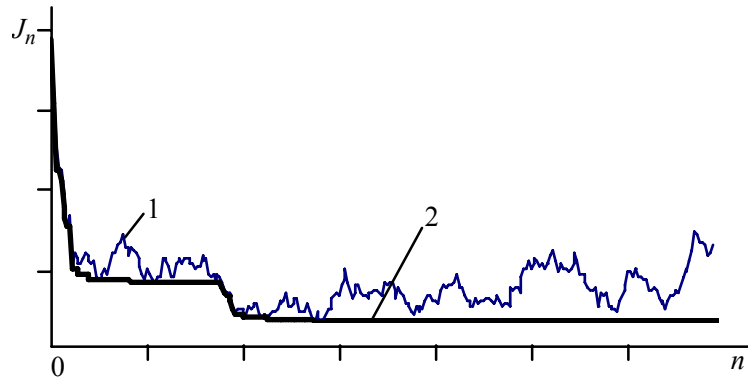


Fig. 4. Module modification of the resulting objective function in the optimization process: 1 — Classic taboo-search; 2 — Taboo-search with a sliding posteriori optimization

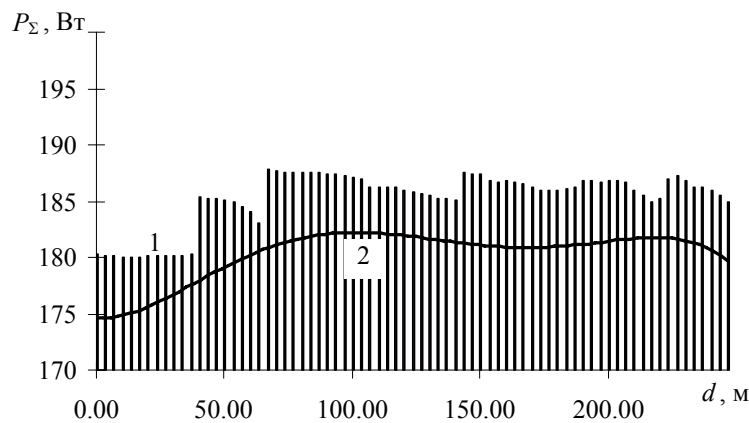


Fig. 5. Changing the parameter S_{Rr} of the objective function when the switching node moves along the horizontal coordinate: 1 — Classic taboo-search; 2 — Taboo-search with a sliding posteriori optimization

Thus, upon reaching the optimal number of hierarchy levels and the optimal number of devices (final and intermediate) at the same level, there is an improvement in the quality of service in a software-configured network.

Conclusions

Modern computer networks should serve resource-intensive applications such as voice and video, CAD and cloud services that generate huge amounts of traffic with a given quality, subject to limited resources.

Classical distributed systems for monitoring and managing a computer network are implemented according to the concept “manager-agent”, use MIBs and transmit messages via the SNMP protocol. The advantage of such systems is their distribution and ease of implementation, tested for

decades. The disadvantage is the control of each device separately. This introduces additional load on network resources and does not allow for efficient load balancing, since there is no coherent picture of the state. This architectural solution is suitable for office networks of small companies.

The centralized system architecture used in SDN networks allows concentrating all monitoring and management functions in a single central device — the controller. This allows you to calculate the global optimum control and load balancing. The disadvantage is the low survivability of the network, high required computing power of the central point, complexity of management due to the lack of information and resources.

A complex system management with using heuristic or metaheuristic methods for optimizing

large systems is a solution to the problem. An algorithm with sliding a posteriori optimization is suggested. Upon reaching the optimal number of hierarchy levels and the optimal number of devices (final and intermediate) on the same level, there is an improvement in the quality of service.

The centralized architecture of the system allows you to concentrate all the functions of monitoring and control in a single central device — the controller. The use of the controller as a single intelligent control point allows you to significantly simplify the logic of the network, and flow control instead of packets, to reduce the load on the network. The disadvantage of this approach is the low survivability of the network, the high required computing power of the central point, and the complexity of management due to the lack of information and resources. Obviously, such architectures and solutions should be used in large corporate networks.

In conclusion, it should be noted that, in addition to the architecture, for any monitoring and management system, it is important to develop policies and rules, load balancing, i.e. development of control actions on the network. It seems appropriate to use the concept of “optimal administrator”, which allows you to implement management most efficiently, regardless of the system architecture and staff qualifications.

REFERENCES

1. **Віноградов М. А., Савченко А. С.** Концепція управління корпоративною комп'ютерною мережею на основі психофізіологічних механізмів професійної діяльності людини / Наукові записки

Українського науково-дослідного інституту зв'язку: зб. наук. праць. — К. : УНДІЗ, 2013. — Вип. 3(27). — С. 5-14.

2. **Олифер В., Олифер Н.** Компьютерные сети: принципы, технологии, протоколы. — 5-е изд. — СПб. : Питер, 2016. — 992 с.

3. HPE One View [Electronic resource]. — Mode of access: <https://www.hpe.com/us/en/integrated-systems/software.html> — date of the application 15.07.2018 p.

4. **Göransson P.** Software Defined Networks: A Comprehensive Approach. Second Edition / Paul Göransson, Chuck Black, Timothy Culver — Elsevier, 50 Hampshire Street, 5th Floor, Cambridge, MA 02139, United States, 2017. — 409 pp.

5. Architecture SDN [Electronic resource] // Open Networking Foundation. — [2014]. — Mode of access: <https://www.opennetworking.org/> — date of the application 28.07.2018 p.

6. Software-Defined Networking: The New Norm for Networks [Electronic resource] // Open Networking Foundation. — [2012]. — Mode of access: <https://www.opennetworking.org/images/stories/downloads/sdn-resources/whitepapers/wp-sdn-newnorm.pdf>.

7. **Floudas C. A. and Pardalos P. M.** (Eds.) Encyclopedia of Optimization Second Edition / Springer Science+BusinessMedia, LLC, 2009. — 4626 pp.

8. **Ralph E. Steuer.** Multiple criteria optimization; theory, computation, and application / Wiley Series in Probability and Mathematical Statistics — Wiley, 1986, 546 pp.

9. **Gendreau M., Potvin J.-I.** Handbook of Metaheuristic. — Second Edition. — Springer New York Dordrecht Heidelberg London, 2010. — 668 pp.

Savchenko A. S., Vasylenko V. A., Kolisnyk O. V., Holiavkina T. V.

COMPUTER NETWORKS MONITORING AND MANAGEMENT METHODS

The distributed architecture of monitoring and management systems based on the SNMP protocol, the MIB databases and the centralized architecture based on the SDN network concept and the Openflow protocol are considered. The advantage of centralized monitoring and control is the ability to form a holistic view of the network status, respectively, to calculate the global optimum control and load balancing. The disadvantage is the low resiliency of the network, the complexity of managing a large system. Monitoring and management of such a complex system is possible with the help of decentralization, the creation of a hierarchical structure, the use of heuristic or metaheuristic methods for optimizing large systems. A method with sliding a posteriori optimization, which allows to achieve the optimal number of hierarchy levels and the optimal number of devices on the same level, is proposed.

Keywords: computer network, network monitoring, network management, SNMP protocol, SDN architecture, openflow.

Савченко А. С., Василенко В. А., Колісник О. В., Холявкіна Т. В.

МЕТОД МОНІТОРИНГУ ТА УПРАВЛІННЯ СУЧАСНИМИ КОМП'ЮТЕРНИМИ МЕРЕЖАМИ

Розглянуто розподілену архітектуру систем моніторингу та управління на основі протоколу SNMP і баз MIB та централізовану архітектуру на базі концепції мережі SDN і протоколу Openflow. Перевагою централізації моніторингу та управління є можливість сформувати цілісне уявлення про стан мережі, відповідно розрахувати глобальний оптимум управління і проводити балансування навантаження. Недоліком є низька відмовостійкість мережі, складність управління великою системою. Моніторинг та управління такою

складною системою можливе за допомогою децентралізації, створення ієрархічної структури, застосування евристичних або метаевристичних методів оптимізації великих систем. Запропоновано метод з ковзною апостеріорною оптимізацією, який дозволяє досягти оптимальної кількості рівнів ієрархії і оптимальної кількості пристроїв на одному рівні.

Ключові слова: комп'ютерна мережа, моніторинг мережі, управління мережею, SNMP-протокол, архітектура SDN, апостеріорна оптимізація.

Савченко А. С., Василенко В. А., Колисник Е. В., Холявкина Т. В.

МЕТОД МОНИТОРИНГА И УПРАВЛЕНИЯ СОВРЕМЕННЫМИ КОМПЬЮТЕРНЫМИ СЕТЯМИ

Рассмотрены распределенная архитектура систем мониторинга и управления на основе протокола SNMP, баз MIB и централизованная архитектура на базе концепции сети SDN и протокола Openflow. Преимуществом централизации мониторинга и управления является возможность сформировать целостное представление о состоянии сети, соответственно рассчитать глобальный оптимум управления и проводить балансировку нагрузки. Недостатком является низкая отказоустойчивость сети, сложность управления большой системой. Мониторинг и управление такой сложной системой возможно с помощью децентрализации, создания иерархической структуры, применения эвристических или метаэвристических методов оптимизации больших систем. Предложен метод со скользящей апостериорной оптимизацией, который позволяет достичь оптимального количества уровней иерархии и оптимального количества устройств на одном уровне.

Ключевые слова: компьютерная сеть, мониторинг сети, управление сетью, SNMP-протокол, архитектура SDN, апостериорная оптимизация.

Стаття надійшла до редакції 17.09.2018 р.

Прийнято до друку 26.09.2018 р.

Рецензент – д-р техн. наук, проф. Віноградов М. А.

О. В. Азаренко, д-р фіз.-мат. наук, проф.
Національний авіаційний університет
orcid.org/0000-0003-2927-5545
e-mail: azarenko_ev@ukr.net

М. В. Куклінський, канд. техн. наук, доц.
Національний авіаційний університет
orcid.org/0000-0002-2028-9206
e-mail: maximum_inc@ua.fm

А. С. Клімова, канд. техн. наук, доц.
Національний авіаційний університет
orcid.org/0000-0002-4721-2241
e-mail: asie@ukr.net

ФАКТОГРАФІЧНА ІНФОРМАЦІЙНА СИСТЕМА МУЛЬТИМЕДІЙНОЇ БАЗИ ДАНИХ

Вступ

Натепер у світі існує величезна кількість графічної інформації яка зберігається в цифровому вигляді. Не зважаючи на сучасні методи архівації та алгоритми стиснення, ця інформація займає надвеликий обсяг пам'яті на носіях. На відміну від попередніх років, коли загальний обсяг носіїв був малим, та залежав від багатьох факторів, зараз проблема обсягу не настільки критична.

Але з накопиченням у одному місці великої кількості мультимедійних даних, гарантовано, рано чи пізно стане питання про забезпечення їх послідовності, паралелізму, цілісності, безпеки та доступності, і тоді можна казати не про звичайне скупчення мультимедійних даних, а про повноцінну мультимедійну базу даних. Актуальність цих тверджень, також підтверджується елементарним бажанням користувача здійснювати легкий пошук, запит і маніпулювання актуальною для нього інформації в величезній колекції збережених мультимедійних даних. Проте для забезпечення оптимізації зберігання та обробки великої кількості графічного матеріалу необхідно цей матеріал структурувати.

Постановка проблеми

Будь яке структуроване або систематизоване об'єднання графічних об'єктів можна назвати базою даних, у нашому випадку мультимедійною базою даних, або базою зображень. Робота з такими базами передбачає насамперед пошук та ідентифікацію мультимедійних об'єктів які входять до неї.

Однак завдання ідентифікації, саме по собі, припускає інтелектуальну обробку отриманої інформації, що представляє певні складності. Безсумнівно, в задачах розпізнавання символів (розпізнавання тексту, автомобільних номерів, тощо) досягнуті величезні успіхи. Але, тим не

менш, будь-яких універсальних методів обробки та розпізнавання зображення, які за продуктивністю та якістю можна порівняти з людськими здібностями, немає [1].

Наприклад, у задачах, які ставляться перед експертними системами, потрібно більш глибокий інтелектуальний аналіз і високу швидкодію, цими самими властивостями повинні володіти роботизовані системи обслуговування. Тому обробка зображення в задачі розпізнавання є однією з центральних проблем.

Аналіз досліджень і публікацій та формулювання цілей статті

Відомо, що проблеми упорядкування та структуризації даних відрізняються високим рівнем невизначеності, неповнотою і фрагментарністю, а також великою часткою суб'єктивності [2]. Сучасні комп'ютерні технології пропонують розробникам і користувачам найрізноманітніші засоби створення, ведення та використання комп'ютерних баз даних і знань, які дозволяють кожному створювати їх на свій смак. Крім цього слід зауважити що, практично кожна база даних і знань будується на власній структурно-класифікаційній основі [3; 4].

Ураховуючи специфіку мультимедійної бази даних можна зробити висновок, що одним з шляхів побудови її ефективної інформаційно-управляючої системи є використання фактографічної інформації про її об'єкти [5].

Використання фактографічної інформації перш за все дозволить здійснювати морфологічний пошук, який дасть можливість більш коректного пошуку інформації. Крім цього, у поєднанні з функціями аналізу змісту зображення, з'явиться можливість знаходження графічних об'єктів виходячи з його змісту, що у свою чергу дозволить уникнути наповнювання бази даних однаковою або схожою інформацією.

Якість прийняття рішень у цьому випадку буде визначатися тільки якістю використовуваної первинної фактографічної інформації, а саме ступінь її адекватності, повноти, точності, надійності, своєчасності, наочності та однозначності.

Ще одним позитивним фактором застосування фактографічної інформації до мультимедійних об'єктів є відсутність чітких механізмів ідентифікації сутностей всередині цих об'єктів. Тому ціллю статті є розробка таких механізмів, які б дозволили структурувати і структуровано зберігати мультимедійні дані за допомогою фактографічної інформації.

Фактографічна інформаційна система

Фактографічна інформаційна система (ФІС), як і люба інформаційна система є основним засобом, інструментарієм рішення задач інформаційного забезпечення. Співвідношення понять, пов'язаних з інформаційним забезпеченням, можна відобразити у вигляді наступної схеми (рис. 1) [5].



Рис. 1. Схема поняття інформаційного забезпечення

Як правило ФІС накопичує і зберігає дані у вигляді сукупності інформації яка відображає який-небудь факт, подію тощо. Структура кожного типу інформаційного об'єкта складається з кінцевого набору реквізитів, аспектів та характеристик відомостей для об'єктів даної предметної області.

Архітектуру підсистеми подання та обробки інформації ФІС можна представити так (рис. 2) [5].

Дана архітектура визначає локальні представлення про предметну область користувачів-абонентів інформаційної системи та їх уявленнями про власні інформаційні потреби. На основі аналізу цих уявлень визначається інформаційно-

логічна схема предметної області (опис об'єктів), та концептуальна модель використання інформаційної системи.

Найнижчий рівень подання інформації в фактографічних інформаційних системах виражається внутрішньою схемою бази даних, що визначає структуру організації та особливості зберігання інформаційних масивів, у яких і знаходяться власне самі дані [3; 5].

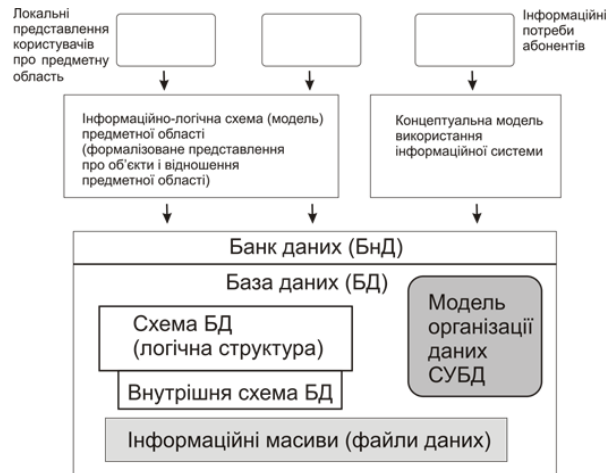


Рис. 2. Підсистема подання та обробки інформації ФІС

Технологія реалізації мультимедійної бази даних

При проектуванні та розробці інформаційної системи керування мультимедійною базою даних, треба враховувати, що прямий вплив на технології їх створення мають основні якості та особливості її даних. Відомо, що мультимедійні дані наділені низкою цікавих особливостей притаманні тільки їм. По-перше вони, зазвичай характеризуються великим об'ємом, а по-друге, зазвичай, пошук цих даних відбувається не за їхнім вмістом, а за суб'єктивним описом цього вмісту.

Дослідивши і розглянувши способи збереження мультимедійних даних, можна зробити висновок, що реляційні та об'єктно-орієнтовані бази даних не добре пристосовані для великих мультимедійних даних. У реляційних базах даних реалізація такого збереження є досить складною, оскільки файл не може зберігатися як один цілий об'єкт, що призводить до розбиття його на частини, що, в свою чергу, уповільнює обробку мультимедійних даних та впливає на рівень безпеки. Об'єктно-орієнтовані бази даних, на відміну від реляційних, майже не мають достатньо добре налаштованих систем керування, які б достатньо легко можна було пристосувати до мультимедійних даних. Найбільш прийнятною є документо-орієнтована база даних, перевагою якої є можливість зберігати мультимедійні

дані у вигляді документів, не поділяючи їх на частини, а технологією, яка найбільш підходить до керування цих баз є технологія NoSQL.

Хоча частина характеристик NoSQL не є унікальною, все ж вони мають ряд вагомих переваг, які полегшують та пришвидшують роботу, забезпечують більшу надійність. А для ще більшого пришвидшення можна застосувати підходи до збереження мультимедійних даних з застосуванням сховищ даних.

Організація пошуку мультимедійних даних

Операції з пошуку, фільтрації та сортування даних реалізують найпростіші інформаційно-довідкові потреби користувачів, але є, мабуть, найбільш частими при роботі з базами даних. Тому в фактографічній інформаційній системі мультимедійної бази даних необхідно звернути на них особливу увагу, особливо на операцію пошуку.

Засоби ФІС дозволяють крім контентного пошуку (пошуку за змістом) здійснювати повнотекстовий пошук, але необхідно враховувати ряд особливостей.

Алгоритм пошуку повинен аналізувати зміст мультимедійних даних, наприклад, колір представлених на ньому об'єктів, їх форму, текстуру, композицію сцени. За відсутності можливості проаналізувати сцену під час пошуку розглядаються метадані: ключові слова, мітки тощо.

Проте не для усіх таких даних можна застосувати пошук за змістом. Потенційні області застосування алгоритмів пошуку за змістом:

- пошук зображень в мережі Інтернет;
- каталогізація зображень творів мистецтва;
- організація роботи з архівами фотографічних знімків;
- організація каталогів роздрібного продажу товарів;
- медична діагностика захворювань;
- запобігання злочинів і заворушень;
- контроль за вмістом масивів зображень, тощо [6].

Використання у ФІС пошуку за змістом передбачає, що система робить пошук на основі вхідного зображення, яке вказується користувачем. Користувач може подати на вхід як існуюче зображення, так і грубий начерк необхідного результату (розмітку на кольорові області або прості геометричні форми) (рис. 3). При даному способі побудови запитів не виникає труднощів, пов'язаних з представленням до зображення наборів слів. Алгоритми, які входять до блоку обробки, можуть мати різні способи опису та роботи з вхідним зображенням, але всі результуючі екземпляри зображень повинні мати спільні елементи з входом, зазначеним користувачем.

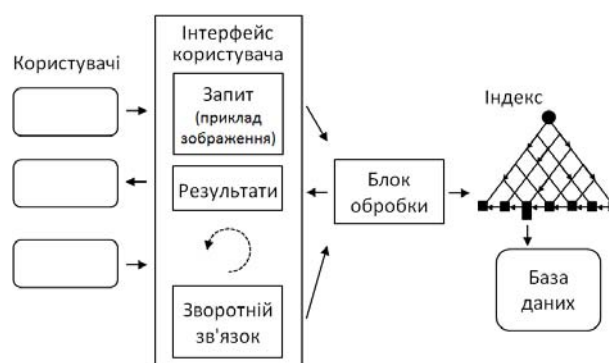


Рис. 3. Система пошуку зображень за змістом

До найпростіших алгоритмів можна віднести пошук за інтенсивністю зображення.

Сутність алгоритму полягає у зменшенні порівнюваних зображень до розміру 15×15 пікселів. Потім визначається інтенсивність Y цих зображень, залежно від колірної моделі, за формулою (для колірної моделі RGB) [7].

$$Y = 0,299 \cdot \text{Red} + 0,587 \cdot \text{Green} + 0,114 \cdot \text{Blue}.$$

Обчислення інтенсивності дає можливість порівнювати зображення не звертаючи увагу на їх кольори. Після обрахунку інтенсивності усіх пікселів в матрицях 15×15 , можна дізнатися відношення інтенсивності кожного пікселя до середнього значення інтенсивності усієї матриці. Дані відношення необхідні для формування одномірного масиву довжиною 225. Далі за формулою

$$P = \frac{\text{array1} \& \text{array2}}{225} \cdot 100 \%,$$

де P — відсоток подібності, $\text{array1} \& \text{array2}$ — повертає масив, що містить всі значення array1 , які присутні в array2 , вираховується відсоток подібності двох зображень.

До складніших алгоритмів можна віднести пошук з використанням нейромережевих класифікаторів та ін.

Хоча пошук на основі контенту є досить зручним, та все ж він більше пристосований до статичних зображень, а не для відео, і його реалізація дуже непроста.

Засоби ФІС дозволяють також здійснювати повнотекстовий пошук. Перевагою повнотекстовому пошуку є можливість морфологічного та семантичного пошуку.

Проте для повнотекстового пошуку необхідне постійне наповнення бази фактографічною інформацією. Фактографічна інформаційна система накопичує відомості про кожний конкретний мультимедійний об'єкт в базі даних, ставить у відповідність запис, що складається з визначеного набору характерних для цього об'єкту реквізитів, таких, наприклад, як форма, колір, опис, жанр, тип і т. ін.

Комплект інформаційної бази в фактографічній системі включає, як правило, обов'язковий процес структуризації вхідної інформації. Структуризація при цьому здійснюється через визначення інформаційних об'єктів певного типу, інформація про яких береться з заповнених реквізитів [5].

Структуризація фактографічних даних

Структуризація даних, перш за все, необхідна для виконання основних операцій з ними. Коли кількість об'єктів для пошуку потенційно велика або кількість пошукових запитів є досить істотною, проблема повнотекстового пошуку часто ділиться на два завдання: індексації та пошуку. Етап індексації «сканує» текст усіх реквізитів і створює список пошукових термінів. На стадії пошуку, при виконанні конкретного запиту, надсилається тільки індекс, а не текст оригінального реквізиту. Індикатор робить запис в індекс для кожного терміну або слова, знайденого в базі реквізитів.

Дуже часто в мультимедійних базах даних об'єкти намагаються структурувати за ієрархічною моделлю. Тобто спочатку організувати їх за певними категоріями, потім розбити їх на підкатегорії, а ті в свою чергу, на більш вузькі категорії. Аналогічним чином організовується фактографічна інформація. Причому чим вища категорія, тим менше вона змінюється в базі.

Проте, створення моделі для зберігання ієрархічних даних непросте завдання.

Стандартною технікою для моделювання ієрархічних структур в технології NoSQL є вкладені множини [8]. Вона широко використовується в реляційних базах даних, але вона ідеально може бути застосовна до реквізитів фактографічної системи.

Ієрархічна структура це модель, де чітко відстежується зв'язок батьків і нащадків. У випадку з ієрархічною структурою кожний вузол повинен мати свій унікальний ID і ID свого батька (рис. 5). Самі ID не мають ніякого відношення до даних, вони лише слугують унікальними визначниками вузла.

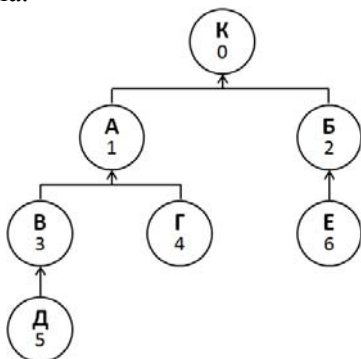


Рис. 5. Схема ієрархічної структури даних

Ідея вкладених множин полягає в тому, що замість ID батька використовується ліве і праве значення вузла, тобто ID лівого і правого сусіда того самого рівня. Причому ID сусідів отримуються за особливим алгоритмом (рис. 6) [9].

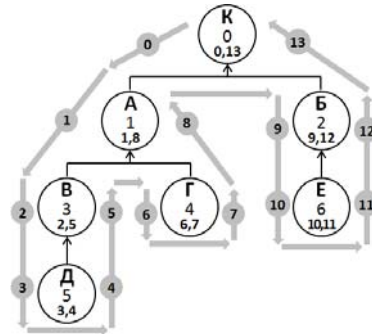


Рис. 6. Схема ієрархічної структури з вкладеними множинами, та алгоритм отримання ID сусідів

Вкладені множини дуже ефективні при отриманні списку нащадків елемента. Але є і свої недоліки, наприклад, при видаленні або додаванні вузла необхідно виконувати велику кількість оновлених даних в базі. Тому ця структура досить ефективна лише для незмінних даних, у зв'язку з чим можна рекомендувати для використання у фактографічній інформаційній системі концепцію сховища даних.

Висновок

Фактографічні інформаційні системи оперують фактичними відомостями, представленими у вигляді спеціальним чином організованих сукупностей формалізованих записів даних. Застосування підходів ФІС, методів контентного та повнотекстового пошуку, технології NoSQL та концепції сховища даних до об'єктів мультимедійної бази даних, дасть можливість суттєво оптимізувати роботу бази та забезпечити її більшу надійність.

ЛІТЕРАТУРА

1. **Shalkoff R. J.** Digital image processing and computer vision. — New York-Chichester-Brisbane-Toronto-Singapore: John Wiley & Sons, Inc., 1989. — 489 p.
2. **Бойко В. В., Савинков В. М.** Проектирование баз данных и информационных систем. — М. : Финансы и статистика, 1989. — 350 с.
3. **Гагарина Л. Г., Киселев Д. В., Федотова Е. Л.** Разработка и эксплуатация автоматизированных информационных систем: учеб. пособие. — М. : ИД «Форум»: ИНФРА-М, 2007. — 384 с.
4. **Емельянова Н. З., Партыка Т. Л., Попов И. И.** Основы построения автоматизированных информационных систем: учеб. пособие. — М. : ФОРУМ: ИНФРА-М, 2007. — 416 с.

5. **Гайдамакин Н. А.** Автоматизированные информационные системы, базы и банки данных. Вводный курс: учеб. пособие. — М. : Гелиос АРВ, 2002. — 368 с.

6. **Datta R., Joshi D., Li J. and Wang J.Z.** 2008. Image retrieval: Ideas, influences, and trends of the new age. ACM Comput. Surv. 40, 2, Article 5 (April 2008). — 60 p.

7. **Селянкин В. В., Скороход С. В.** Анализ и обработка изображений в задачах компьютерного зрения: учеб. пособие. — Таганрог: Изд-во ЮФУ, 2015. — 82 с.

8. NoSQL data modeling techniques / <https://highlyscalable.wordpress.com/2012/03/01/nosql-data-modeling-techniques/>

9. Nested Set/<http://devacademy.ru/posts/nested-set>.

Азаренко О. В., Куклінський М. В., Клімова А. С.

ФАКТОГРАФІЧНА ІНФОРМАЦІЙНА СИСТЕМА МУЛЬТИМЕДІЙНОЇ БАЗИ ДАНИХ

У статті приведено вирішення проблеми підвищення ефективності керування мультимедійними об'єктами, які зберігаються в базі даних. У якості рішення розглядається застосування фактографічних інформаційних систем, причому не тільки для реалізації довідкових функцій, але і для вирішення задач обробки даних, таких як введення, зберігання, сортування, пошук та структурування даних. У статті розглядаються основні проблеми, які виникають при проектуванні баз даних з мультимедійним контентом. Дані проблеми, зазвичай, викликані характеристиками, які притаманні лише мультимедійним даним. Саме з урахуванням цих характеристик пропонується разом з фактографічною інформаційною системою використання NoSQL у якості додаткової технології для реалізації мультимедійної бази даних, застосування концепції сховища даних та схеми ієрархічної структури з вкладеними множинами. Запропоновані підходи створюють умови щодо підвищення продуктивності функціонування інформаційних систем мультимедійних баз даних необхідні для представлення підсумкових результатів, які пред'являються користувачами.

Ключові слова: мультимедійна база даних; фактографічна інформаційна система; система керування базою даних; NoSQL; концепція сховища даних; ієрархічна структура з вкладеними множинами.

Azarenko O., Kuklinskyi M., Klymova A.

FACTOGRAPHIC INFORMATION SYSTEM OF MULTIMEDIA DATABASE

The article provides a solution to the problem of improving the efficiency of managing multimedia objects that are stored in the database. The use of factographic information systems is considered as a solution, and not only for the implementation of reference functions, but also for solving data processing tasks such as data entry, storage, sorting, searching and structuring. The article discusses the main problems encountered in the design of databases with multimedia content. These problems are usually caused by characteristics that are inherent only in multimedia data. It is with these characteristics in mind that the use of NoSQL as an additional technology for the implementation of a multimedia database, the application of the data warehouse concept and a hierarchical structure with nested sets is proposed along with the factographic information system. The proposed approaches will create conditions for improving the performance of the information systems of multimedia databases necessary for the presentation of the final results presented by users.

Keywords: multimedia database; factographic information system; database management system; NoSQL; data warehouse concept; hierarchical structure with nested sets.

Азаренко Е. В., Куклинский М. В., Климова А. С.

ФАКТОГРАФИЧЕСКАЯ ИНФОРМАЦИОННАЯ СИСТЕМА МУЛЬТИМЕДИЙНОЙ БАЗЫ ДАННЫХ

В статье приведено решение проблемы повышения эффективности управления мультимедийными объектами, которые хранятся в базе данных. В качестве решения рассматривается применение фактографических информационных систем, причем не только для реализации справочных функций, но и для решения задач обработки данных, таких как ввод, хранение, сортировка, поиск и структурирование данных. В статье рассматриваются основные проблемы, возникающие при проектировании баз данных с мультимедийным контентом. Данные проблемы, как правило, вызваны характеристиками, которые присущи только мультимедийным данным. Именно с учетом этих характеристик предлагается вместе с фактографической информационной системой использование NoSQL в качестве дополнительной технологии для реализации мультимедийной базы данных, применение концепции хранилища данных и схемы иерархической структуры с вложенными множествами. Предложенные подходы создадут условия для повышения производительности функционирования информационных систем мультимедийных баз данных необходимых для представления итоговых результатов, которые предъявляются пользователями.

Ключевые слова: мультимедийная база данных; фактографическая информационная система; система управления базой данных; NoSQL; концепция хранилища данных; иерархическая структура с вложенными множествами.

Стаття надійшла до редакції 04.09.2018 р.

Прийнято до друку 18.09.2018 р.

Рецензент – д. т. н., проф. Зіатдінов Ю.К.

УДК 004.056.5:35.078.3(02)

DOI: 10.18372/2310-5461.39.13083

В. В. Бараннік, д-р техн. наук, проф.
Харківський національний університет Повітряних Сил імені Івана Кожедуба
orcid.org/0000-0002-2848-4524
e-mail: vvbar.off@gmail.com

Д. В. Бараннік
Харківський національний університет радіоелектроніки
orcid.org/0000-0003-4235-300X
e-mail: d.v.barannik@gmail.com

А. Д. Сорокун, аспірант
Національний авіаційний університет
orcid.org/0000-0001-8469-641X
e-mail: sorokun@gmail.com

М. В. Дворський
Харківський національний університет Повітряних Сил імені Івана Кожедуба
e-mail: dmv06@i.ua

ВДОСКОНАЛЕННЯ МЕТОДІВ КОМПЕНСАЦІЇ РУХУ ДИНАМІЧНИХ ОБ'ЄКТІВ У ВІДЕОПОТОЦІ В СИСТЕМІ ВІДЕОКОНФЕРЕНЦІВ'ЯЗКУ

Вступ

У зв'язку з бурхливим розвитком мережевих, а також комунікаційних технологій, збільшеною продуктивністю комп'ютерів і з необхідністю обробляти все більшу кількість інформації (як локальну, мережеву так і міжмережеву) зростає роль програмного забезпечення і устаткування.

Віддалений доступ, дистанційна освіта і управління, а також кошти на проведення відеоконференцій, переживають період бурхливого зростання.

Все це призначає полегшити і збільшити ефективність взаємодії людини з комп'ютером, а також і груп людей з комп'ютерами, об'єднаними в мережу.

Відеоконференції надають можливість працювати і спілкуватися в режимі реального часу, а також використовувати колективні додатки, інтерактивного обміну інформацією.

Відеоконференції починають розглядати не тільки як щось експериментальне, а й як часткове вирішення проблеми автоматизації діяльності, що дає суттєву перевагу порівняно з традиційними рішеннями.

В основі алгоритмів кодування відеопотоку лежить надмірність інформації і особливості людського сприйняття візуального зображення. Зображення змінюється плавно, невеликі спотворення при відновленні зображення стають непомітними. Так з'явилися алгоритми кодування відеопотоку з втратою якості. Такі алгоритми дозволяють ефективно кодувати відеопотік, але не гарантують точне відновлення інформації.

Аналіз останніх досліджень і публікацій

Проаналізувавши останні наукові публікації можна сказати, що кодеки на базі стандарту MJPEG враховують тільки внутрішню кадрову залежність відліків відеоінформації, і тому мають низьку обчислювальну складність, але при цьому поступаються за ефективністю кодування.

H.264, MPEG-4 Part 10 або AVC (Advanced Video Coding) — ліцензований стандарт стиснення відео, призначений для досягнення високого ступеня стиснення відеопотоку при збереженні високої якості. Стандарт H.264 надійний, підтримується практично будь-якими пристроями і дає гарне стиснення. Відео, якості HD, буде відображатися зі швидкістю потоку не більше 7–8 Мбіт/с, у той час як попередній стандарт (HD, MPG-2) вимагав 12–20 Мбіт/с, приблизно в два рази більше.

Новий стандарт в кодеку H.265 зміг суттєво зменшити розміри стислих файлів і тим самим заслужив міжнародне визнання, як засіб просування нових форматів відео. У H.265 використані нові технології стиснення і «розумна» модель кодування/декодування, що дозволяє економно використовувати пропускні ресурси каналу. Кодек розроблявся з урахуванням усіх особливостей 4К (підтримку 10-бітного відео, високу частоту кадрів).

З моменту появи H.264 проводилися численні порівняння цього стандарту і MPEG. Результати, зазвичай, показували виграш в 1–3 дБ стандарту H.264 в широкому діапазоні швидкостей кодування. Візуально відео, в стандарті H.264, також

виглядає краще (багато в чому завдяки використанню деблочного фільтра). Відзначимо, що для високотекстурованих зображень великої різниці не спостерігається. У багатьох тестах різниця по ефективності кодування між окремими відекодеками H.264 досягає двох і більше разів. Отже, будь то MPEG або H.264 — основна ефективність кодеків заснована на нюансах реалізації.

Мета статті (постановка завдання) — проведення дослідження методів компенсації руху динамічних об'єктів в системі відеоконференцз'язку.

Виклад основного матеріалу. Відеоконференція (від англ. *videoconference*) — область інформаційної технології, що забезпечує одночас-

но двосторонню передачу, обробку, перетворення та представлення інтерактивної інформації на відстань в режимі реального часу за допомогою апаратно-програмних засобів обчислювальної техніки [1].

Взаємодію в режимі відеоконференції також називають сеансом відеоконференцз'язку.

Відеоконференцз'язок — це телекомунікаційна технологія інтерактивної взаємодії двох і більше віддалених абонентів, за якої між ними можливий обмін аудіо- і відеоінформацією в реальному часі, з урахуванням передачі керуючих даних (табл. 1). Діаграма, що показує обсяг інформаційного потоку залежно від розміру кадру і глибини оцифровки пікселів, показана на рис. 1.

Таблиця 1

Характеристики значень середньої швидкості потоку некованого відеоінформації залежно від просторового дозволу і частоти кадрів для комплексів ВКЗ у відомчих системах управління

Рівні якості відеозображень	Формат GIF	Нормальний (SD)	Підвищений (ED)	Високий (HD)	Просунутий (Full HD)	Advantage HD
Кількість рядків	320 – 352	640	720	1280	1280 – 1920	1920 – 2048
Роздільна здатність по вертикалі	240 – 288	480 – 576	480 – 576	720	720 – 1080	1080
Частота кадрів/сек	24 – 30	24 – 30	50	50	24 – 30; 50	48; 60
Середня швидкість (Мбіт/сек)	66	252	500	1105	1500; 2500	2548; 3180

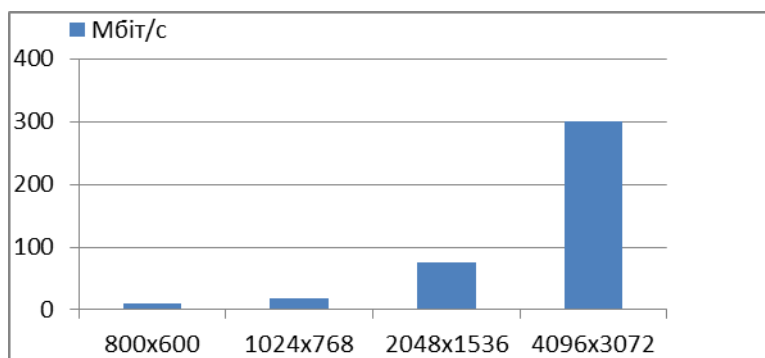


Рис. 1. Обсяг інформаційного потоку (Мбіт/с) залежно від розміру кадру і глибини оцифровки пікселів (частота кадрів 50 кадрів в с)

Наведені оцінки виконані на основі аналізу основних характеристик телекомунікаційних технологій, що використовуються при організації ВКЗ в системі управління військами і оцінок необхідних обсягів відеоінформаційного ресурсу ВКЗ залежно від необхідного просторового дозволу відеозображень і частоти кадрів. При тенденції зростання обсягів відеоінформації і не забезпечення відповідними даними обсягами продуктивності технологій передачі та обробки від-

еоінформації в комплексах ВКЗ виникають умови порушення категорій безпеки відеоінформаційного ресурсу ВКЗ — доступності та цілісності [1].

Висока якість звуку і повноекранне відео, оперативний обмін документами і даними (що дозволяють відеоконференції) дає цьому інструменту дистанційного спілкування найширший спектр практичного застосування. На сьогодні ці системи вже знайшли застосування у великих

компаніях, юридичних фірмах, в медицині та збройних силах. Після телефонних розмов інформація, яку отримують від співрозмовника слухачі, досягає, в середньому, до 10 % від загального обсягу інформації.

Під час телефонних переговорів з можливістю обміну даними, обсяг засвоєної інформації може бути збільшений приблизно до 25 %.

У разі якщо є можливість протягом бесіди візуально стежити за співрозмовником, є можливість забезпечити засвоєння інформації до 60 %. Але не тільки ця статистика переконує нас в тому, що відеоконференція дозволяє забезпечувати зв'язок нового рівня.

На практиці, відеоконференція — це незамінний помічник в управлінні і взаємодії військовими підрозділами, які територіально рознесені, консультування в управлінні військами досвідченими фахівцями, у забезпеченні морально-психологічної підтримки військовослужбовців в зонах проведення бойових дій, в телемедицині, у передачі аудіовізуальної передачі з поля бою. При цьому немає ніякої необхідності відправляти їх в дорогу відрядження. Економія на відрядженні витрат це не всі переваги, головне — за допомогою використання відеоконференції збільшується ефективність роботи.

Відеоконференція може бути організована по дротових та бездротових каналах зв'язку. Провідні канали відрізняються від бездротових швидкістю передачі даних, вартістю побудови, простотою реалізації.

Останнім часом набули поширення системи доступу до Інтернету, що базуються на використанні систем супутникового зв'язку. Оскільки передавальне обладнання коштує досить дорого, багато компаній використовують системи DirecPC. Найчастіше при роботі з Інтернет вхідний трафік (тобто, «з Інтернет») набагато вище вихідного. Системи DirecPC як приймальні пристрої використовують супутникові антени, а передають інформацію від користувачів в Інтернет по звичайних наземних каналах зв'язку. Звичайні супутники зв'язку знаходяться на стаціонарних орбітах на висоті близько 35 км над Землею. Нові низькоорбітальні супутники (low-orbit satellites) працюють на орбітах, максимально наближених до земної поверхні, що дозволяє їм приймати сигнали навіть від малопотужних передавачів. Такі супутники споживають менше енергії, а їх запуск і експлуатація обходиться значно дешевше традиційних супутникових систем зв'язку. Використання низькоорбітальних супутників робить можливим користуватися послугами зв'язку, перебуваючи в будь-якій точці земної кулі.

Варіанти технологічної реалізації, телекомунікаційна мережа зазвичай містить різноманітні апаратні і програмні компоненти, яким необхідно працювати спільно, щоб передавати інформацію. Різні компоненти мережі «спілкуються» один з одним, дотримуючись певних правил, що дозволяє їм працювати всім разом. Такий набір правил, що регулює процес передачі даних між двома точками мережі, називається протоколом (protocol). Кожен пристрій в мережі має правильно «розуміти» протокол іншого пристрою.

Ефективність систем ВКЗ, у цій статті, розглядається, як оперативність передачі відеопотоку.

Методи стиснення поділяють на дві групи: методи з втратою якості зображень і методи без втрати якості. Метод стиснення зображення без втрат — це метод, при якому не проводиться ніякої втрати якості зображення порівняно з вихідним [2]. Нестиснене зображення математично ідентичне його оригіналу. Стиснення без втрат зазвичай забезпечує менші коефіцієнти стиснення, ніж стиснення з втратами.

Існуючі методи стиснення не забезпечують ефективне функціонування систем об'єктивного відеоконтролю. Це проявляється в затримці відображення інформації на екрані оператора, в низькій якості отриманої інформації.

Компенсація руху є однією з найважливіших складових частин стандартів MPEG 1 і MPEG 2. Метод компенсаційного передбачення руху дозволяє значно зменшити часову надмірність відеопотоку [4]. Якщо наступний кадр містить зсунуті частини попереднього кадру, то в цьому випадку вигідно передавати не весь кадр, а тільки інформацію про рух і зміни зрушеного пікселя.

Алгоритми компенсації руху можна провести за такими критеріями:

- аналізований елемент — кадр, блоки, або об'єкти;
 - тип руху — операції паралельних зрушень, поворотів, масштабування;
 - міра прийняття рішення.
- Існують такі методи компенсації руху:
- піксельний метод;
 - об'єктний метод;
 - метод зіставлення блоків.

Піксельний метод є одним з найбільш ранніх методів компенсації руху. Компенсація проводиться окремо для кожного пікселя кадру, що розглядається клас перетворень — лінійні зсуви.

Підхід заснований на припущенні, що яскравість можна наблизити лінійною функцією від положення точки в кадрі. Це припущення справедливо тільки для порівняно невеликій околиці цієї точки, що істотно знижує область застосування даного методу і дозволяє йому правильно

оцінювати лише невеликі зрушення. Це обмеження можна подолати, оцінюючи не саме вектор зсуву, а його різницю з деяким вектором передбачення, який розташований ближче до шуканого вектора, ніж нульовий. У загальному випадку, коли рух може становити десятки пікселів, вектор зсуву шукається за допомогою ітеративного алгоритму — на кожному кроці відбувається уточнення знайденого на попередньому етапі значення. Як початкове наближення можна взяти вектор зсуву для цієї самої точки, знайдений при обробці попереднього кадру. Цей метод має ряд серйозних недоліків, унаслідок чого в даний час він являє собою чисто теоретичний інтерес і практично ніде не використовується. Основні його недоліки — висока складність, низька точність і великий обсяг інформації.

Об'єктний метод є попередником методу зіставлення блоків, де як елемент компенсації виступає прямокутний блок кадру і компенсації виступає прямокутний блок кадру і розглядаються лінійні зсуви.

Метод зіставлення блоків ґрунтується на тому, що об'єкти і їх місце розташування на кадрі з плином часу змінюються незначно. Тоді в околиці будь-якої точки кадру це зміна з високим ступенем точності можна наблизити паралельним перенесенням цієї околиці на деякий вектор.

При блоковому підході (об'єктний метод) для кожного блоку компенсація проводиться незалежно від сусідніх блоків. Виходячи з того, що рух по сцені здійснюють об'єкти, необхідно, щоб компенсації по всіх блоках одного і того самого об'єкта давали один і той же результат. Це можна зробити, якщо співвіднести кожному блоку кадру той чи інший об'єкт руху сцени. Після цього можна буде оцінювати сумарну помилку компенсації по всіх блоках.

Процес сегментації може відбуватися незалежно від процесу пошуку параметрів руху, або і те, і інше може визначатися в рамках єдиного процесу, що повторюється ітеративно. У першому випадку підставою для сегментації слугує зазвичай яскравісна інформація, у другому — сегментація проводиться з урахуванням знайдених параметрів руху, які потім уточнюються. Іноді сегментація кадру на об'єкти застосовується після визначення векторів зсуву для окремих блоків з метою корекції знайденого векторного поля.

Таким чином, в рамках запропонованого методу пропонується таке:

– накопичувати інформацію про фон в тимчасовій площині (умовою тимчасових рамок накопичення інформації слугує різка зміна фонові частини сцени) і акумуляцією її у вигляді єдиного фону для деякої послідовності кадрів. Крім

того, можливо аналогічне накопичення інформації про рухомі об'єкти сцени з урахуванням характеру їх руху;

– проведення одночасного побудови різничевого зображення сцени з заданим порогом і сегментації, виділяються об'єктів руху (для сегментації пропонується використовувати інформацію про восьмизв'язний околиці пікселя зображення). Крім того, на етапі сегментації фільтрується шум, який залишився після різничевого порівняння із заданим порогом.

Використання запропонованого методу дозволить підвищити якість компенсації руху за рахунок згладжування випадкових викидів в полі векторів руху, властивих блоковим методам. Накопичення інформації в тимчасовій площині дозволить знизити рівень зашумленості сцени, а також дозволить підвищити ступінь стиснення відеоряду.

Для підвищення працездатності і якості роботи запропонованого методу необхідно виробити критерій, на підставі якого буде відбуватися обмеження часової площині накопичення інформації по сцені. Залежно від типу розв'язуваних практичних завдань даний критерій може відповідати різним вимогам. Так, наприклад, для відеофільмів якість зображення грає дуже важливу роль.

Відповідно, вимоги будуть пред'являтися до якості зображення всієї сцени (контрастність, освітленість). А ось, наприклад, для охоронних систем, в першу чергу, буде корисна інформація, що дозволяє ідентифікувати об'єкти руху, в той час, як значення фону буде другорядним.

Також являє інтерес розробка підходів до накопичення інформації по об'єктах руху (аналогічно накопичення інформації про фонові частини сцени) в тимчасовій площині з урахуванням характеру їх руху.

Даний підхід є одним з найбільш перспективних і обіцяє стати популярним у найближчому майбутньому, хоча в даний час має досить високу обчислювальну складність. Потенційно це найбільш точний і стійкий до шуму метод (при правильно виконаній сегментації).

Метод зіставлення блоків, точніше, клас методів, є логічним наслідком піксельного методу динамічних об'єктів, усуває більшу частину його недоліків, оскільки одиницею компенсації в ньому прийнятий прямокутний блок (зазвичай квадрат 16×16 пікселів або меншого розміру). Рух також шукається в класі лінійних зсувів, тому описується такий рух двовимірним вектором зміщення для кожного блоку.

Основне припущення методу, за час, що проходить між двома послідовними кадрами,

об'єкти в сцені і їх місце розташування змінюються незначно. Тоді в околиці будь-якої точки кадру це зміну, з досить високим ступенем точності, можна наблизити паралельним перенесенням цієї околиці на деякий вектор. Насправді, переважна більшість звичайних відеопослідовностей задовольняють цьому обмеженню, за винятком ділянок різкої зміни сцени, тобто характер руху об'єктів можна вважати майже всюди безперервним.

Різні модифікації цього підходу розрізняються тим, яким чином знаходиться мінімум функції помилки компенсації у всій області. Перевіркою всього декількох точок в області можна локалі-

зувати цей мінімум. Алгоритм, за яким ці точки вибираються, називається шаблоном.

Методи, засновані на шаблонах, демонструють непогану швидкість роботи, проте часто знаходять локальний мінімум замість глобального. Як перевага можна відзначити те, що пошук вектора руху для кожного окремого блоку не залежить від результатів пошуку в сусідніх блоках і в попередньому кадрі, що робить метод більш ефективним при дуже інтенсивному і складному русі.

Провівши аналіз даних методів виявлено їх основні переваги та недоліки, які представлені в табл. 2.

Таблиця 2

Недоліки та переваги методів компенсації руху

Метод компенсації руху	Переваги	Недоліки
Піксельний метод	–	Висока складність, низька точність, великий об'єм інформації
Об'єктний метод	Стійкий до шуму метод	Висока обчислювальна складність
Метод зіставлення блоків	Висока точність	Не висока швидкість обробки

Для підвищення ефективності роботи методу зіставлення блоків використовують різні шаблони пошуку схожих блоків на сусідніх кадрах.

Для оптимальної роботи відеоконференцзв'язку в системі управління та оперативного зв'язку пропонується розробка нового шаблону — шеститочкового.

Схема виконання шеститочкового пошуку така. Спочатку розглядаються шість блоків (рис. 2).

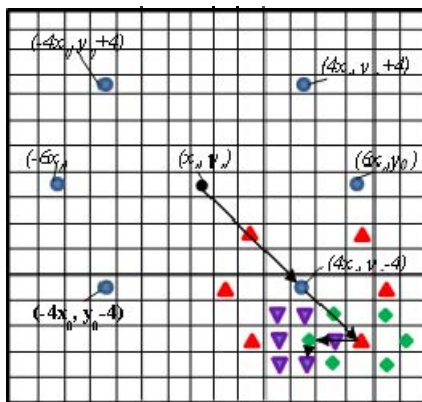


Рис. 2. Можливі шляхи збіжності шеститочкового алгоритму пошуку

Потім, якщо один із блоків є найкращим кандидатом серед інших, то центр пошуку зміщується туди, і відстань між точками скорочується

вдвічі. Такі дії повторюються доти доки відстань між блоками стає рівним одиниці

$$K_{j+1}(x_1; y_1) = K_j(x_0; y_0), \quad (1)$$

де K_{j+1} — інтерпольований кадр; K_j — поточний кадр; $(x_1; y_1)$ — координати центру інтерпольованого кадру; $(x_0; y_0)$ — координати центру поточного кадру.

Формула (1) являє собою рівність координат центру двох сусідніх кадрів.

Обрахування верхньої лівої точки:

$$K_{j+1}(-4x_1; (y_1 + 4)) = \frac{[K_j(x_0; y_0) + K_j(-4x_0; (y_0 + 4))]}{2}. \quad (2)$$

Обрахування верхньої правої точки:

$$K_{j+1}(4x_1; (y_1 + 4)) = \frac{[K_j(x_0; y_0) + K_j(4x_0; (y_0 + 4))]}{2}. \quad (3)$$

Обрахування лівої точки:

$$K_{j+1}(-6x_1; y_1) = \frac{[K_j(x_0; y_0) + K_j(-6x_0; y_0)]}{2}. \quad (4)$$

Обрахування правої точки:

$$K_{j+1}(6x_1; y_1) = \frac{[K_j(x_0; y_0) + K_j(6x_0; y_0)]}{2}. \quad (5)$$

Обрахування нижньої лівої точки:

$$K_{j+1}(-4x_1; (y_1 - 4)) = \frac{[K_j(x_0; y_0) + K_j(-4x_0; (y_0 - 4))]}{2}. \quad (6)$$

Обрахування нижньої правої точки:

$$K_{j+1}(4x_1; y_1 - 4) = \frac{[K_j(x_0; y_0) + K_j(4x_0; (y_0 - 4))]}{2}. \quad (7)$$

За формулами (1)–(7) розраховується наступні координати кожної із шести точок. Дані перерахунки повторюються доти, доки відстань між блоками стає рівним одиниці.

Висновки

1. Розглянуті методи компенсації руху у відеопотоці даних. З аналізу методів кодування відеопотоку даних виникає інтерес дослідження можливості подальшого збільшення коефіцієнта стиснення для методів довжин серій за рахунок додаткового використання методів компенсації руху. Як наслідок, пропонується вдосконалити метод зіставлення блоків компенсації руху шляхом спрощення використання шаблонів.

2. Проведено оцінку швидкості відеопотоку відеоінформації залежно від необхідної якості відеоданих, від просторового дозволу і частоти кадрів. При тенденції зростання обсягів відеоінформації і не забезпечення відповідними даними обсягами продуктивності технологій передачі та обробки відеоінформації в комплексах ВКЗ — необхідно вдосконалити методи кодування.

Перспективи подальших досліджень

Визначений напрям, спонукає на вдосконалення існуючих методів кодування динамічних об'єктів відеопотоку даних алгоритмами компенсації руху для покращення ефективності використання відеоконференцв'язку в системі управління.

ЛІТЕРАТУРА

1. **Олифер В. Г.** Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов / В. Г. Олифер, Н. А. Олифер. — СПб. : Питер, 2006. — 958 с.
2. **Гонсалес Р.** Цифровая обработка изображений / Р. Гонсалес, Р. Вудс. — М. : Техносфера, 2005. — 1072 с.
3. **Алімпієв А. М., Бараннік В. В., Белікова Т. В., Сідченко С. О.** Теоретичні основи створення технологій протидії прихованим інформаційним атакам в сучасній гібридній війні // Системи обробки інформації. — Харків : ХНУПС. — 2017. — № 4(150). — С. 113–121. (ukr)

Бараннік В. В., Бараннік Д. В., Сорокун А. Д., Дворський М. В. ВДОСКОНАЛЕННЯ МЕТОДІВ КОМПЕНСАЦІЇ РУХУ ДИНАМІЧНИХ ОБ'ЄКТІВ У ВІДЕОПОТОЦІ В СИСТЕМІ ВІДЕОКОНФЕРЕНЦВ'ЯЗКУ

У статті розглянуто питання, пов'язані з швидкістю відеопотоку відеоінформації залежно від необхідної якості відеоданих, від просторового дозволу і частоти кадрів. При тенденції зростання обсягів відеоінформації і не забезпечення відповідними даними обсягами продуктивності технологій передачі та обробки відеоінформації в комплексах ВКЗ — необхідно вдосконалити методи кодування. Для підвищення ефективності

4. **Yudin O., Frolov O., Ziubina R.** Quantitative quality indicators of the invariant spatial method of compressing video data // Problems of Infocommunications Science and Technology (PIC S&T), 2015 Second International Scientific-Practical Conference. — IEEE, 2015. — P. 227–229, doi: 10.1109/INFOCOMMST.2015.7357320. (eng)

5. **Miano J.** Compressed image file formats: JPEG, PNG, GIF, XBM / John Miano. — 1999. — 264 p.

6. **Yudin O., Boiko Y., Frolov O.** Organization of decision support systems for crisis management // Problems of Infocommunications Science and Technology (PIC S&T), 2015 Second International Scientific-Practical Conference. — IEEE, 2015. — P. 115–117, doi: 10.1109/INFOCOMMST.2015.7357287. (eng)

7. **Barannik V. V., Komolov D., Musienko A. P., Tarnopolov R. V.** Methodological basis for determining the energy significance of the structural unit of a video frame based on the estimation of low-frequency components of the matrices of the DCT blocks of the luminance component // Modern Problems of Radio Engineering, Telecommunications and Computer Science, Proceedings (TCSET), 2016 13th International Conference. — IEEE, 2016. — P. 739–741, doi: 10.1109/TCSET.2016.7452168. (eng)

8. **Barannik V. V., Ryabukha Yu. N., Podlesnyi S. A.** Structural slotting with uniform redistribution for enhancing trustworthiness of information streams // Telecommunications and Radio Engineering (English translation of Elektrosvyaz and Radiotekhnika), 2017. - №76. — P. 607–615, doi: 10.1615/TelecomRadEng.v76.i7.40. (eng)

9. **Barannik V., Ryabukha Yu., Barannik D., Podlesny S.** The Information Integrity Enhance in Telecommunication Systems with the Binomial Coding // Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), 2017 4th International Scientific-Practical Conference. — IEEE, 2017. — P. 547–550, doi: 10.1109/INFOCOMMST.2017.8246459. (eng)

10. **Barannik V., Podlesny S., Tarasenko D., Barannik D., Kulitsa O.** The video stream encoding method in infocommunication systems // on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), 2018 14th International Conference. — IEEE, 2018. — P. 538–541, doi: 10.1109/TCSET.2018.8336259. (eng)

управлінської та експлуатаційної діяльності пропонується вдосконалювати існуючі методи кодування динамічних об'єктів відеопотоку даних алгоритмами компенсації руху для відеоконференцзв'язку в системі управління.

Ключові слова: відеоконференцзв'язок, відеопотік, кодування, компенсація руху.

Barannik V. V., Barannik D.V., Sorokun A.D., Dvorsky M. V.
IMPROVEMENT OF METHODS OF COMPENSATING MOTION OF DYNAMIC OBJECTS IN A VIDEO STREAM IN A VIDEO CONFERENCING SYSTEM

The article deals with issues related to the speed of the video stream of video information, depending on the quality of video data required, from spatial resolution and frame rate. With the tendency of growth of volumes of video information and not providing the corresponding data volumes of the productivity of technologies of transmission and processing of video information in complexes videoconferencing - it is necessary to improve the coding methods. In order to increase the efficiency of management and operational activities, it is proposed to improve the existing methods of encoding a dynamic video stream object with algorithms for motion compensation for video conferencing in the control system.

Keywords: videoconferencing, video stream, coding, motion compensation.

Баранник В. В., Баранник Д. В., Сорокун А. Д., Дворский М. В.
СОВЕРШЕНСТВОВАНИЕ МЕТОДОВ КОМПЕНСАЦИИ ДВИЖЕНИЯ ДИНАМИЧЕСКИХ ОБЪЕКТОВ В ВИДЕОПОТОКЕ В СИСТЕМЕ ВИДЕОКОНФЕРЕНЦСВЯЗИ

В статье рассмотрены вопросы, связанные со скоростью видеопотока видеoinформации в зависимости от требуемого качества видеоданных, от пространственного разрешения и частоты кадров. При тенденции роста объемов видеoinформации и не обеспечении соответствующими данными объемами производительности технологий передачи и обработки видеoinформации в комплексах ВКЗ - необходимо совершенствовать методы кодирования. Для повышения эффективности управленческой и эксплуатационной деятельности предлагается совершенствовать существующие методы кодирования динамических объекте видеопотока данных алгоритмами компенсации движения для видеоконференцсвязи в системе управления.

Ключевые слова: видеоконференцсвязь, видеопоток, кодирования, компенсация движения

Стаття надійшла до редакції 07.09.2018 р.

Прийнято до друку 18.09.2018 р.

Рецензент – д-р техн. наук, проф. Мачалін І. О.

УДК 621.39

DOI: 10.18372/2310-5461.39.13084

В. В. Бараннік, д-р техн. наук, проф.
Харківський національний університет Повітряних Сил імені Івана Кожедуба
orcid.org/0000-0002-2848-4524
e-mail: vvbar.off@gmail.com

Д. С. Гаврилов, аспірант
Харківський національний університет радіоелектроніки
orcid.org/0000-0002-3344-7808
e-mail: havrylov_d@ukr.net

В. С. Фустій
Харківський національний університет Повітряних Сил імені Івана Кожедуба
orcid.org/0000-0003-4763-533X

В. В. Бараннік
Харківський національний університет радіоелектроніки
orcid.org/0000-0003-3516-5553
e-mail: valera462000@gmail.com

ТЕХНОЛОГІЯ БАГАТОРІВНЕВОЇ СЕЛЕКТИВНОЇ ОБРОБКИ АЕРОФОТОЗНІМКУ ДЛЯ ПЕРСПЕКТИВНИХ ЛІТАЛЬНИХ СЕНСОРНИХ МЕРЕЖ

Вступ

Значна популяризація безпілотних літальних апаратів (БПЛА) у комерційних та відомчих установах останніми роками призвела до значного поширення їх функціональних задач. Тенденція змін покладених на БПЛА задач вказує на неможливість одного літального апарату виконувати завдання в повному обсязі. Отже, пропонується використовувати сенсорні мережі в рамках концепції Інтернету Речей (англ. *Internet of Things*, IoT), а саме літаючу сенсорну мережу, яка побудована на новітніх технологіях бездротового зв'язку 3G, 4G й перспективної технології 5G. При цьому, літальна мережа з використанням БПЛА має бути побудована за принципом міжмашинної комутації (англ. *Machine to Machine*, M2M), що в свою чергу призведе до збільшення об'ємів даних, що передаються.

Аналіз останніх досліджень і публікацій

Існуючі методи обробки цифрових аерофото-знімків (JPEG, JPEG2000) показали, що найбільш

важливою є інформація про контури, границі об'єктів [3–4]. З метою забезпечення оперативності та конфіденційності переданих даних використовують селективні методи обробки зображень, які на сьогодні мають показники близькі до допустимих. Отже, можна зробити висновок, що подальший розвиток літальних сенсорних мереж призведе до неможливості виконувати наявними селективними методами покладені на них завдання.

Метою статті є розробка технології багаторівневої селективної обробки аерофото-знімків з урахуванням рівня насиченості важливою інформацією для літальних сенсорних мереж в умовах перспективного збільшення об'ємів даних, що передаються.

Виклад основного матеріалу

Дослідження сфер застосування БПЛА показало, що для відомчих структур основним завданням є моніторинг об'єктів критичної інфраструктури (рис. 1).



Рис. 1. Задачі аеромоніторингу

Під об'єктами критичної інфраструктури (ОКІ) розуміють підприємства та установи таких галузей — як енергетика, промисловість, транспорт, банки та фінанси, інформаційні технології та телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство, яке є стратегічно важливим для функціонування економіки, безпеки держави, суспільства та населення.

При цьому, добуті дані можуть містити конфіденційну інформацію, яка при потраплянні до несанкціонованого користувача призведе до представлених в таблиці негативних наслідків.

Виходячи з даних міркувань необхідним є застосування алгоритмів криптографічного захисту, що допоможе зберегти інформацію від зловмисників.

Можливі наслідки в результаті несанкціонованого доступу до інформації

Задачі аеромоніторингу	Час $T_{\text{акт}}$ актуальності інформації (активна фаза)	Відеоінформаційний ресурс містить відомості про	Володіння даними несанкціонованим користувачем призведе до
Пошук та порятунок в кризових обставинах	До 24 год	Місцезнаходження об'єкту інтересу	Заволодіння противником об'єкту інтересу
Контроль та ліквідація наслідків аварії на АЕС	До 24 год	Масштаб трагедії	Соціальні хвилювання (паніка, бастування тощо)
Стихійні лиха	До 24 год		
Моніторинг об'єктів під час соціальних конфліктів	До 24 год	Місцезнаходження та дії сторін конфлікту	Збільшення інтенсивності соціального конфлікту
Оцінка стану власних сил системи безпеки	До 24 год	Місцезнаходження, склад, озброєння, слабкі та сильні місця власних сил (військ)	Фізичне знищення об'єктів критичної інфраструктури
Контроль завантаженості автомагістралі	До 12 год	Рівень завантаженості автомагістралі	Розуміння маршруту руху перших осіб держави чи організації з подальшим їх фізичним знищенням

Варто відмітити, що ОКІ, як правило, займають значну територію. Тож, для постійного контролю в перспективі планується використовувати літальну сенсорну мережу (рис. 2). Нова стратегія використання БПЛА в «командній» роботі створює апаратно-програмну задачу підтримувати не лише багатоканальний зв'язок, а й підтримувати режим ретрансляції сигналу. Отже, БПЛА планується використовувати як комутатори (ретранслятори), що значно підвищить робочий радіус використання БПЛА. Наприклад, як видно з рис. 2, потужності передатчика БПЛА Л1 не вистачає для передачі даних на пункт дистанційного управління (ПДУ), але за допомогою

БПЛА Л4, в якості ретранслятора, БПЛА Л1 має змогу передати добути інформацію на ПДУ. Важливо відмітити, що при даній системі приймання-передавання даних зберігається можливість управління будь-яким БПЛА оператором з ПДУ. Слід відзначити, що використання БПЛА в якості ретранслятора (комутатора) значно підвищить об'єм даних (X), що передаються, особливо на кінцевих вузлах перед приймальною антеною ПДУ (рис. 3).

Тож, актуальною науково-прикладною задачею є відшукування технологій зменшення об'ємів даних, що передаються, з збереженням необхідного рівня захисту інформації.

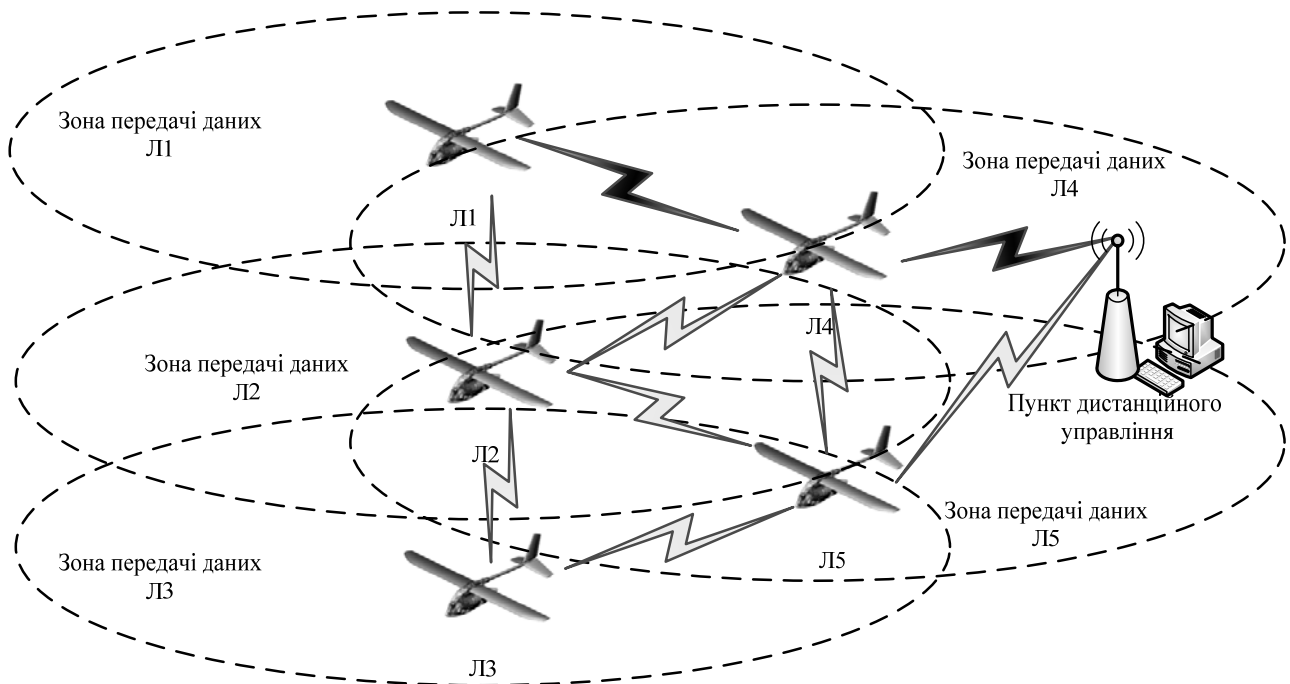


Рис. 2. Схема літальної сенсорної мережі

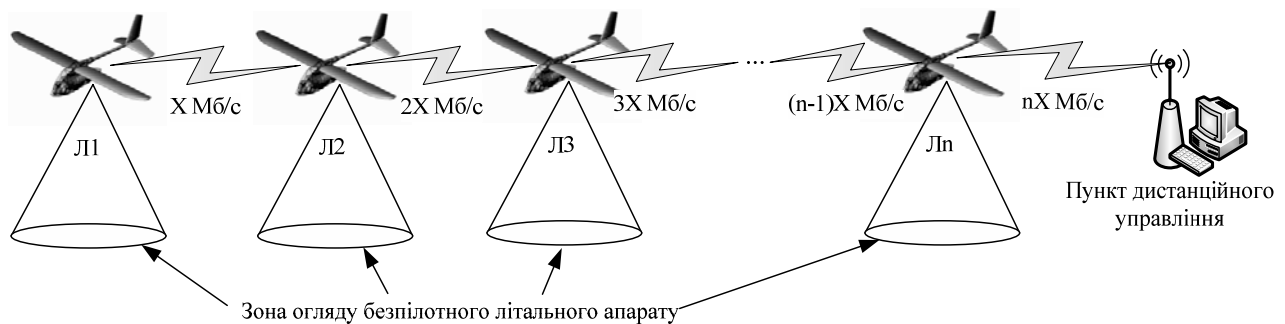


Рис. 3. Схема збільшення об'єму даних, що передаються в літальній сенсорній системі

Дослідження показали, що навіть використання технології 4G не дозволить повною мірою задовольнити потребу в оперативній доставці даних при передачі через останній мобільний вузол інформації з 4-х БПЛА. Тож, для підвищення оперативності передачі даних пропонується використовувати багаторівневий селективний метод обробки даних [5].

Більш детально представлений на рис. 4, де $A_y(v, u)$, $A_{cr}(v, u)$ та $A_{cb}(v, u)$ — складові з яскравості, червона та синя хроматична складова відповідно; $A_y(v, u)^+$ та $A_y(v, u)^-$ — складові з яскравості, які мітять та не містять ключову інформацію відповідно; $D(v, u)$ — трансформанта після дискретного косинусного перетворення

(dct); $HF(D, v, u)$ та $LF(D, v, u)$ — високочастотні та низькочастотні компоненти трансформанти відповідно; $S(v, u)$ — лінеаризована трансформанта; $E_{(v,u)}^\psi$ — закодоване зображення ψ -м методом; E_{jreg}^{cgrp} — зображення, оброблене селективним методом на основі JPEG-платформи.

Для підтвердження ефективності розробленого багаторівневого селективного методу обробки аерофотознімків проводиться дослідження у порівнянні з відомими селективними методами за критерієм оперативності для слабонасиченого (рис. 5), середньонасиченого (рис. 6) та сильнонасиченого (рис. 7) кадру.

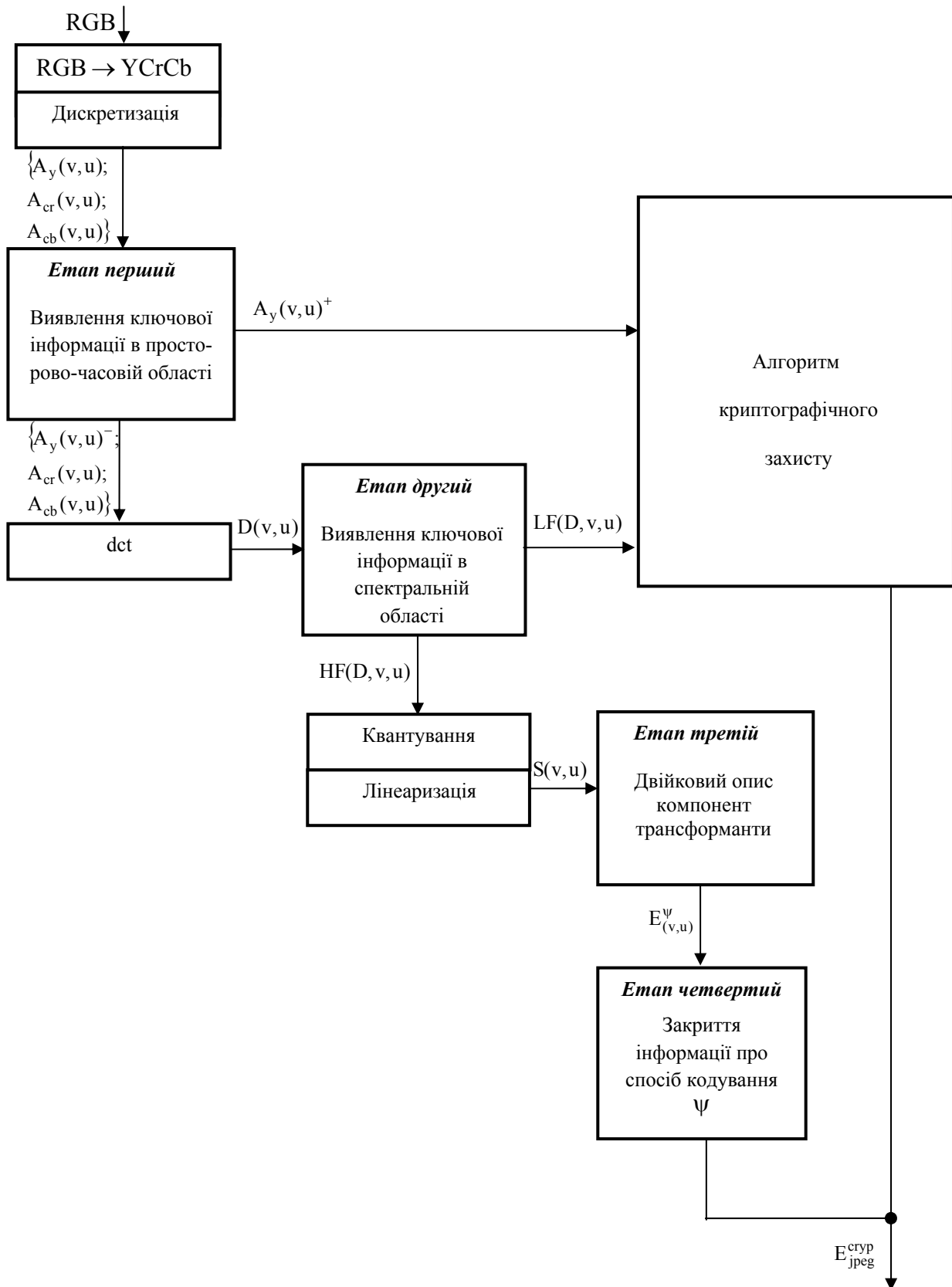


Рис. 4. Блок-схема багаторівневої селективної обробки на основі JPEG-платформи

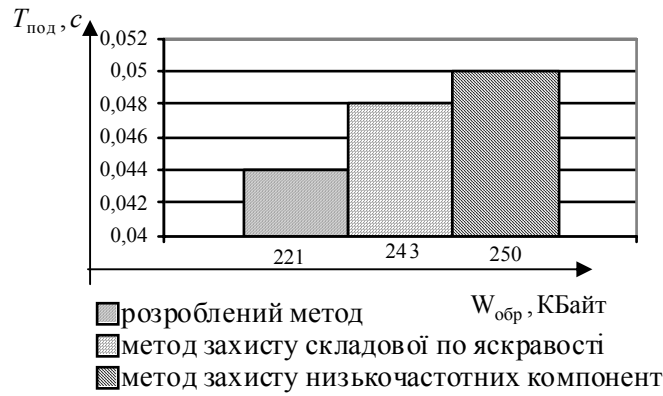


Рис. 5. Діаграма дослідження методів селективної обробки даних за критерієм оперативності доведення даних для слабонасиченого кадру



Рис. 6. Діаграма дослідження методів селективної обробки даних за критерієм оперативності доведення даних для середньонасиченого кадру



Рис. 7. Діаграма дослідження методів селективної обробки даних за критерієм оперативності доведення даних для сильнонасиченого кадру

Під оперативністю розуміється властивість інформації певного об'єму ($W_{обр}$) проходити процес обробки та передачі за час $T_{под}$, менший ніж час який вимагається системою. У досліді використовувався канал з пропускнуою спроможністю комплексу супутникового зв'язку єдиної відомчої телекомунікаційної мережі $\alpha = 5$ Мбіт/с.

Проведене дослідження вказало, що для слабонасиченого та середньонасиченого кадру спо-

стерігається підвищення оперативності доведення даних на 820 та 109 % відповідно по відношенню до ближнього конкуренту. У разі обробки сильнонасиченого кадру спостерігається незначне покращення оперативності передачі даних.

Висновки

Розглянуто перспективну стратегію використання безпілотних літальних апаратів, яка полягає у застосуванні технології літальних сенсорних мереж з підтримкою технології 3G, 4G та

перспективної технології 5G, що значно підвищить об'єм даних, що передаються по каналах зв'язку з пропускною спроможністю комплексу супутникового зв'язку єдиної відомчої телекомунікаційної мережі $\alpha = 5$ Мбіт/с.

Наукова новизна

Для забезпечення оперативності та конфіденційності даних, що передаються, пропонується використовувати багаторівневий селективний метод обробки даних, який полягає у виявленні та захисті ключових компонентів на декількох етапах обробки даних.

Проведено дослідження ефективності використання розробленого методу у порівнянні з існуючими методами, яке вказало, що для слабонасиченого та середньо-насиченого кадру спостерігається підвищення оперативності доведення даних на 820 та 109 % відповідно, по відношенню до ближнього конкуренту.

Подальший напрямок роботи полягає у відшуванні шляхів підвищення оперативності передачі даних сильно насичених кадрів.

ЛІТЕРАТУРА

1. Мельник А. С. Інформаційні системи та мережі. Вісник / М. М. Голобородько НУ «Львівська політехніка». — № 673. — Львів, 2010. — С. 365-374.
2. Гонсалес Р. С., Вудс Р. Э. Цифровая обработка изображений / Р. С. Гонсалес, Р. Э. Вудс. — М.: Техносфера, 2006. — 1072 с.
3. Гаврилов Д. С. Метод забезпечення безпеки відеоінформаційного ресурсу на основі багаторівневої селективної обробки в телекомунікаційних / Д. С. Гаврилов, О. Г. Оксіюк, П. М. Гуржій, Б. О. Демідов // Наука і техніка. — № 26, 2017. — С. 46-48.

4. Баранник В. В. Основы теории структурно-комбинаторного стеганографического кодирования: монография / В. В. Баранник, Д. В. Баранник, А. Э. Бекиров. — Х.: Издательство «Лидер», 2017. — 256 с.

5. Yudin O., Frolov O., Ziubina R. Quantitative quality indicators of the invariant spatial method of compressing video data // Problems of Infocommunications Science and Technology (PIC S&T), 2015 Second International Scientific-Practical Conference. — IEEE, 2015. — P. 227-229, doi: 10.1109/INFOCOMMST.2015.7357320 (eng).

6. Miano J. Compressed image file formats: JPEG, PNG, GIF, XBM / John Miano, 1999. — 264 p.

7. Barannik V., Ryabukha Yu., Barannik D., Podlesny S. The Information Integrity Enhance in Telecommunication Systems with the Binomial Coding // Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), 2017 4th International Scientific-Practical Conference. — IEEE, 2017. — P. 547-550, doi: 10.1109/INFOCOMMST.2017.8246459 (eng).

8. Barannik V., Podlesny S., Tarasenko D., Barannik D., Kulitsa O. The video stream encoding method in infocommunication systems // on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), 2018 14th International Conference. — IEEE, 2018. — P. 538-541, doi: 10.1109/TCSET.2018.8336259 (eng).

9. Barannik V., Ryabukha Yu., Tverdokhlib V., Dodukh A., Suprun O., Tarasenko D. Integration the non-equilibrium position encoding into the compression technology of the transformed images // East-West Design & Test Symposium (EWDTS). — IEEE, 2017. — P. 1-4. DOI: 10.1109/EWDTS.2017.8110030.

10. Barannik V., Alimpiev A., Bekirov A., Barannik D., Barannik N. Detections of sustainable areas for steganographic embedding // East-West Design & Test Symposium (EWDTS). — IEEE, 2017. — P. 555-558. DOI: 10.1109/EWDTS.2017.8110028.

Бараннік В. В., Гаврилов Д. С., Фустій В. С., Бараннік В. В. ТЕХНОЛОГІЯ БАГАТОРІВНЕВОЇ СЕЛЕКТИВНОЇ ОБРОБКИ АЕРОФОТОЗНІМКУ ДЛЯ ПЕРСПЕКТИВНИХ ЛІТАЛЬНИХ СЕНСОРНИХ МЕРЕЖ

У статті розглянуто питання, пов'язані зі збільшення об'ємів даних, що передаються за рахунок розвитку технологій безпілотних літальних апаратів та збільшення обсягів використання їх у комерційній та відомчій сфері. Пропонується метод багаторівневої селективної обробки даних, який дозволить зберігати оперативність доведення даних в умовах підвищення інтенсивності потоку даних з заданим рівнем конфіденційності. Проводиться дослідження ефективності використання розробленого багаторівневого селективного методу обробки даних у порівнянні з відомими селективними методами за критерієм оперативності для кадрів різної насиченості.

Ключові слова: літальна сенсорна мережа, об'єкти критичної інфраструктури, селективна обробка, оперативність, конфіденційність, значущі компоненти.

Barannik V. V., Havrylov D. S., Fustii V. S., Barannik V. V.

TECHNOLOGIES OF MULTILEVEL SELECTIVE PROCESSING OF AERIAL PHOTOGRAPHS FOR PERSPECTIVE FLYING SENSOR NETWORKS

The article deals with issues related to the increase in the volume of transmitted data, as a result of the development unmanned aerial vehicle technologies, and increasing their use in commercial and departmental areas. A method of multilevel selective data processing is proposed that will allow to maintain the efficiency transmission data in conditions of increasing the intensity of the data flow with a given confidentiality level. The research of the effectiveness used the developed multilevel selective data processing method in comparison with the known selective methods for the efficiency criterion for frames of different saturation is carried out.

Keywords: fly sensor network, critical infrastructure objects, selective processing, efficiency, confidentiality, meaningful components.

Баранник В. В., Гаврилов Д. С., Фустий В. С., Баранник В. В.

ТЕХНОЛОГИЯ МНОГОУРОВНЕВОЙ СЕЛЕКТИВНОЙ ОБРАБОТКИ АЭРОФОТОСНИМКЕ ДЛЯ ПЕРСПЕКТИВНЫХ ЛЕТАТЕЛЬНЫХ СЕНСОРНЫХ СЕТЕЙ

В статье рассматриваются вопросы, связанные с увеличением объемов передаваемых данных за счет развития технологий беспилотных летательных аппаратов и увеличения объемов использования в коммерческой и ведомственной сфере. Предлагается метод многоуровневой селективной обработки данных, который позволит сохранять оперативность доведения данных в условиях повышения интенсивности потока данных с заданным уровнем конфиденциальности. Проводится исследование эффективности использования разработанного многоуровневого селективного метода обработки данных по сравнению с известными селективными методами по критерию оперативности для кадров различной насыщенности.

Ключевые слова: летательная сенсорная сеть, объекты критической инфраструктуры, селективная обработка, оперативность, конфиденциальность, значимые компоненты.

Стаття надійшла до редакції 06.09.2018 р.

Прийнято до друку 26.09.2018 р.

Рецензент – д-р техн. наук, проф. Конахович Г. Ф.

УДК 004.822 (045)

DOI: 10.18372/2310-5461.39.13085

І. А. Жуков, д-р. техн. наук, проф.
Національний авіаційний університет
orcid.org/0000-0002-9785-0233
e-mail: zhuia@ukr.net

М. К. Печурін, д-р. техн. наук, проф.
Національний авіаційний університет
orcid.org/0000-0001-1727-7455
e-mail: nkpech@i.ua

Л. П. Кондратова, канд. техн. наук
НТУУ «КПІ імені Ігоря Сікорського»
orcid.org/0000-0002-9170-4198
e-mail: ljupav@ukr.net

О. О. Печуріна
Національний авіаційний університет
orcid.org/0000-0003-2563-5869
e-mail: nkpech@i.ua

СПОСІБ ОЦІНЮВАННЯ ІНТЕНСИВНОСТЕЙ ПЕРВИННИХ ІНФОРМАЦІЙНИХ ПОТОКІВ, ГЕНЕРОВАНИХ АБОНЕНТАМИ КОМП'ЮТЕРНОЇ МЕРЕЖІ РЕЧЕЙ

Вступ

В умовах глобалізації (інтеграції) комп'ютерних мереж різного рівня, слід звернути увагу хоча б на ідею створення телекомунікаційної інфраструктури на основі низькоорбітальних супутників [1], оцінку динаміки їх розвитку, що набуває все більшого значення через величезні витрати (нарешті — за рахунок населення) обмежених ресурсів на створення і експлуатацію такого роду комп'ютерної інфраструктури. При цьому основним параметром, що визначає динаміку розвитку комп'ютерних мереж і дозволяє оцінити витрати ресурсів на її створення, є інформаційне навантаження, що виникає від кінцевих (термінальних) пристроїв.

Оцінювання сукупної інформаційної потужності (продуктивності) програмно-апаратних засобів — джерел первинної, для мережі, інформації, є досить складним завданням: авторам це нагадало труднощі початку 70-х ХХ ст. оцінювання аналогічного показника силами ВНДІ проблем організації та управління для (комп'ютерної) мережі обчислювальних центрів колективного користування, яку створювали для загальнодержавної автоматизованої системи під науковим керівництвом академіка В. М. Глушкова [2].

Оцінка (для цілей прогнозування) первинного, від існуючих або потенціальних абонентів, інформаційного навантаження на комп'ютерні ме-

режі речей, або на їх інтеграцію Інтернет-речей [3], є необхідною умовою успішного розвитку цього відносно нового об'єкта інформаційних технологій, зокрема, для ефективного розподілу зусиль на створення інформаційно-телекомунікаційної інфраструктури.

Аналіз досліджень та підходи до розв'язання проблеми

Оцінку (для цілей прогнозування) інтенсивностей інформаційних потоків (первинного інформаційного навантаження на створювану комп'ютерну мережу) що вони генеруються абонентами (термінальними програмно-апаратними пристроями), можна проводити декількома способами.

Першим, найбільш «перевіраним» способом, є оцінювання інтенсивностей первинних потоків з використання класичних (AR, MA, ARMA) алгоритмів прогнозування на базі апріорі сформованого часового ряду.

Поряд з відомими «невиліковними» вадами алгоритмів прогнозування на основі часових рядів, маємо дуже коротку вибірку з причини новизни такого об'єкту, як киберфізичні мережі.

Носіями інформації, що надходять в мережу речей від термінальних пристроїв кінцевих користувачів в одиницю часу, є самі «речі», тобто матеріальні об'єкти, що забезпечуються пристроями введення-виведення, роль яких можуть грати різні програмно-апаратні засоби, зокрема,

виконавчі пристрої і (інтелектуальні) сенсори [4]. Тому наступним, для оцінки первинного інформаційного навантаження підходом є оцінювання інтенсивностей потоків саме «речей», на основі чого отримуються дані про інтенсивності інформаційних потоків, що витікають від кожного з n джерел (абонентів мережі). Для цього також треба встановити (функціональну) залежність між інтенсивностями потоків кожного типу речей і відповідними інформаційними потоками.

Такий спосіб важко застосувати безпосередньо через складність відповідної багатопродуктової моделі та відсутність системи моніторингу.

Інші підходи до оцінки інтенсивностей інформаційних потоків засновані на використанні оцінок інтенсивностей потоків речей; при цьому найбільш вживаним (опосередкованим) показником є економетричний показник — ВВП [5].

Постановка завдання оцінювання інтенсивностей первинних інформаційних потоків

Маємо n абонентів-учасників створення кіберфізичної мережі, кожен з яких генерує інформаційний потік, значення інтенсивності якого позначимо через p_i . Інтенсивність загального первинного інформаційного потоку, що надходить в мережу, позначимо через s .

Необхідно оцінити значення s , а також інтенсивності p_i інформаційних потоків, що вони генеруються кожним з n абонентів.

Розв'язання завдання

Як висхідний показник для оцінювання s обираємо такий з доступних, який найбільшою мірою характеризує інтенсивність потоку речей — генераторів інформації, що вона надходить в мережу речей (звісно, через термінальні пристрої). Цим показником обрано ВВП, який опосередковано являє собою обсяг речей (читай — інтелектуальних сенсорів і виконавчих пристроїв), які можуть (потенційно) і породити інформаційне навантаження на кіберфізичну мережу (Інтернет-речей). Цей показник (ВВП ППС, ВВП та ін.) розраховується щорічно (тобто одиницею часу в нашій задачі вибираємо рік) для всіх країн, абоненти яких можуть скласти саму комп'ютерну мережу речей; у межах країни ці розрахунки виконує Держкомстат [5].

Уведемо припущення про пряму лінійну залежність кількості інформації, що генерується термінальними пристроями та надходить в мережу за одиницю часу, від кількості речей-терміналів: чим більше речей продукується за одиницю часу, тим більше інформаційне навантаження на мережу.

Головна похибка, що виникає при розв'язанні нашої проблеми оцінювання s за значенням ВВП,

виникає через (адитивну) згортку, в класичному макроекономічному ВВП, двох складових: річного обсягу вироблених товарів (тобто речей, які визначають s , на продаж) і послуг (шум в контексті нашої статті і в ньому — ideas з [6]).

Аддитивний характер згортки дозволяє виокремити складову ВВП, пов'язану з продукуванням речей, але напівволютаристське визначення ціни речі для замірювання обсягу вироблених товарів у ВВП знижує точність оцінювання s [7; 8]. Такі самі міркування стосуються проблем оцінювання p_i на основі ВВП.

Прийнявши вищезгадане припущення і маючи статистичні дані про загальний ВВП, оцінюємо s з точністю до цін речей як товарів.

Така сама процедура може бути застосована для (автономного) оцінювання p_i на основі ВВП, але з метою отримання більш точної оцінки p_i за рахунок побудови моделі з більшою ступінню адекватності, будемо враховувати зв'язки, що існують між абонентами комп'ютерної мережі речей в процесі продукування ВВП. Як абоненти для регіональних мереж можуть виступати галузі народного господарства, як інтегровані сукупності підприємств — генераторів речей.

Припустивши збалансованість (врівноважене зростання) виробничо-економічного процесу, обираємо модель міжгалузевого балансу В. В. Леонтєва [9], як найпростішої математичної конструкції, яка враховує згадані зв'язки:

$$(E - A(t)) \cdot X(t) - R(t) = 0,$$

де $A = A_{nn}$ — технологічна матриця; X — загальний обсяг вироблених товарів і послуг; R — ВВП; складові A , X , R суть функції часу.

Матриця $A(t)$ враховує «приховану» частину потоків речей, які утворюються у власне процесі виробництва і «споживаються всередині» потенційного абонента створення комп'ютерної мережі речей [9].

Дескриптивна модель для оцінювання інтенсивностей первинних інформаційних потоків

Позначення:

1) $X_E = [x^i]_{1 \times n}$ матриця, елементи якої пропорційні інтенсивностям потоків речей, спродукованих абонентом PP_i $| i = \overline{1, n}$.

2) $X_{tel} = [x^{ij}]_{n \times n}$ — матриця, елементи якої пропорційні інтенсивностям потоків речей (вихідному інформаційному навантаженню), вироблених абонентом PP_i для абонента PP_j (x^{ij} — значення, пропорційне інтенсивності потоку речей, що їх вироблено абонентом PP_i і які транспортуються абоненту PP_j).

3) $C_{\text{cost}} = [c^i]_{1 \times n}$ матриця, елементи якої являють собою «інформаційну цінність» одиниці x^i .

4) $A_{n \times n} = [a_{ij}]$ — матриця (технологічних) коефіцієнтів, де a_{ij} — коефіцієнт, що являють собою витрати продукту (речей), вироблених абонентом $PP_i | i = \overline{1, n}$ при продукуванні одиниці потоку речей в PP_j .

Обмеження:

1) Кожний $PP_i | i = \overline{1, n}$ продукує тільки один, властивий цьому абоненту, продукт (тип речей).

2) Кожний тип речей продукується тільки одним $PP_i | i = \overline{1, n}$.

3) Кожний $PP_i | i = \overline{1, n}$ має свою технологію перетворення речей, що надходять у вигляді ресурсу.

4) Існує матриця $X_{\text{cost}} = [c^i \cdot x^{ij}]_{n \times n}$, елемент якої суть інтенсивність потоку речей, в інформаційному вимірі, від $PP_i | i = \overline{1, n}$ до PP_j , тобто маємо лінійну за x^{ij} функцію $f^{ij}(x^{ij}, c^i) = c^i \cdot x^{ij}$.

5) Для всіх i виконуються умови $\sum_j x^{ij} \cdot c^i = \sum_j x^{ji} \cdot c^j$; $X \geq 0$.

6) Виконуються співвідношення балансу: $E \cdot X_E^T - A \cdot X_E^T - R^T = 0$.

Заміною змінних запропонована модель зв'язана до потокової (див. рисунок), що дало змогу дослідити її з використанням алгоритму типу алгоритму Форда–Фалкерсона.

Приклад розв'язання задачі оцінювання інтенсивностей первинних інформаційних потоків комп'ютерної мережі регіонального рівня.

Запропоновану модель застосовано для розв'язання задачі оцінювання інтенсивностей первинних інформаційних потоків комп'ютерної мережі речей регіонального (державного) рівня (абонент — галузь народного господарства).

В таблиці наведено деякі результати [8].

З таблиці видно, що доля первинного інформаційного навантаження на створювану (державну) комп'ютерну мережу речей, що воно пов'язане з джерелами — галузями промисловості, і оцінена безпосередньо за показником ВВП, суттєво відрізняється від оцінки, отриманої за запропонованою моделлю.

Висновки

1. Урахування, в рекомендованій до використання моделі, зв'язків між потенційними абонентами мережі речей в процесі їх (речей) виробництва дозволяє отримати адекватну картину

розподілу інтенсивностей первинної інформації, що виходить від кінцевих пристроїв і навантажує мережу речей.

2. Алгоритми для дослідження запропонованої статичної моделі мають відносно невелику трудомісткість, — орієнтовно $O(n^3)$, як і трудомісткість алгоритмів розв'язання задач класу задач лінійного програмування або застосованої модифікації потокового алгоритму.

3. Розбіжність розподілів інформаційного навантаження від галузей народного господарства на створювану (державну) комп'ютерну мережу речей, які отримано різними способами, виникає з того, що існуюча офіційна статистична звітність спотворює фактичну інтенсивність потоків вироблених речей — генераторів інформаційного трафіку для мережі.

ЛІТЕРАТУРА

1. Вэнс Э., Маск И. Tesla, SpaceX и дорога в будущее = Musk E.: Tesla, SpaceX, and the Quest for a Fantastic Future. — М.: Олимп-Бизнес, 2016. — 416 с. — ISBN 978-59693-0330-0.

2. Зайченко Ю. П., Печурин М. К. Алгоритм математичного програмування для визначення раціональної структури мережі ОЦ // Автоматизовані системи управління і обробки даних. — К.: ІК АН УРСР, 1975. — 4 с.

3. Kevin Ashton. That 'Internet of Things' Thing. In the real world, things matter more than ideas. — RFID Journal (June, 22, 2009).

4. Войтович І. Д. Інтелектуальні сенсори // Україна. Наука і культура. — 2009. — Вип. 35. — С. 106–111.

5. Державна служба статистики України. — www.ukrstat.gov.ua.

6. Моисеев. Н. Н. Математические задачи системного анализа. — М.: Главная редакция физико-математической литературы. — 1981. — 488 с.

7. Zhukov I. A. Implementation of integral telecommunication environment for harmonized air traffic control with scalable flight display systems // Aviation. — 2010, №14(4). — P. 117–122.

8. Печуріна О. О. Балансування мережевого трафіку на основі моделі Леонтьєва // XIV Міжнародна науково-практична конференція молодих учених і студентів «Політ. Сучасні проблеми науки» (8-9 квітня 2015 р.). — Київ, 2015.

9. Жуков І. А., Печурин Н. К., Кондратова Л. П., Печурин С. Н. Распределение ресурсов в вычислительном кластере для БПЛА // Проблемы информатизації та управління: зб. наук. праць. — 2016. — Вип. 3 (55). — С. 1–5.

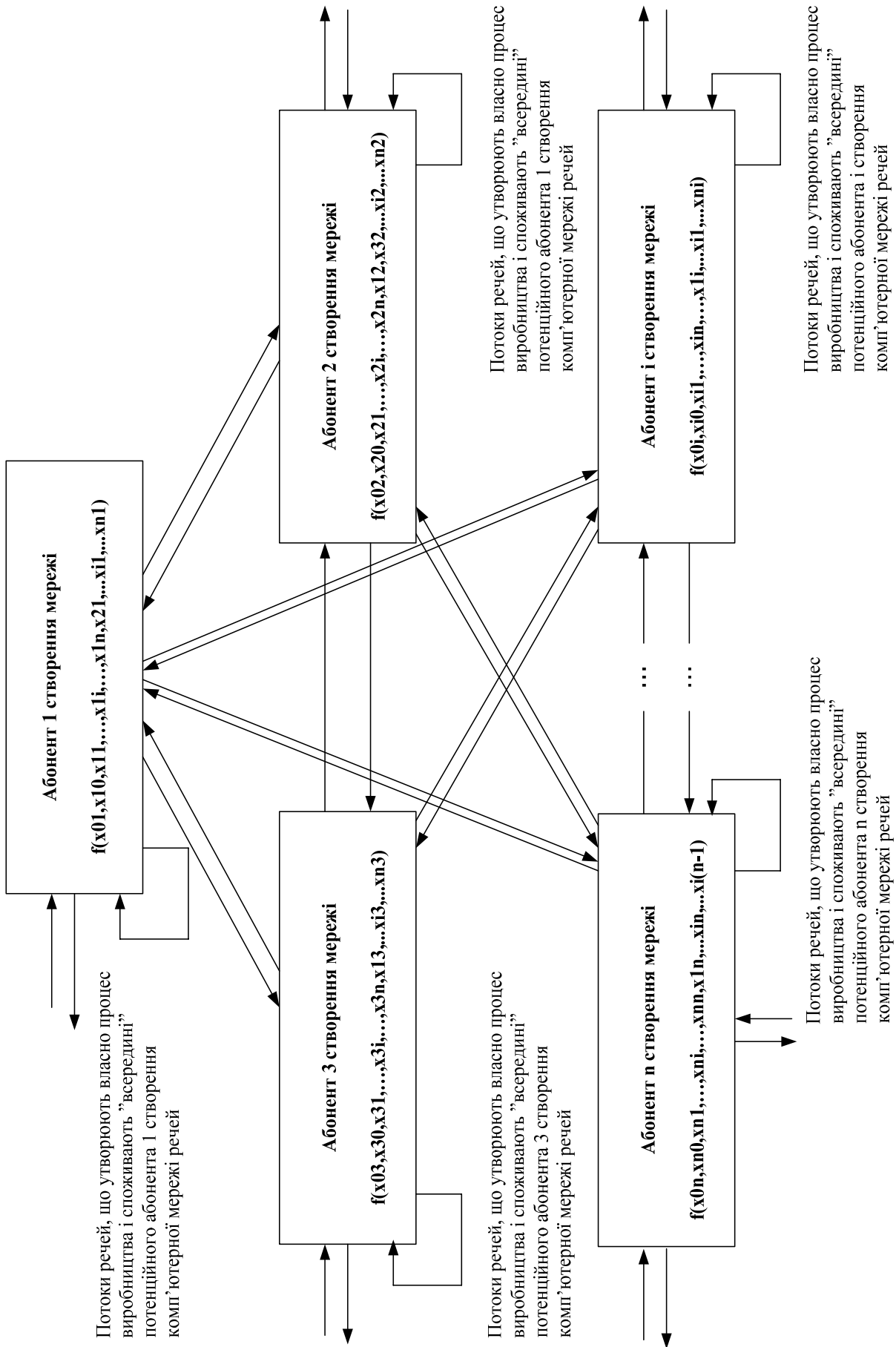


Рисунок – Потокове представлення дескриптивної моделі

Таблиця

**Оцінки інтенсивностей первинних інформаційних потоків
від галузей народного господарства на створювану (державну) комп'ютерну мережу речей**

Галузі народного господарства — учасники створення мережі речей [5] (генератори первинних інформаційних потоків)	Оцінка інформаційного навантаження від галузей народного господарства на створювану (державну) комп'ютерну мережу речей, що отримана безпосередньо (автономно) за даними про галузеві обсяги виробництва товарів і послуг від [9], доля від s	Оцінка інформаційного навантаження від галузей народного господарства на створювану (державну) комп'ютерну мережу речей, що отримана за даними про галузеві обсяги виробництва товарів і послуг з використанням моделі В. В. Леонтьєва, доля від s
Сільське господарство, лісове та рибне господарство	0,09	0,1
Добувна промисловість і розробка кар'єрів	0,06	0,05
Переробна промисловість	0,19	0,37
Постачання електроенергії, газу, пари та кондиціонованого повітря	0,03	0,04
Водопостачання, каналізація, поводження з відходами	0,01	0,01
Будівництво	0,03	0,05
Оптова та роздрібна торгівля; ремонт автотранспортних засобів	0,15	0,11
Транспорт, складське господарство, поштова та кур'єрська діяльність	0,08	0,06
Тимчасове розміщення та організація харчування	0,01	0,01
Інформація та телекомунікації	0,04	0,03
Фінансова та страхова діяльність	0,05	0,03
Операції з нерухомим майном	0,07	0,04
Професійна, наукова та технічна діяльність	0,03	0,03
Діяльність у сфері адміністративного та допоміжного обслуговування	0,01	0,01
Державне управління та оборона; обов'язкове соціальне страхування	0,05	0,03
Освіта	0,05	0,03
Охорона здоров'я та надання соціальної допомоги	0,03	0,02
Мистецтво, спорт, розваги та відпочинок	0,01	0,01
Надання інших видів послуг	0,01	0,01

Жуков І. А., Печурін М. К., Кондратова Л. П., Печуріна О. О.
**СПОСІБ ОЦІНЮВАННЯ ІНТЕНСИВНОСТЕЙ ПЕРВИННИХ ІНФОРМАЦІЙНИХ ПОТОКІВ,
ЗГЕНЕРОВАНИХ АБОНЕНТАМИ КОМП'ЮТЕРНОЇ МЕРЕЖІ РЕЧЕЙ**

Статтю присвячено проблемі оцінювання інтенсивностей первинних інформаційних потоків, що вони генеруються абонентами відносно нового об'єкту інформаційних технологій, — комп'ютерних мереж речей, для прогнозування їх розвитку. З цією метою пропонується модель, побудована на основі моделі міжгалузевого балансу В. В. Леонтьєва. Оцінюються пропорції у розподілі інтенсивностей первинних інформаційних потоків, що вони генеруються абонентами (термінальними програмно-апаратними пристроями) створеної кіберфізичної системи. Для формування параметрів моделі використано ВВП — загальнодоступний макроекономічний показник, який опосередковано представляє інтенсивність інформаційних потоків, що вони генеруються потенціальними абонентами створеної комп'ютерної мережі речей.

Ключові слова: оцінка стану, розвиток Інтернету, Інтернет-речей, інформаційне навантаження.

Zhukov I. A., Pechurin N. K., Kondratova L.P., Pechurina O.O.
**METHOD OF EVALUATION OF INTENSITY OF THE PRIMARY INFORMATION FLOWS,
GENERATED BY COMPUTER NETWORK NETWORK COMPONENTS**

The article is devoted to the problem of estimate the value of the primary information flows generated by abonents of the relatively new object of information technology, the so-called computer network of things to predict its development. To this end, a model is proposed on based of V.V. Leontiev model of inter-industry balance. There are estimated the proportions in the distribution of primary information flows, which are generated by the software-hardware (terminal) devices created cyber-physics system. In order to formulate the model parameters, a public macroeconomic indicator is used, only indirectly represented the intensity of information flows that they derive from potential abonents of created computer network of things.

Keywords: Evaluation of the state, development of the internet, internet of things, information load.

Жуков И. А., Печурин Н. К., Кондратова Л. П., Печурина О. О.
**СПОСОБ ОЦЕНКИ ИНТЕНСИВНОСТИ ПЕРВИЧНЫХ ИНФОРМАЦИОННЫХ ПОТОКОВ,
СГЕНЕРИРОВАННЫХ АБОНЕНТАМИ КОМПЬЮТЕРНОЙ СЕТИ ВЕЩЕЙ**

Статья посвящена проблеме оценки интенсивностей первичных информационных потоков, генерируемых абонентами относительно нового объекта информационных технологий, компьютерных сетей вещей, для прогнозирования их развития. С этой целью предлагается модель, построенная на основе модели межотраслевого баланса В. В. Леонтьева. Оцениваются пропорции в распределении интенсивностей первичных информационных потоков, генерируемых абонентами (терминальными программно-аппаратными устройствами) создаваемой киберфизической системы. Для формирования параметров модели использовано ВВП — общедоступный макроэкономический показатель, который косвенно представляет интенсивность информационных потоков, генерируемых потенциальными абонентами создаваемой компьютерной сети вещей.

Ключевые слова: Оценка состояния, развитие Интернета, Интернет вещей, информационная нагрузка.

Стаття надійшла до редакції 09.09.2018 р.

Прийнято до друку 20.09.2018 р.

Рецензент – чл.-кор. НАН України, д-р техн. наук, проф. Мохор В. В.

В. В. Козловський, д-р. техн. наук, проф.
Національний авіаційний університет
orcid.org/0000-0002-8301-5501
e-mail: vvkzeos@gmail.com

В. А. Глива, д-р. техн. наук, проф.
НТУУ «КПІ імені Ігоря Сікорського»
orcid.org/0000-0003-1257-3351
e-mail: glyva.valentin@gmail.com

О. В. Ходаковський, канд. техн. наук, доц.
НТУУ «КПІ імені Ігоря Сікорського»
orcid.org/0000-0002-3930-0030
e-mail: dzgeron@gmail.com

ЗАХИСНІ ВЛАСТИВОСТІ ЕЛЕКТРОМАГНІТНИХ ЕКРАНІВ НА ОСНОВІ ЗАЛІЗОРУДНОГО ПИЛУ ТА ЇХ ЗАСТОСУВАННЯ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ ТА ЛЮДЕЙ

Вступ

Розвиток технологій розроблення, виробництва та експлуатації електричного та електронного обладнання дозволяє підвищити його продуктивність, знизити енергоспоживання тощо. Поряд з цим, використання сучасного обладнання має наслідком зміни електромагнітної обстановки у виробничому середовищі та довкіллі. Це обумовлене розширенням частотного спектра електромагнітних полів комплексу технічних засобів, зростанням амплітуд електричних та магнітних складових гармонік електромагнітного поля промислової частоти. Наведене потребує розроблення та впровадження сучасних заходів і засобів захисту людей у виробничих та побутових умовах від впливу електромагнітних полів. Це відповідає Стратегії сталого розвитку «Україна 2020» і є однією з цілей реалізації Стратегії.

Екранування електромагнітних полів є актуальною проблемою захисту здоров'я, інформаційної безпеки, електромагнітної сумісності та електромагнітної екології житлових приміщень, захисту приміщень для серверів та іншого електронного обладнання.

Швидкий розвиток мобільного зв'язку, Інтернету, збільшення кількості електричних мереж значно збільшує забруднення навколишнього середовища. Електротранспорт, побутові електроприлади, комп'ютерні мережі також дають суттєвий внесок щодо забруднення навколишнього середовища. Наведені електромагнітні поля все частіше викликають помилки в роботі ІТ-обладнання, впливають на якість зв'язку.

Одночасно з цим існує реальна можливість за допомогою спеціальних засобів, які використовують побічні електромагнітні випромінювання електронних приладів, знімати конфіденційну інформацію з серверів, втручатися у роботу інформаційних систем, прослуховувати переговори або знищувати дані на електронних носіях умисно, а також з необережності.

Традиційні матеріали для екранування електромагнітних полів, рекомендовані національними нормативними актами, у таких умовах недостатньо ефективні та універсальні.

Найбільш перспективними захисними матеріалами є композитні металополімерні матеріали, що підтверджено низкою вітчизняних та закордонних досліджень. Але більшість розробок виконано на модельних матеріалах, непридатних для практичного використання. Тому актуальними є задачі розроблення технологій виготовлення та дослідження захисних властивостей композитних матеріалів малої вартості, придатних для облицювання поверхонь великих площ з прийнятними коефіцієнтами екранування.

Аналіз літературних даних та постановка проблеми

Розробленню сучасних матеріалів для екранування електромагнітних полів та виготовленню екранів різних конструкцій присвячено багато досліджень та прикладних розробок. Це пояснюється недостатньою ефективністю екрануючих поверхонь, які традиційно використовуються, зокрема великими коефіцієнтами відбиття електромагнітних хвиль ультрависоких та вищих час-

тот, що дедалі більше використовуються для засобів бездротового зв'язку.

Праця [1] присвячена розробленню та дослідженню властивостей електромагнітних екранів на основі феромагнетиків, але більшість їх коефіцієнтів екранування забезпечується за рахунок відбиття електромагнітних хвиль, що може погіршувати електромагнітну обстановку поза зоною, яку вони захищають. При цьому їх власне намагнічування може підвищувати рівні магнітних полів наднизької частоти. Дослідження [2] стосується захисту від потужного електромагнітного випромінювання радіолокаторів і має спеціальне призначення.

Розробки вузького застосування досить поширені. Так, праця [3] присвячена розробленню та дослідженню захисних властивостей матеріалів для зниження рівнів електромагнітних полів засобів обчислювальної техніки. А дослідження [4] — для захисту від впливу випромінювань телефонів мобільного зв'язку.

Значна кількість досліджень і розробок присвячена металополімерним захисним матеріалам на основі дрібнодисперсних металевих частинок. Але такі матеріали мають велику вартість через складність технологій отримання металевих частинок нанорозмірів, які потім ще вміщуються у полімерну матрицю [5].

У праці [6] наведено технологію отримання наночастинок безпосереднім синтезом під час полімеризації, але вироблення таким способом захисного матеріалу великої площі практично неможливе.

Багато досліджень стосуються захисних матеріалів для екранування електромагнітного поля широкого діапазону. Але вони або метастабільні через вміст вологи [7], або дуже громіздкі [8], що ускладнює їх практичне використання.

Зниження вартості матеріалу і спрощення технології виготовлення може бути досягнуто за рахунок використання виробничих відходів у якості екрануючого наповнювача. У праці [8] наведено результати розроблення, вироблення та випробувань захисних властивостей електромагнітних екранів на основі відходів виробництва чавуну.

Розміри частинок, які забезпечують екранування прийнятні — 5–30 мкм, але їх вміст у відходах малий (Fe_2O_3 — до 11.5%, FeO — до 4,5 %), тому для забезпечення прийнятних коефіцієнтів екранування — до 10 дБ використовується конструкція клиноподібної форми, що збільшує товщину екрана і робить його непридатним для облицювання поверхонь приміщень будь-якого призначення. При цьому коефіцієнти відбиття складають до 3 дБ, що для діапазонів

ультрависоких і вищих частот, для яких розроблялися екрани, не відповідає сучасним потребам.

Наші попередні дослідження [9] свідчать що коефіцієнти екранування зростають, а коефіцієнти відбиття знижуються зі зменшенням розмірів металевих та металовмісних частинок у полімерній матриці. За вмісту частинок нанорозмірів у 11–12 % (за вагою) забезпечуються коефіцієнти екранування до 10 дБ та коефіцієнти відбиття до 0,3. Підвищення дисперсності частинок у 2–4 рази знижує коефіцієнти відбиття на 0,15–0,20, що особливо важливо для захисту від високочастотних випромінювань. При цьому коефіцієнти екранування складають 7–8 дБ. Товщина екрана складала 5 мм. Наведене свідчить, що за використання наночастинок металеві субстанції можна знижувати рівні електромагнітних випромінювань у 8–10 разів. Досвід натурних вимірювань електромагнітних полів і випромінювань свідчить, що навіть у виробничих умовах, при експлуатації потужного електротехнічного обладнання та радіотехнічних об'єктів цивільної авіації рівні цього фізичного фактору майже ніколи не перевищують гранично допустимі більш ніж у 3–4 рази.

Тому для виготовлення захисних матеріалів доцільно використовувати металеві та металовмісні частинки більших розмірів, які є відходами виробничих процесів. У праці [10] запропоновано виготовлення металополімерного матеріалу на основі дрібнодисперсного пилу залізної руди. Показано, що вміст Fe та FeO у ньому становить до 57 та 15 % відповідно. При цьому дисперсність пилу залежно від місця його відбору у аспіраційній системі становить від 2,5 до 60 мкм. Екрани з цієї субстанції виготовлялися з використанням матриці з полівінілацетату. Коефіцієнти екранування таких екранів з вмістом металеві субстанції 10 % складають 2–5, а коефіцієнти відбиття — 0,2–0,5. Але наведені у працях [9; 10] результати досліджень стосуються електромагнітних екранів, виготовлених на основі модельних полімерів, які не пристосовані для використання у реальних виробничих та побутових умовах. Таким чином, постає проблема розроблення технології, вироблення та дослідження захисних властивостей екрануючого металополімерного матеріалу, спроектованого на принципах розумної достатності захисту, технологічності та економічності доцільності впровадження.

Мета та задачі дослідження

Мета роботи – розроблення технології вироблення, виготовлення та дослідження захисних властивостей композитного металополімерного матеріалу для екранування електромагнітних полів найбільш критичних частот.

Для досягнення мети визначені такі задачі:

– розробити технологію виготовлення металополімерного екрана на основі залізородного пилю;

– виготовити електромагнітні екрани на основі залізних та залізвмісних частинок з різними їх концентраціями у полімерній матриці, придатні для використання у реальних умовах;

– дослідити захисні властивості електромагнітних екранів для різних частот і частотних діапазонів, найбільш критичних для виробничих та побутових умов;

– визначити методологію прогнозування захисних властивостей електромагнітних екранів на стадіях їх проектування з урахуванням частотно-амплітудних характеристик електромагнітного поля, що потребує екранування.

Методи і методики досліджень захисних властивостей електромагнітних екранів

Методи і методики вимірювання захисних властивостей електромагнітних екранів для різних частот або частотних діапазонів суттєво відрізняються. Це зумовлене не тільки використанням різних вимірювальних приладів, а й різними методиками.

У низькочастотній частині електромагнітного спектра критичними є магнітні поля промислової частоти 50 Гц та її гармонік та інтергармонік.

Для вимірювання значень магнітного поля промислової частоти використовувався повірений вимірювач напруженостей електричного і магнітного полів промислової частоти ПЗ–50 згідно інструкції з експлуатації.

Для визначення амплітуд гармонік та інтергармонік магнітного поля промислової частоти, а також усього спектрального складу магнітного поля наднизької частоти використовувався повірений аналізатор спектра Spectran 5030 згідно інструкції з експлуатації.

Для електромагнітних випромінювань ультрависоких і вищих частот критичними, з точки зору впливу на людей, є випромінювання засобів бездротового зв'язку, а саме: 1,8 ГГц, 2,4 ГГц, 2,6 ГГц, 5,1 ГГц. Для вимірювання щільностей потоків енергії від високочастотних джерел використовувався прилад ПЗ–41 згідно інструкції з експлуатації. Цей прилад також дає змогу виміряти інтегральне значення щільностей потоку енергії у потрібному місці діапазону частот 0,3–30 ГГц, що необхідно в умовах впливу багатьох високочастотних джерел електромагнітних випромінювань.

Для визначення коефіцієнтів екранування захисними матеріалами магнітних полів наднизьких частот виготовлялися геометрично замкнені екрани у формі циліндра.

У загальному випадку розміри такого екрана можуть впливати на результати вимірювань у разі використання для його виготовлення феромагнітного матеріалу через намагнічування у зовнішньому магнітному полі. Але випробування показали, що за використання для виготовлення екрана заліза та його окислів у малих кількостях (до 15 % за вагою) такий вплив незначний і не перевищує похибки вимірювальної апаратури.

Для всіх вимірювань похибка не перевищувала 20 %.

Визначення коефіцієнтів екранування електромагнітних випромінювань ультрависоких частот здійснювалося таким чином. Виготовлялися електромагнітні екрани розмірами 0,75×0,75 м. Вони вміщувалися у проріз відповідної форми у металевому листі, що гарантувало неможливість проникнення випромінювання поза екраном. Екран розташовувався між джерелом електромагнітного випромінювання та вимірювальною антеною. Похибка вимірювань також не перевищувала 20 %.

Для розроблення засобів захисту від впливу електромагнітних випромінювань ультрависоких і вищих частот обов'язковим є визначення внеску у загальний коефіцієнт екранування за рахунок відбиття електромагнітних хвиль.

При проведенні усіх експериментів фон зовнішніх магнітного та електромагнітного полів перебував з межами чутливості апаратури.

Технологія виготовлення електромагнітних екранів на основі залізородного пилю та пінолатькесу

Збагачення залізної руди супроводжується виділенням великої кількості пилю, який відводиться і поглинається фільтрами у аспіраційних системах.

За використання шестирядного волоконного фільтру на перших завісах затримуються частинки більших розмірів.

Для проведення досліджень було відібрано металевий та металовмісний пил з 1–2, 3–4 та 5–6 завіс шестирядного волоконного фільтра.

Проаналізувавши вимоги до матеріалу, провівши ряд випробувань різних матеріалів, як основи (матриці) майбутніх електромагнітних екранів, було прийняте рішення зупинитися на композитному матеріалі який в своїй основі має пінолатькесу.

На основі проведених досліджень розроблено матеріал та режими формування виробу електромагнітних екранів з композитного матеріалу із заданими властивостями.

Основними перевагами пінолатькесу, що привели нас до обрання саме цього матеріалу, як до

основи майбутніх електромагнітних екранів визначено таке: пружність, гідрофобність, відсутність деградації за довготривалої експлуатації, можливість вироблення у будь-якому вигляді (листи, рулони), добра адгезія при облицюванні поверхонь та можливість додавання екрануючої субстанції (Fe, FeO, CaO) у потрібних кількостях без суттєвих змін перелічених властивостей.

Процес виготовлення складається з кількох етапів. Найважливішими з них є додавання у стандартну суміш екрануючих частинок потрібної кількості та дисперсності, а також прокатка матеріалу крізь вальці з необхідним зазором з вулканізацією поверхневого шару глибиною 1,0–1,5 мм.

Розроблена технологія є достатньо складною. Тому для проектування електромагнітного екрана бажано попередньо визначити необхідні технологічні параметри розрахунковими методами. Але запропонований нами у попередній роботі [9] математичний апарат не пристосований для прогнозування коефіцієнтів поглинання та відбиття даного матеріалу. Це ж стосується ефектної магнітної проникності – головного показника щодо екранування магнітного поля наднизької частоти.

Дослідження захисних властивостей металополімерних електромагнітних екранів та обговорення результатів

Для проведення випробувань було виготовлено електромагнітні екрани товщиною 5 мм з різною концентрацією (за вагою) металеві та металовмісної субстанції.

Дослідження проводилися з використанням у якості наповнювача залізородних частинок різної дисперсності: 5–10 мкм, 15–25 мкм, 50–100 мкм.

Частота екранованого електромагнітного поля — 1,8 ГГц. Ця частота обрана, виходячи з її найбільшого, на сьогодні, використання у засобах бездротового зв'язку.

Аналіз отриманих результатів свідчить, що підвищення дисперсності екрануючої субстанції у 2–3 рази гарантовано підвищує коефіцієнт екранування у два рази. При цьому суттєво (до 0,1) знижується коефіцієнт відбиття.

З досліджених матеріалів було виготовлено геометрично замкнені конструкції для визначення ефективності екранування магнітної складової електромагнітного поля промислової частоти 50 Гц. Враховуючи квазістаціонарність такого поля, вимірювання коефіцієнта відбиття не має сенсу.

Наведене свідчить, що розроблений екран дозволяє гарантовано знизити рівні магнітних полів наднизьких частот удвічі за вмісту наповнювача на 12 %.

Визначення питомої провідності матеріалу здійснювалося за рахунок вимірювання зворотної величини — питомого опору методом подвійного мосту.

Вимірювання діелектричної провідності виконувалися за мостовою схемою, яка дозволяла отримувати окремо значення електричної ємності від 10 пФ до 10 мкФ та активної складової повного електричного опору (10 Ом – 10 МОм) за $\text{tg}\delta \leq 1000$ (рис. 1).

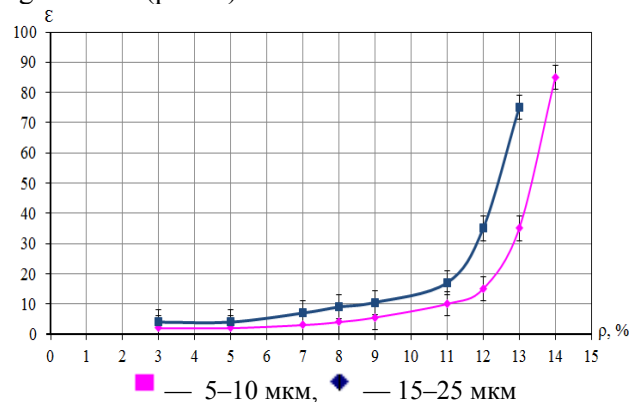


Рис. 1. Залежність діелектричної проникності ϵ металополімерних екранів від вмісту ρ та дисперсності екрануючої субстанції

Отримані дані є основою для прогнозування ефективності електромагнітних екранів залежно від параметрів електромагнітного поля, яке потребує екранування. Кількісні значення питомої провідності та відносної діелектричної проникності використовуються для визначення комплексної діелектричної проникності та її дійсної та уявної складових, необхідних для розрахунків коефіцієнтів поглинання та відбиття електромагнітних хвиль з використанням раніше розробленого математичного апарату [9].

Для розрахункового прогнозування захисних властивостей екрана, для екранування магнітного поля наднизької частоти, необхідні відомості про магнітні проникності матеріалів. Їх пряме визначення складне через залежність від щільності розташування залізних та залізновмісних частинок та складність суміші.

Доцільно визначити цей показник, виходячи з експериментальних даних, враховуючи функціональний зв'язок цих показників.

Розглянемо циліндричний магнітний екран внутрішнім радіусом a , зовнішнім — b , який перебуває у зовнішньому квазістаціонарному магнітному полі напруженістю H_0 (рис. 2).

Зауважимо, що відносна проникність матеріалу екрана μ . Магнітні проникності поза екраном та усередині екрана дорівнюють одиниці. Циліндричний екран вважаємо достатньо довгим уздовж осі Z (перпендикулярно площині рисунку).

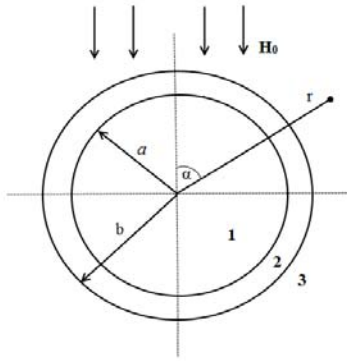


Рис. 2. Схема до розрахунку коефіцієнта екранування магнітного поля наднизької частоти циліндричним екраном

Через відсутність електричного струму в усіх трьох зонах (1, 2, 3), магнітне поле у них описується рівнянням Лапласа:

$$\nabla^2 \varphi = 0, \quad (1)$$

де φ — скалярний магнітний потенціал.

Значення φ залежить тільки від координат r та α циліндричної системи координат. Рівняння (1) у цих координатах має вигляд:

$$\nabla^2 \varphi = \frac{1}{r} \frac{\partial}{\partial r} \left(r \frac{\partial \varphi}{\partial r} \right) + \frac{\partial^2 \varphi}{r^2 \partial \alpha^2} = 0.$$

Розв'язок цього рівняння методом Фур'є надає:

$$\text{— для першої зони: } \varphi_1 = \left(C_1 r + \frac{C_2}{r} \right) \cos \alpha;$$

$$\text{— для другої зони: } \varphi_2 = \left(C_3 r + \frac{C_4}{r} \right) \cos \alpha;$$

$$\text{— для третьої зони: } \varphi_3 = \left(C_5 + \frac{C_6}{r} \right) \cos \alpha.$$

Стала інтегрування, з точністю до якої визначається потенціал, прийнята такою, що дорівнює нулю.

Для визначення шести сталих ($C_1 - C_6$) складемо відповідні рівняння.

Порівняємо φ_3 з виразом на нескінченній відстані $\varphi = H_0 r \cos \alpha$. Це рівняння дає $C_5 = H_0$.

У зоні 1 за $r = 0$ φ повинне залишатися кінцевим. Це може бути тільки у випадку, коли у виразі буде відсутня складова $\frac{C_2}{r}$. Це відбувається за $C_2 = 0$. Рівність φ_1 та φ_2 при

$$r = a \text{ дає рівняння } C_1 a = C_3 a + \frac{C_4}{a}$$

Значення φ на межі зон 2 та 3 ($r = b$) можна визначити з рівняння: $C_5 b + \frac{C_6}{b} = C_3 b + \frac{C_4}{b}$

Рівність нормальних складових індукції $B_r = -\mu_a \frac{\partial \varphi}{\partial r}$ на межі цих зон (за $r = a$):

$$C_1 = \left(C_3 - \frac{C_4}{a^2} \right) \mu,$$

де μ — шукана відносна магнітна проникність екрана.

Рівність нормальних складових індукції за $r = b$ можна визначити з рівняння:

$$C_5 - \frac{C_6}{b^2} = \left(C_3 - \frac{C_4}{b^2} \right) \mu.$$

Спільне розв'язання цих двох рівнянь дає вираз для потенціалу у зоні 1:

$$\varphi_1 = H_0 \frac{2qb^2}{\Delta} r \cos \alpha.$$

Напруженість магнітного поля у зоні 1:

$$H_1 = \frac{\partial \varphi_1}{\partial x} = H_0 \frac{2qb^2}{\Delta}.$$

Коефіцієнтом екранування вважається відношення напруженостей поля поза екраном та у зоні, захищеної екраном, тому

$$K_s = \frac{H_0}{H_1} = \frac{\Delta}{2qb^2} \approx \frac{\mu(b^2 - a^2)}{4b^2}.$$

Таким чином, маючи експериментальні дані щодо коефіцієнтів екранування, можемо визначити магнітні проникності захисних матеріалів, що є головним показником для розрахункового прогнозування захисних властивостей магнітних екранів у низькочастотній області спектра.

Наведені результати дозволяють дійти висновку, що електромагнітні екрани на основі залізорудного пилу мають суттєві переваги порівняно з іншими металополімерними захисними матеріалами.

Отримані дані щодо електрофізичних та магнітних властивостей матеріалу залежно від вмісту та дисперсності металеві та металовмісної субстанції достатні для розрахункового прогнозування ступенів захисту під час розроблення організаційно-технічних заходів з електромагнітної безпеки.

Висновки

1. Висока дисперсність та хімічний склад залізорудного пилу дозволяють використовувати його у якості екрануючого наповнювача у мета-

лополімерних електромагнітних екранах. Його низька вартість обумовлює економічну доцільність виготовлення захисних поверхонь великих площ.

2. Технологія виготовлення матеріалу для екранування електромагнітних полів у вигляді пінолатексу дозволяє керувати захисними властивостями як вмістом провідної субстанції, так і за рахунок використання частинок різної дисперсності.

3. Випробування розроблених матеріалів свідчить, що за вмісту металевих та металовмісних частинок у полімерній матриці 12 % коефіцієнт екранування для частинок розмірами 50–100 мкм складає 2,5 за коефіцієнта відбиття 0,23. Для частинок розмірами 5–10 мкм ці показники складають 12 та 0,1 відповідно. Значне підвищення захисних властивостей з підвищенням дисперсності частинок (особливо зниження коефіцієнта відбиття) обумовлене також структурою пінолатексу.

4. Визначені електрофізичні властивості розробленого захисного матеріалу (питома провідність та діелектрична проникність) та спосіб визначення магнітної проникності залежно від дисперсності та вагового вмісту екрануючої субстанції є вихідними даними для розрахункового прогнозування за відомими співвідношеннями захисних властивостей матеріалів на стадіях проектних робіт з електромагнітної безпеки.

ЛІТЕРАТУРА

1. Экраны электромагнитного излучения на основе магнитных материалов. Технологии. Конструкции. Применение [Текст] / В. А. Богуш, Т. В. Борботько, Н. В. Насонов и др. — Минск : Бестпринт, 2016. — 222 с.

2. **Mei Li**. An Ultrathin and Broadband Radar Absorber Using Resistive FSS [Text] / Li Mei, ShaoQiu Xiao, Yan-Ying Bai, Bing-Zhong Wang // IEEE Antennas and Wireless Propagation Letters. — 2012. № 11. — P. 748–751.

3. **Singh J.** Computer Generated Energy Effects on Users and Shielding Interference [Text] / J. Singh // International Journal of Innovative Research in Computer and Communication Engineering. — 2015. Vol. 3. — P. 10022–10027.

4. **Kasar V.** Novel Approach to Electromagnetic Interference Shielding for Cell Phones [Text] / V. Kasar, A. Pawar // International Journal of Science and Research. — 2014. — Vol. 3. — P. 1869–1872.

5. **Jalali M.** Electromagnetic shielding of polymer—matrix composites with metallic nanoparticles / M. Jalali, S. Dauterstedt, A. Michaud, R. Wuthrich // Composites Part B: Engineering. — 2011. — P. 1420–1426.

6. **Fionov A. S.** Polymer nanocomposites: synthesis and physical properties [Text] / A. S. Fionov, G. Y. Yurkov, O. V. Popkov, I. D. Kosobudskii, N. A. Taratanov, O. V. Potemkina // Advances in Composite Materials or Medicine and Nanotechnology. Rijeka, Croatia: IN-TECH Education and Publishing. — 2011. — P. 343–364.

7. **Аль-Адеми Я.Т.А.** Широкодиапазонные конструкции экранов электромагнитного излучения на основе влагосодержащей целлюлозы [Текст] / Я.Т.А. Аль-Адеми, А.А.А. Ахмед, Т.А. Пулко, Н. В. Насонова, Л. Н. Лыньков // Труды МАИ. — 2014. — № 77. — С. 1–15.

8. Экран электромагнитного излучения на основе порошкообразных отходов производства чугуна [Текст] / О. В. Бойправ, Т. В. Борботько, Л. М. Линьков, В. Б. Соколов // Труды МАИ. — 2014. — Вып. 67. — С. 3–19.

9. **Glyva V.** Research into protective properties of electromagnetic screens based on the metal-containing nanostructures / V. Glyva, V. Kovalenko, L. Levchenko, O. Tykhenko // Eastern-European Journal of Enterprise Technologies. — 2017. — Iss. 3/12 (87). — P. 50–55.

10. Дослідження захисних властивостей електромагнітних екранів на основі дрібно-дисперсного заліза та його сполук [Текст] / В. А. Глива, О. Є. Лапшин, В. В. Коваленко, М. В. Худик // Вісті Донецького гірничого інституту. — 2017. — № 1(40). м. С. 123–127.

Козловський В. В., Глива В. А., Ходаковський О. В.

ЗАХИСНІ ВЛАСТИВОСТІ ЕЛЕКТРОМАГНІТНИХ ЕКРАНІВ НА ОСНОВІ ЗАЛІЗОРУДНОГО ПИЛУ ТА ЇХ ЗАСТОСУВАННЯ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ ТА ЛЮДЕЙ

На основі дослідження хімічного складу та дисперсності залізорудного пилу обґрунтовано доцільність його використання у якості наповнювача для виготовлення композитних металополімерних електромагнітних екранів. Розроблено технологію виготовлення захисних екрануючих матеріалів з керованими захисними властивостями. Досліджено захисні властивості розроблених матеріалів. Встановлено, що збільшення дисперсності металевих та металовмісних частинок у 10–20 разів підвищує загальний коефіцієнт екранування електромагнітного поля надвисокої частоти у 6–8 разів. При цьому коефіцієнт відбиття електромагнітних хвиль знижується з 0,25 до 0,10. Гарантований коефіцієнт екранування магнітного поля промислової частоти за вмісту екрануючої субстанції 12 % складає 1,8–2,2. З'ясовано, що різке підвищення захисних властивостей відбувається за вмісту провідної субстанції 11–12 %. Отримано залежності питомої електричної провідності та діелектричної проникності від вмісту та дисперсності металевої та металовмісної субстанції у полімерній

матриці. Ці дані є основою для розрахункового прогнозування захисних властивостей електромагнітних екранів у залежності від умов їх використання.

Ключові слова: електромагнітний екран, залізорудний пил, коефіцієнт екранування, коефіцієнт відбиття, електрофізичні властивості.

Козловський В. В., Глива В. А., Ходаковський А. В.

ЗАЩИТНЫЕ СВОЙСТВА ЭЛЕКТРОМАГНИТНЫХ ЭКРАНОВ НА ОСНОВЕ ЖЕЛЕЗОРУДНОЙ ПЫЛИ И ИХ ПРИМЕНЕНИЕ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ И ЛЮДЕЙ

На основе исследования химического состава и дисперсности железорудного пыли обоснована целесообразность его использования в качестве наполнителя для изготовления композитных металлополимерных электромагнитных экранов. Разработана технология изготовления защитных экранирующих материалов с управляемыми защитными свойствами. Исследованы защитные свойства разработанных материалов. Установлено, что увеличение дисперсности металлических и металлосодержащих частиц в 10—20 раз повышает общий коэффициент экранирования электромагнитного поля сверхвысокой частоты в 6—8 раз. При этом коэффициент отражения электромагнитных волн снижается с 0,25 до 0,10. Гарантированный коэффициент экранирования магнитного поля промышленной частоты при содержании экранирующей субстанции 12 % составляет 1,8—2,2. Выяснено, что резкое повышение защитных свойств происходит при содержании ведущей субстанции 11—12 %. Получены зависимости удельной электрической проводимости и диэлектрической проницаемости от содержания и дисперсности металлической и металлосодержащего субстанции в полимерной матрице. Эти данные являются основой для расчетного прогнозирования защитных свойств электромагнитных экранов в зависимости от условий их использования.

Ключевые слова: электромагнитный экран, железорудная пыль, коэффициент экранирования, коэффициент отражения, электрофизические свойства.

Kozlovsky V. V., Gliva V. A., Khodakovsky A. V.

PROTECTIVE PROPERTIES OF ELECTROMAGNETIC SCREENS ON THE BASIS OF IRON OER DUST AND THEIR APPLICATION FOR PROTECTION OF INFORMATION AND PEOPLE

Based on the study of the chemical composition and dispersion of iron ore dust, the feasibility of its use as a filler for the manufacture of composite metal—polymer electromagnetic screens was substantiated. The technology of manufacturing protective shielding materials with guided protective properties has been developed. The protective properties of the developed materials are investigated. It was established that an increase in the dispersion of metal and metal—containing particles by 10—20 times increases the overall coefficient of shielding of a high—frequency electromagnetic field by 6—8 times. In this case, the reflection coefficient of electromagnetic waves is reduced from 0.25 to 0.10. The guaranteed shielding coefficient of the magnetic field of the industrial frequency for the contents of the shielding substance is 12% and is 1.8—2.2. It was found out that the sharp increase of protective properties occurs in the content of the lead substance 11—12%. The dependences of the specific electrical conductivity and dielectric constant on the content and dispersion of the metal and metal—containing substance in the polymer matrix are obtained. These data are the basis for the estimated prediction of the protective properties of electromagnetic screens, depending on the conditions of their use.

Keywords: electromagnetic screen, iron-iron dust, shielding coefficient, coefficient of reflection, electrophysical properties.

Стаття надійшла до редакції 04.09.2018 р.

Прийнято до друку 18.09.2018 р.

Рецензент – д-р техн. наук, проф. Мачалін І. О.

V. V. Kozlovskii, Doctor of engineering, Professor
National aviation university
orcid.org/0000-0002-8301-5501
e-mail: vvkzeos@gmail.com

O. V. Ivanov, Head of Foreign Affairs Department
National aviation university,
orcid.org/0000-0001-6550-4419
e-mail: alexkorea5@gmail.com

V. V. Snizhko, postgraduate student
National aviation university
orcid.org/0000-0002-8767-9073
e-mail: bb_c@ukr.net

ANALYSIS AND SECURITY MANAGEMENT OF TELECOMMUNICATION SYSTEMS BASED ON PREDICTIVE TECHNOLOGIES

Introduction

Solving of problems of information security and information security management is becoming vital to the existence and development of any modern organization.

Security is a comprehensive concept and can not be viewed as the sum of its parts. These parts are interconnected and interdependent [1]. In addition, each of these parts is critically significant. Consequently, the methods that involve partial neglect of safety criteria in overall safety assessment are unacceptable. Therefore, the development of the algorithm that allows unifying the approaches of integrated security system management is an urgent task.

Analysis of published data and problem definition

Security is a state and trends of development of protection of critical systems from external and internal negative factors. It is necessary to consider that security is a dynamic multiple objective category [2]. Security activities arise in the course of solving the contradiction between the risk and the need to manage the security: predict, prevent, eliminate and localize the damage from the impact of threats [3]. Comprehensive Security Assessment (CSA) cannot be more than conservative estimates obtained for different aspects of the system [4].

Security does not exist by itself, without human influence. It is provided for people and it is estimated by them. Therefore, the concept of security is not only objective, but also subjective,

because of its evaluation carried out in the end by human [5]. The specific features of the task of creating security systems are [6]:

- incomplete initial information about the composition and nature of threats;
- complex problem of the need to take in account a large number of local indicators;
- presence of both quantitative and qualitative indicators that must be considered in solving problems of design and implementation of security systems;
- inability to use the classical optimization methods [7].

Cognitive analysis of the research object allows [8]:

- to predict the direction of the system (situation) development;
- to identify the factors, which affecting the situation;
- to formalize the decision-making processes;
- to get both qualitative and quantitative characteristics of the situation;

Information risk assessment, which is based on fuzzy cognitive modeling allows [9]:

- to identify the most dangerous threats and vulnerabilities affecting the telecommunication system;
- to assess possible damage from the effects of threats to telecommunication system;
- to adapt to new external and internal threats and technologies;

- to provide a simple and effective mechanism for decision-making services, dealing with information security.

Development of an algorithm that will unify approaches of integrated security managing will solve a number of issues related to the subjective side in the analysis and management of integrated security [10]

The aims and objectives of the research

The aim is to develop an algorithm of analysis and integrated security management based on cognitive modeling. This algorithm will unify approaches in constructing telecommunication security systems.

To achieve this goal it is necessary:

1. To form a matrix, by which the integrated security level can be described.
2. To form a matrix of preventive measures.
3. To form the matrix through which the implementation of preventive measures will be formalized.
4. Present the evaluation of integrated security system in the form of fuzzy cognitive model.

Development of algorithm of analysis and integrated security management

Let's formulate a mathematical model describing the dynamics of changes in the level of integrated security of different systems.

The integrated security level of a system is estimation, based on a set of indicators and criteria that characterize the state of the system in terms of protection of its critical elements.

The integrated security level of a system can be described by such a matrix (security matrix):

$$B = \begin{pmatrix} K_1 & F_1 & V_1 & T_1 & S_1 \\ K_2 & F_2 & V_2 & T_2 & S_2 \\ K_3 & F_3 & V_3 & T_3 & S_3 \\ \dots & \dots & \dots & \dots & \dots \\ K_n & F_n & V_n & T_n & S_n \end{pmatrix}$$

where K_i — the security level of i^{th} criterion; F_i — trend of changes of i^{th} criterion (increases, decreases, neutral); V_i — the speed of changes of i^{th} criterion (low, below average, average, above average, high); T_i — the time, which is characteristic for i^{th} criterion, which can correctly interpret the parameter value V_i ; S_i — the degree of criticality of negative consequences of implementing risk, which decreasing the value of i^{th} criterion.

The first and the fourth column of security matrix characterize the current state of integrated security.

Other columns of the matrix represent the dynamics of the process and allow building a forecast of the future.

In this case, the multiplicative convolution of integrated security integral criterion is a value of:

$$K = \prod_{i=1} K_i^{S_i}.$$

Estimates of S_i can be received by experts. However, in most cases it is difficult to give a direct numerical evaluation of these factors for an expert. Therefore, different ranking methods, during the implementation of which the streamline of criteria is only required, may be used preferably.

It can be used, for example, non-strict ranking method. In accordance with this method, the expert makes the numbering of all the criteria descending degree of acceptability of the negative consequences associated with the safety criterion. Moreover, it is assumed that the expert will not be able to distinguish between a certain criteria. In this case, during the ranking he puts them together in random order. Then ranked criteria are consecutively numbered. The rank of criterion is determined by its number.

If in one place there are several criteria, which are indistinguishable among themselves, generally, the evaluation of each of them shall be equal to the average of their new numbers. However, it seems appropriate to modify such valuation method, taking the rank of each of the criteria for the number of indistinguishable entire group as a whole object in the ordering.

In this way, it can be evaluated the degree of influence of each parameter on private safety criteria K_i as well as the degree of acceptability of impacts of threats S_i .

For example, let an expert streamlined criteria as follows:

$$K_5(K_3, K_7, K_2), K_1(K_6, K_8), K_9, K_4.$$

The criteria, which are not distinguishable between themselves are combined in parentheses.

Then the scores for each of the criteria assessed in accordance with the procedure described above, are:

$$S_5 = 1; S_3 = S_7 = S_2 = 2; S_1 = 3;$$

$$S_6 = S_8 = 4; S_9 = 5; S_4 = 6.$$

Let's apply a valuation on the value equal to the sum of all the evaluations:

$$R = \prod_i S_i.$$

In this case $R = 29$. Thus, after conversion to linear scale [0, 1] to R rate, we will obtain:

$$S_5 = 1/29; S_3 = S_7 = S_2 = 2/29; S_1 = 3/29;$$

$$S_6 = S_8 = 4/29; S_9 = 5/29; S_4 = 6/29.$$

Assessments, which were found with the proposed method are a generalization of Fishburne system of weights for the case of a mixed distribution of preferences, when along with the preferences, the ratios of indifference are included in the system.

Criteria can be grouped in the relevant areas of security in the security matrix, such as: economic, environmental, social, technical, etc.

Thus, each tuple $(K_i, F_i, V_i, S_i, T_i)$ characterizes the state of security on the i -th criterion.

Partial matrix consisting of lines representing a certain direction of safety insurance, describe the condition in the certain field.

K_i safety indicators are closely linked to the consequences of the possible implementation of the existing threats in the system, measures of preventing of such consequences and measures of localization and eliminating of the consequences, if any do arise. It should be emphasized that threats can be divided into primary and secondary. Primary threats exist regardless of the state of the system and have a certain unconditional probability of occurrence. The probability of occurrence of secondary threat is conditional and depends on the state of the system and the state of the environment.

In particular, some of the system can provoke threats, the occurrence of which in other circumstances would have been impossible.

Let's introduce the following notation:

\overline{UG}_i and $\widetilde{UG}_j (i, j = 1, 2, 3, \dots)$ — a set of primary and secondary threats arising with probabilities \overline{PUG}_i and \widetilde{PUG}_j , and have an influence \overline{n}_{km} and \widetilde{n}_{km} on element (k, m) of matrix $B (k = 1, 2, 3, \dots; m = 1, 2, 3, 4, 5)$.

The influence of each of the primary or secondary threats can be described as an influence matrix (IM):

$$N_i = \begin{pmatrix} n_{11} & n_{12} & n_{13} & n_{14} & n_{15} \\ n_{21} & n_{22} & n_{23} & n_{24} & n_{25} \\ --- & --- & --- & --- & --- \\ n_{n1} & n_{n2} & n_{n3} & n_{n4} & n_{n5} \end{pmatrix}$$

It should be noted that the influence \overline{n}_{km} and \widetilde{n}_{km} on some elements of security matrix B can be either negative or positive.

Elements of influence matrix, that have negative influence, are said to be negative regarding elements

of SM. Elements that have a positive influence — positive elements regarding elements of SM. Elements that have no influence, are said to be neutral $\overline{R}_i = \{\overline{N}_i; \overline{PUG}_i\}$ is said to be execution risk of the i^{th} primary threat.

This reflects the emergence of a tuple with probability \overline{PUG}_i effects that change state of the system through the appropriate influence matrix \overline{N}_i .

The probabilities of occurrence of the primary threats. \overline{PUG}_i are not depend from us. However, a set of preventive measures allows to weaken the influence of the primary threats to the level of system security.

It is necessary to analyze the main threats of security of telecommunication systems. They can be divided into two categories: primary and secondary.

The occurrences of the primary threats are independent from us. However, a set of preventive measures of protection allows weakening the influence of the primary threats to the security level of the system [11]. This fact can be described by a matrix of preventive measures (MPM):

$$Z_j = \begin{pmatrix} z_{11} & z_{12} & z_{13} & z_{14} & z_{15} \\ z_{21} & z_{22} & z_{23} & z_{24} & z_{25} \\ --- & --- & --- & --- & --- \\ z_{n1} & z_{n2} & z_{n3} & z_{n4} & z_{n5} \end{pmatrix}$$

where $j = 1 \dots M$, M — total number of preventive measures.

If, despite the preventive protection measures, the implementation of a set of primary threats resulted in consequences, it is necessary to take measures for their localization and elimination.

These measures can be formalized by a matrix of elimination of the consequences (MEC):

$$L = \begin{pmatrix} l_{11} & l_{12} & l_{13} & l_{14} & l_{15} \\ l_{21} & l_{22} & l_{23} & l_{24} & l_{25} \\ --- & --- & --- & --- & --- \\ l_{n1} & l_{n2} & l_{n3} & l_{n4} & l_{n5} \end{pmatrix}$$

We begin to deal with the primary threats before they attack. In the case of secondary threats we have to prevent them, and that is to deal with the reasons that cause them. This is the fundamental difference in units of measures whose effect is formalized by the set of matrices Z_j and matrix L .

In constructing of fuzzy cognitive model (FCM) the object of study is represented as a semantic-oriented graph [12]. As such models in the

evaluation of integrated security system (ISS) may be adopted:

$$KBS = \langle G, QL, E \rangle.$$

G — oriented graph that has one root apex and contains no loop and horizontal edges within the same hierarchy level:

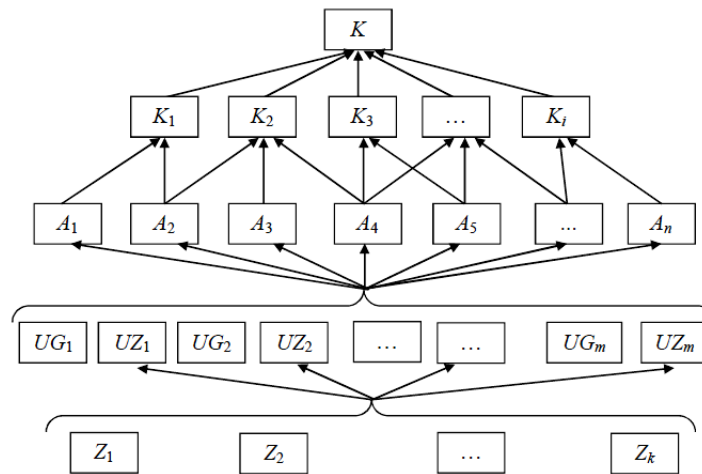
$$G = \langle \{GF_i\}; \{GD_{ij}\} \rangle$$

where $\{GF_i\}$ — set of root apexes (factors or concepts in terms of FCM); $\{GD_{ij}\}$ — the set of arcs, connecting i^{th} and j^{th} apexes (the set of causal relationships between concepts, with the arc arranged so that the beginning of the arc corresponds to the top of the lower level of the hierarchy (rank) and the end of the arc is the top rank in lesser level); $GF_0 = K$ — root apex, which corresponds to the level of integrated security in general (integral security

criterion — target concept); QL — a set of qualitative assessments of levels of each factor in the hierarchy; E — the system of relationships some advantages over other factors according to their impact on a given element.

A generalized example of a graph for a comprehensive assessment of the security of telecommunication system is presented in Figure.

$Z\{1,2,3,\dots\}$ — are preventive measures of protection (security mechanisms), designed to reduce vulnerabilities of telecommunication system — $UZ\{1,2,3,\dots\}$, $UG\{1,2,3,\dots\}$ — are threats to the security of the system, $A\{1,2,3,\dots\}$ — attacks on telecommunication system, $K\{1,2,3,\dots\}$ — individual safety performance indicators at the appropriate criteria, K — comprehensive (integral) Index of telecommunication system security.



Impact of factors on the level of integrated security

It should be noted that this connected graph is not a tree, since it does not meet the requirement of absence of simple cycles. This is because the factors in the lowest level of the hierarchy, may simultaneously affect several factors of higher level.

For example, the use of preventive security measures to protect against a vulnerability can simultaneously remove any other vulnerability or lead to a new one.

Some attacks can cause a change of several individual security criteria (sometimes in the opposite direction).

The general algorithm of analysis and integrated security management, based on fuzzy cognitive modeling, can be represented as follows:

1. Gathering of information about the object of protection: identification of assets and the establishment of an entry-level security. In the process of identification the main characteristics of assets should be considered: information value,

sensitivity to threats, the availability of protective measures. It is necessary to consider that among the factors that affect the safety, the subjective factors, that are the least predictable, occupy a special place.

2. Selection of criteria, which are characterizing the state of various aspects of security, the definition of its acceptable level.

3. Building a cognitive model as a semantic-oriented graph.

4. Calculation and analysis of integrated security level (ISL) of the systems.

5. If ISL is not in the acceptable range of values, then the changes in the concepts involved in building cognitive models should be made. In aspect of relationships between concepts, their values are being changed through the introduction of protective measures.

Thus, the providing of system security provides a solution to two interrelated problems: the direct problem (analysis of system state) and the inverse problem of management (impact on the system).

In addressing the first problem you need to determine the value of protection criteria K_i and integral criterion K for given values of concepts that affect them.

If the values are outside the range of acceptability, then the solution of the inverse problem must choose such control actions of Z_j and L that will provide a return of target criteria in a safe range.

If there is no single set of necessary control actions, at this stage might appear an optimization problem, consisting in finding such combination of Z_j and L , that provides maximum exposure to negative factors in the set or minimal cost for the implementation of methods of protection.

Conclusions

As a result of research:

1. The security matrix was formed, in which indicators of protection, trends and rate of change and the degree of criticality of negative consequences were selected.

2. The set of preventive measures of protection was defined, that allows weakening of the influence of the primary threats to the security of the system.

3. The implementation of preventive measures was formalized, based on the MEC.

4. The algorithm of analysis and management of integrated security systems, based on cognitive modeling, was developed.

Information security management is greatly simplified and formalized using the fuzzy cognitive modeling. Using this approach contributes to solving problems related to the subjective side in the analysis of information risks and threats. The

algorithm allows unifying of approaches to managing of integrated security and beginning of developing of appropriate computational procedures and modules, which can be further used for constructing of telecommunication security systems.

REFERENCES

1. **Haydamakin N.** Concurrent access to information in computer systems — E. : Ural, 2003. — 328 p.
2. **Zegjda D.** Fundamentals of Information System's Security. — M. :Telecom, 2000. — 286 p.
3. **Devianin P.** Computer systems security models — M. : Akademia, 2005. — 144 p.
4. **Kort S.** Theoretical fundamentals of information security. — M. :Gelios, 2004. — 240 p.
5. **Kurilo A.** Information security audit. — M. : BDC-press, 2006. — 304 p.
6. **Saderdinov A.** Information security/ — M. : Dashkovka, 2005. — 336 p.
7. **Petrenko S.** Information Risk Management. Economically justified security. — M. :Press, 2005. — 384 p.
8. **Borisov V.** Fuzzy models and networks. — M. :Telecom, 2007. — 284 p.
9. **Raykov A.** Intelligent Information Technologies. — M. :MGIREA, 2000. — 96 p.
10. **Vasiliev V.** Analysis and management of information security of colleges on the basis of cognitive modeling. — 2007. — № 1, T. 27. — P. 74–81.
11. **Ajmuamedov I.** Management of information security in the region based on cognitive modeling. — 2010. — № 1. — P. 96–102.
12. **Ajmuamedov I.** Modeling based on expert judgments of the evaluation process of information security. — 2009. — № 2. — P. 101–109.

Козловський В. В., Іванов О. В., Сніжко В. В.

АНАЛІЗ ТА УПРАВЛІННЯ БЕЗПЕКОЮ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ НА ОСНОВІ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ

У даній статті аналізуються особливості забезпечення захисту інформації, приймаючи до уваги суб'єктивну сторону даного процесу. Основною метою дослідження є розробка алгоритму аналізу та управління комплексною безпекою, котрий дозволить уніфікувати підходи до управління інформаційною безпекою. Безпека не існує сама по собі, у відриві від людини. Вона забезпечується для людини і нею ж оцінюється. Тому, поняття безпеки має не тільки об'єктивну, але й суб'єктивну сторону, оскільки оцінка її рівня проводиться в кінцевому підсумку людиною. Використання методів когнітивного моделювання дозволяє значно покращити процеси аналізу та управління безпекою телекомунікаційної системи. Переваги когнітивного підходу полягають у можливості моделювання слабоструктурованих (тих, що погано формалізуються) систем, які характеризуються неповнотою або невизначеністю знань про них. Застосування розробленого алгоритму дозволить фахівцям приступити до розробки відповідних обчислювальних процедур і модулів, які можуть бути в подальшому використовуватися при забезпеченні захисту телекомунікаційної системи. Результати досліджень будуть також корисні службам, які займаються забезпеченням інформаційної безпеки.

Ключові слова: інформаційна безпека, комплексна безпека, когнітивне моделювання, телекомунікаційна система.

Козловский В. В., Иванов А. В., Снижко В. В.

АНАЛИЗ И УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ НА ОСНОВЕ ИНТЕЛЛЕКТУАЛЬНЫХ ТЕХНОЛОГИЙ

В данной статье анализируются особенности обеспечения защиты информации, принимая во внимание субъективную сторону данного процесса. Основной целью исследования является разработка алгоритма анализа и управления комплексной безопасностью, который позволит унифицировать подходы к управлению информационной безопасностью. Безопасность не существует сама по себе, в отрыве от человека. Она обеспечивается для человека и им же оценивается. Поэтому, понятие безопасности имеет не только объективную, но и субъективную сторону, поскольку оценка ее уровня проводится в конечном итоге человеком. Использование методов когнитивного моделирования позволяет значительно улучшить процессы анализа и управления безопасностью телекоммуникационной системы. Преимущества когнитивного подхода заключаются в возможности моделирования слабоструктурированных (тех, что плохо формализуются) систем, которые характеризуются неполнотой или неопределенностью знаний о них. Применение разработанного алгоритма позволит специалистам приступить к разработке соответствующих вычислительных процедур и модулей, которые могут быть в дальнейшем использоваться при обеспечении защиты телекоммуникационной системы. Результаты исследований будут также полезны службам, которые занимаются обеспечением информационной безопасности.

Ключевые слова: информационная безопасность, комплексная безопасность, когнитивное моделирование, телекоммуникационная система.

Kozlovskii V. V., Ivanov O. V., Snizhko V. V.

ANALYSIS AND SECURITY MANAGEMENT OF TELECOMMUNICATION SYSTEMS BASED ON PREDICTIVE TECHNOLOGIES

This paper presents the peculiarities of providing information, taking into account the subjective aspect of this process. The main purpose of the study is to develop an algorithm for analyzing and managing integrated security, which will unify the approaches to information security management. Security does not exist by itself, in isolation from a person. It is provided for a person and it is appreciated. Therefore, the notion of security has not only an objective but also a subjective aspect, since the assessment of its level is ultimately man. Using cognitive modeling methods can greatly improve the analysis and management of the security of the telecommunication system. The advantages of the cognitive approach are the ability to simulate poorly structured (poorly formalized) systems that are characterized by incomplete or uncertain knowledge of them. The application of the developed algorithm will allow the specialists to begin to develop appropriate computational procedures and modules, which can be further used in telecommunication system security. The results of the research will be useful for information security specialists.

Keywords: information security, integrated security, cognitive modeling, telecommunication system.

Стаття надійшла до редакції 05.09.2018 р.

Прийнято до друку 18.09.2018 р.

Рецензент – д-р техн. наук, проф. Мачалін І. О.

V. V. Kozlovskii, Doctor of engineering, Professor
National aviation university
orcid.org/0000-0002-8301-5501
e-mail: vvkzeos@gmail.com

S. I. Kubiv, cand. of techn. sciences, associate professor
National aviation university
orcid.org/0000-0001-8567-8765
e-mail: vvkzeos@gmail.com

Yu. V. Balanyuk, cand. of techn. sciences, associate professor
National aviation university
orcid.org/0000-0002-1596-7754
e-mail: vvkzeos@gmail.com

**SINGLE-FACTOR MODEL OF INFORMATION SECURITY THREATS
OF THE AUTOMATED MANAGEMENT SYSTEM OF PRODUCTION
OF HIGH-SPEED TELECOMMUNICATION DISTRIBUTED DATA TRANSFER SYSTEMS**

Introduction

When developing information security systems of the automated control system (ACS) by the production of high-speed distributed data transmission paths, it is necessary to take into account the complex technological process of the whole life cycle of production, which, first of all, includes: software products of information technology supporting the adoption of operational decisions at various stages of the technological cycle, differences between the permittivity of distributed paths and the required values, which caused by technological instability of the manufacturing process, range of geometric dimensions of hard-shaped conductors, deviation of load parameters from nominal values etc. Management of such a complex production process requires enhanced information security of the automated control system: its protection against accidental and deliberate impacts of different nature.

Analysis of published data and problem definition

Analysis of the characteristics of automated control systems [1–3] for the production of high-speed distributed paths and the opinions of experts in this field showed that the dominant mathematical model of risk (risk factor) $\tilde{W}(y)$ and threat $\tilde{N}(y)$ can be represented in the form of stochastic equations

$$\tilde{N}(y) = N(y) + \Delta_1(y), \quad (1)$$

$$\tilde{N}(y) = \frac{\tilde{W}'(y)}{2\tilde{W}(y)}, \quad N(y) = \frac{W'(y)}{2W'(y)}, \quad (2)$$

where y is a variable that has the meaning of the current geometric coordinate of the information channel or another entity $W(y)$ — a deterministic function that characterizes the parameters of the distributed path in the absence of an ASM threat $\tilde{W}(y)$ — the random function of the distributed path (risk factor) when the threat is applied to the control system. Function

$$\Delta_1(y) = g(y)\Delta(y), \quad (3)$$

determines the random process caused by the impact of the threat on the control system. At the same time, based on the technology of production and the opinions of experts, we can assume that the component of the threat $\Delta(y)$ is normal stationary white noise with a correlation function

$$K_{\Delta}(y_1, y_2) = \frac{N_0}{2} \delta(y_2 - y_1), \quad (4)$$

and zero mathematical expectation

$$m\{\Delta\} = 0, \quad (5)$$

$g(y)$ — deterministic function determined by the production process, $g(y) \geq 0$.

From (2) and (3) we find the parameters of the distributed path in case of absence of an ASC threat

$$W(y) = A(y)X, \quad A(y) = \exp\left\{2\int_0^y N(y)dy\right\}, \quad (6)$$

$$X = \tilde{W}(0)\exp\left\{2\int_0^y \Delta_1(y)dy\right\}. \quad (7)$$

We represent the process X in the form

$$X = \exp\{2V\}, \quad (8)$$

Where

$$V = \int_0^y \Delta_1(y) dy + \frac{1}{2} \ln \tilde{W}(0). \quad (9)$$

From the foregoing we see that V is a Markov process with a diffusion coefficient

$$b(y) = \frac{N_0 g^2(y)}{2}, \quad (10)$$

and zero drift coefficient [4–6]. Instead of the expression (9), we use another form of the notation

$$\frac{dV}{dy} = \Delta_1(y), \quad V(0) = \lambda_0 = \frac{1}{2} \ln \tilde{W}(0), \quad (11)$$

$V(0) = \lambda_0$ — initial random value.

It follows from the relations (6), (8) that the statistical characteristics of the risk factor

$$\tilde{W}(y) = A(y) e^{2V} \quad (12)$$

are completely determined by the Markov process V with some flow function $G(v, y)$

Determining the level of information security

First, we consider the threat in which the characteristics of the ACS are limiting and with further strengthening of the destructive effect, the parameters of the control system do not change. In this case, we can assume that the process V is between fixed boundaries. Without loss of generality, we assume that the boundaries are located in the cross sections $V=0$ and $V=2h$.

The probability density $P(v, y)$ of a random process $V(y)$ is found from the Fokker-Planck-Kolmogorov solution [6]:

$$\frac{\partial}{\partial y} P(v, y) = \frac{1}{2} b(y) \frac{\partial^2}{\partial V^2} P(v, y). \quad (13)$$

Separating the variables in this equation

$$P(v, y) = V(v) Y(y), \quad (14)$$

we find,

$$\frac{1}{b(y) Y(y)} \frac{\partial Y}{\partial y} = \frac{1}{2} \frac{1}{V(v)} \frac{\partial^2 V(v)}{\partial V^2} = -\lambda^2, \quad (15)$$

where λ^2 is a positive number. As result, we get

$$V'' + \lambda^2 V = 0, \quad (16)$$

$$Y' + \frac{\lambda^2}{2} b(y) Y = 0. \quad (17)$$

From this we find the function

$$Y(y) = Y(0) \exp \left\{ -\frac{1}{2} \lambda^2 \int_0^y b(y) dy \right\}. \quad (18)$$

Suppose that the boundaries from which the process V is reflected are in sections $V=0, V=2h$. In these sections, the flow $G(v, y)$ must be zero [3].

Since the flow

$$G(v, y) = -\frac{1}{2} \frac{d}{dV} [b(y) P(v, y)], \quad (19)$$

then for the probability density $P(v, y)$ the boundary conditions are satisfied

$$\frac{\partial}{\partial V} P(v, y) \Big|_{v=0} = \frac{\partial}{\partial V} P(v, y) \Big|_{v=2h} = 0. \quad (20)$$

Consequently

$$V'(0) = V'(2h) = 0. \quad (21)$$

Taking into account conditions (21), the solution of equation (16) can be written as a set of orthogonal normalized functions φ_k [6]:

$$\varphi_0(V) = \frac{1}{\sqrt{2h}}, \quad \varphi_k(V) = \frac{1}{\sqrt{h}} \cos \lambda_k V, \quad \lambda_k = \frac{k\pi}{2h}. \quad (22)$$

Hence we find the general solution

$$P(v, y) = \sum_{k=0}^{\infty} C_k e^{-\frac{1}{2} \lambda_k^2 \int_0^y b(y) dy} \cos \lambda_k V. \quad (23)$$

The constants C_k are found from the initial conditions. In particular, for a deterministic process V at the initial point $V(0) = \lambda_0$, we have

$$P(V, 0) = \delta(V - \lambda_0), \quad (24)$$

where $\delta(v)$ is the Dirac delta function.

Then, in accordance with the results of [5]

$$\delta(V - \lambda_0) = \sum_{k=0}^{\infty} \varphi_k(V) \varphi_k(0) \quad (25)$$

we find

$$C_0 = \frac{1}{2h}, \quad C_k = \frac{1}{h} \cos k\pi \frac{\lambda_0}{2h}. \quad (26)$$

Consequently,

$$P(v, y, \lambda_0) = \frac{1}{2h} + \frac{1}{h} \sum_{k=1}^{\infty} \cos \left[\frac{k\pi}{2h} \lambda_0 \right] \times \cos \left[\frac{k\pi}{2h} v \right] \exp \left\{ -\frac{k^2 \pi^2}{8h^2} \int_0^y b(y) dy \right\}, \quad (27)$$

$$0 < \lambda_0 < 2h, \quad 0 < v < 2h.$$

When considering the process in the region $-h, h$, we get

$$P_{-h, h}(v, y, \lambda_0) = \frac{1}{2h} + \sum_{k=1}^{\infty} \cos \left[\frac{k\pi}{2h} (\lambda_0 + h) \right] \cos \left[\frac{k\pi}{2h} (v + h) \right] \exp + \left\{ -\frac{k^2 \pi^2}{8h^2} \int_0^y b(y) dy \right\}, \quad (28)$$

$$-h < \lambda_0 < h, \quad -h < v < h.$$

If we consider the process between arbitrary boundaries $c, d, c < d$, in the above expression it is necessary to go to the new variable [6]:

$$P_{c, d}(v, y, \lambda_0) = P_{\frac{d-c}{2}, \frac{d-c}{2}} \left(v, y, \lambda_0 - \frac{c+d}{2} \right), \quad (29)$$

$$c < \lambda_0 < d, \quad c < v < d.$$

If the initial condition $\lambda_0 = V(0)$ is a random variable, then according to the method of separation of variables [6] the general solution is:

$$P_{c,d}(v, y) = \int_c^d P_{c,d}(v, y, \lambda_0) P_0(\lambda_0) d\lambda_0, \quad (30)$$

$$c < v < d,$$

where $P_0(\lambda)$ is the probability density of the quantity λ_0 .

Now consider the threat in which the characteristics of the control system change over time and lead to a temporary change in the process of managing the production of information transmission channels. In this case, the level of information security will be determined by the probability $q_{c,d}$ with which the process V does not exceed the limits of acceptable limits.

The probability density of a given process is determined by the direct Fokker-Planck-Kolmogorov equation [5; 6]:

$$\frac{\partial}{\partial y} \tilde{P}(v, y, \lambda_0) = \frac{1}{2} b(y) \frac{\partial^2}{\partial V^2} \tilde{P}(v, y, \lambda_0), \quad (31)$$

and the following condition [5]

$$\tilde{P}(c, y, \lambda_0) = \tilde{P}(d, y, \lambda_0) = 0. \quad (32)$$

It is easy to see that this condition is equivalent to observing equality on the boundaries of the domain c, d :

$$V(c) = V(d) = 0. \quad (33)$$

Separating the variables and assuming $c = -h, d = h$ for a nonrandom (deterministic) initial condition, we find the level of information security of the ACS:

$$q_{-h,h}(y, \lambda_0) = \frac{4}{\pi} \sum_{n=0}^{\infty} \frac{(-1)^n}{2n+1} \cos\left[\frac{(2n+1)\pi\lambda_0}{2h}\right] \exp\left\{-\frac{(2n+1)^2\pi^2}{8h^2} \int_0^y b(y) dy\right\},$$

$$-h < \lambda_0 < h. \quad (34)$$

For an arbitrary region of boundaries c, d , according to [4], we have

$$q_{c,d}(y, \lambda_0) = q_{\frac{d-c}{2}, \frac{d+c}{2}}\left(y, \lambda_0 - \frac{c+d}{2}\right). \quad (35)$$

Kozlovskii V. V., Kubiv S. I., Balanyuk Yu. V.

SINGLE-FACTOR MODEL OF INFORMATION SECURITY THREATS OF THE AUTOMATED MANAGEMENT SYSTEM OF PRODUCTION OF HIGH-SPEED TELECOMMUNICATION DISTRIBUTED DATA TRANSFER SYSTEMS

On the basis of the theory of Markov processes, a model of threats to information security of an automated control system for the production of high-speed irregular distributed data transmission systems has been developed. Analytical expressions have been obtained, which allow us to assess the level of information security of the control system for the production of distributed information transmission channels.

Keywords: information security, threat model, production management system, distributed data transmission system, the theory of Markov processes.

With a statistical initial condition with a probability density $P_0(\lambda_0)$, the level of information security is carried out taking into account (35). Intricate, according to theory of random processes [4–6]

$$q_{c,d}(y) = \int_c^d q_{c,d}(y, \lambda_0) P_0(\lambda_0) d\lambda_0. \quad (36)$$

Example

Suppose that the threat to information security λ_0 in the interval c, d is evenly distributed

$$P_0(\lambda_0) = \frac{1}{d-c}. \quad (37)$$

From (34)–(36) we find the level of information security of the ACS:

$$q_{c,d}(y) = \frac{8}{\pi^2} \sum_{n=0}^{\infty} \frac{1}{2n+1} \exp\left\{-\frac{(2n+1)^2\pi^2}{2(d-c)^2} \int_0^y b(y) dy\right\}. \quad (38)$$

Thus, the obtained results allow to estimate the level of information security of the automated production management system for high-speed distributed data transmission paths.

REFERENCES

1. **Denisenko V. V.** Computer control of the technological process, experiment, equipment. — M. : Hot line-Telecom, 2014. — 608 p.
2. **Gerasimov A. V., Titovtsev A. S.** Designing of automated process control systems using SCADA systems. — Kazan, KNITU, 2014. — 128 p.
3. **Gorbunova A. A.** Electromagnetic radiation of technical means. Identification of parameters of sources of secondary electromagnetic emissions of a technical device from measurements in the nearest zone. Lenand, 2016. — 144 p.
4. **Klyatskin V. I.** Stochastic equations: theory and its applications to acoustics, hydrodynamics and radiophysics. Vol. 2. — M. : Fizmatlit, 2008. — 344 p.
5. **Bulinsky A. V., Shiryaev A. N.** Theory of random processes. Fizmatlit, 2005. — 548 p.
6. **Korn G.** Handbook on mathematics for scientists and engineers / G. Korn, T. Korn. — M. : Lan, 2003. — 832 p.

Козловский В. В., Кубів С. І., Баланюк Ю. В.

ОДНОФАКТОРНА МОДЕЛЬ ЗАПОБІГАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ АВТОМАТИЗОВАНОЇ СИСТЕМИ УПРАВЛІННЯ ВИРОБНИЦТВОМ ВИСОКОШВИДКІСНИХ ТЕЛЕКОМУНІКАЦІЙНИХ РОЗПОДІЛЕНИХ СИСТЕМ ПЕРЕДАЧІ ДАНИХ

На основі основ теорії марковських процесів розроблено модель ризиків інформаційної безпеки автоматизованої системи управління виробництвом високошвидкісних нерегулярних розподілених систем передачі даних. Отримано аналітичні вирази, що дозволяють оцінити рівень інформаційної безпеки системи управління виробництвом розподілених каналів передачі інформації.

Ключові слова: інформаційна безпека, модель загроз, система управління виробництвом, розподілена система передачі даних, теорія марковських процесів.

Козловский В. В., Кубив С. И., Баланюк Ю. В.

Однофакторная модель угроз информационной безопасности автоматизированной системы управления производством высокоскоростных телекоммуникационных распределенных систем передачи данных

На основе теории марковских процессов разработана модель угроз информационной безопасности автоматизированной системы управления производством высокоскоростных нерегулярных распределённых систем передачи данных. Получены аналитические выражения, позволяющие оценить уровень информационной безопасности системы управления производством распределённых каналов передачи информации.

Ключевые слова: информационная безопасность, модель угроз, система управления производством, распределённая система передачи данных, теория марковских процессов.

Стаття надійшла до редакції 04.09.2018 р.

Прийнято до друку 18.09.2018 р.

Рецензент – д-р техн. наук, проф. Мачалін І. О.

УДК 621.39

DOI: 10.18372/2310-5461.39.13089

Бараннік В. В., д-р техн. наук, проф.

Харківський національний університет Повітряних Сил імені Івана Кожедуба
orcid.org/0000-0002-2848-4524
e-mail: vvbar.off@gmail.com

Белікова Т. В., канд. техн. наук

Харківський національний університет Повітряних Сил імені Івана Кожедуба
orcid.org/0000-0001-2356-2356
e-mail: vvbar.off@gmail.com

Мусієнко О. П., канд. техн. наук

Харківський національний університет Повітряних Сил імені Івана Кожедуба
orcid.org/0000-0002-2441-4609
e-mail: healsport@meta.ua

Довбенко О. В.

Харківський національний університет Повітряних Сил імені Івана Кожедуба
orcid.org/0000-0002-8305-8852
e-mail: metall1996@ukr.net

МЕТОДИ ВИЯВЛЕННЯ ПРИХОВАНИХ СУГЕСТИВНИХ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ВПЛИВІВ В ІНФОРМАЦІЙНИХ РЕСУРСАХ ТЕКСТОВОГО ЗМІСТУ

Вступ

Останнім часом стало очевидним істотне зростання ролі негативного інформаційного впливу (ІВ) у ході досягнення економічних, політичних, військових цілей державами-агресорами. Водночас, активний розвиток інформаційних технологій привів до якісного розуміння ролі і місця ІВ в системі забезпечення інформаційної та кібернетичної безпеки держави. Агресія Російської Федерації, інші докорінні зміни у зовнішньому та внутрішньому безпековому середовищі створюють передумови для подальшої інтенсифікації такого негативного явища, як кіберзлочинність. Тому протидія їй, у тому числі й у вигляді протидії інформаційним загрозам (ІЗ) у кіберпросторі (КП), є актуальним науковим та прикладним завданням [1].

Справжній момент часу характеризується посиленням ролі інформаційної безпеки, як ключової складової в системі забезпечення національної безпеки держави. У статті 17 Конституції України визначено, що «... забезпечення ... інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу». Однак рівень розвитку інформаційної безпеки не в повній мірі задовольняє потреби суспільства і держави. Одним з факторів, що

впливають на це, є недостатня розвиненість науково-методичної бази забезпечення інформаційної безпеки.

Інформаційна боротьба являє собою комплекс заходів впливу та захисту об'єктів інформаційної безпеки. Одним з них є інформаційно-психологічне протиборство. Пріоритетом у забезпеченні інформаційно-психологічної боротьби є «встановлення методологічних основ і механізмів нейтралізації інформаційно-психологічних впливів проти держави».

Ця задача стає актуальною ще й тому, що суміжні з Україною держави динамічно розвивають структури для проведення інформаційно-психологічного протиборства, які проводяться з метою маніпуляції масовою свідомістю з використанням всіх видів інформаційно-психологічних впливів, включаючи і на підсвідомість людини [2]. Сьогодні поняття «маніпуляція свідомістю» має на увазі впровадження у свідомість ідей, думок і уявлень шляхом розповсюдження спеціально підготовленої за формою і змістом інформації. Сама маніпуляція свідомістю свого широкого поширення набула не тільки і не стільки у військовій сфері, а й в політиці та економіці (рекламній сфері та сфері послуг). Маніпуляція свідомістю використовується й в системі освіти та дошкільного виховання дітей.

Вона може мати як позитивні, так й негативні наслідки та бути направленою на свідому та підсвідому сферу людини. Оскільки маніпуляція є видом духовного та психологічного впливу, мішенню якої є психіка людини, то для досягнення успіху маніпуляція повинна залишатися непоміченою. Успіх гарантований, коли об'єкт маніпуляції вірить, що все відбувається природно та неминуче, а сам факт маніпуляції не відбитий в його пам'яті.

Такий вплив на підсвідомість вимагає значної майстерності та знань. Оскільки маніпуляція суспільною свідомістю стала технологією, то існують професійні працівники, що володіють цією технологією або її частиною, які відносяться до людей не як до осіб, а як до об'єкту, особливого роду речей. Із збільшенням кількості інформації для здійснення сугестивного впливу та протидії йому потрібна велика кількість фахівців та автоматизація процесів для підвищення оперативності.

Звідси актуальним науково-прикладним завданням є автоматизоване виявлення в текстовій інформації сугестивних впливів на підсвідомість людини, нейтралізація таких негативних дій і складання інформаційних матеріалів із заданим видом дії сугестії.

Аналіз останніх досліджень і публікацій

Аналіз стану питання показав, що протидії гібридним загрозам в кіберпросторі до сьогодні майже не приділялася увага науково-експертного співтовариства. Уперше в науковий обіг поняття гібридної загрози в кіберпросторі України було введено відносно недавно — в 2014 р. Поряд з тим слід зауважити те, що складові гібридної загрози в кіберпросторі були розглянуті та досліджені у більш ранніх публікаціях, зокрема в [3] та в працях ін. вчених. У практичній площині нині на стадії формування знаходиться Європейський Центр передового досвіду протидії гібридним загрозам. Однак наукові та практичні здобутки даного підрозділу на сьогодні невідомі. Альтернативний підхід до аналізу був запропонований А. П. Журавльовим.

Даний підхід заснований на визначенні фонетичного значення (семантичного диференціалу) слів російської мови [4]. У своїх працях він представив експериментальні дані лінгвістичної теорії змістовності звукової форми в російській мові.

Реалізуючи підходи виявлення та аналізу фонетичних значень слів з використанням семантичного диференціалу, можна провести аналіз текстових документів і виступів, визначити їх спрямованість та здійснити коректування відповідно заданим характеристикам впливу.

Тому, *метою статті* є реалізація технології аналізу текстів, що дозволить оцінювати ступінь сприйняття підсвідомістю людини прихований сугестивний вплив.

Способи реалізації виявлення інформаційно-психологічних загроз

Способи ведення інформаційно-психологічних операцій визначають цілий ряд підходів та методів для вирішення поставлених завдань. Одним з основних способів є використання друкованих засобів впливу на підсвідомість людини. Для аналізу даних інформаційних ресурсів використовується ціла низка методів і підходів:

- статистичний підхід;
- семантичний метод;
- лінгвістичний підхід;
- фонетичний метод;
- контент-аналіз.

Статистичний підхід дозволяє отримати інформацію про структуру тексту тільки на основі входження в нього окремих слів, ключовими з яких будуть вважатися ті слова, кількість яких в тексті вище заданого кількості.

Семантичні методи дозволяють визначити зміст тесту (предметний зміст), його тематичну спрямованість, а також визначити зв'язки між окремими частинами тексту і тексту в цілому. При цьому якщо в складі двох пропозицій або абзаців є однакові ключові слова або слова з однаковим значенням, то такі пропозиції або абзаци вважаються семантично пов'язаними.

Лінгвістичні підходи (засновані на синтаксичних і морфологічних методах) дозволяють привести текстові форми слів документа до словникових.

Фонетичні методи аналізу дозволяють визначити сугестивну спрямованість текстів.

Контент-аналіз дозволяє визначити частоту появи в тексті певних характеристик, які цікавлять дослідника, а також дозволяє робити деякі висновки про наміри творця цього тексту або можливі реакції адресата.

Метод аналізу інформації заснований на семантичному диференціалі

Семантичний диференціал (СД) — це вид рейтингової шкали, інструмент кількісного і якісного індексування значення з допомогою двополюсних шкал. Використовуються для отримання відношення до даного об'єкта, події або концепції.

Семантичний диференціал Осгуда був додатком більш загальної спроби виміряти семантику або сенс слів, особливо прикметників, і їх поняття.

Респондентів просять вибрати, де їх позиція по шкалі між двома полярними прикметниками

(наприклад: «адекватна-неадекватна», «добрий-злий» або «цінний-даремний»).

Семантичні відмінності можуть використовуватися для вимірювання думок, відносин і цінностей в психометрично контрольованій шкалою.

Тому СД — це метод аналізу слів і текстових документів, заснований на визначенні знакового аспекту по 25 біполярним шкалами.

Кожна шкала являє собою пару антонімів [4].

На практиці аналіз інформаційних і новинних джерел по всіх біполярних шкалах не підходить.

Тому на підставі експертного висновку був визначений рекомендований перелік шкал для розрахунку семантичного диференціала, який наведено в табл. 1. Залежно від розв’язуваних завдань пропонувані шкали на основі експертних оцінок можуть бути змінені (включаючи розробку нових індикативних біполярних шкал) [5]. Сама шкала представлена на рис. 1.

Таблиця 1

Пара антонімів для розрахунку семантичного диференціала

№ шкали	Біполярні шкала		№ шкали	Біполярні шкала	
	Антонім 1	Антонім 2		Антонім 1	Антонім 2
1	Хороший	Поганий	8	Легкий	Важкий
2	Ніжний	Грубий	9	Безпечний	Страшний
3	Світлий	Темний	10	Яскравий	Тьмянний
4	Активний	Пасивний	11	Радісний	Сумний
5	Простий	Складний	12	Хоробрий	Боягузливий
6	Сильний	Слабкий	13	Добрий	Злий
7	Гарний	Відштовхуючий	14	Могутній	Кволий



Рис. 1. Відхилення семантичного диференціалу

Центральне значення шкали — 3,0. Це нейтральне значення, яке не може виділити жоден ознаковий аспект, так само, як і нейтральна зона від 2,5 до 3,5. Все, що виходить за межі коливань можна вважати відхиленням від норми. Області значних відхилень свідчать про те, яку особливість аспекту можна віднести до речі. Оцінки є ймовірнісними, тобто підтверджуються випадковими коливаннями. При цьому самі відмінні аспекти не повинні узгоджуватися зі значенням слова. Це пов’язано з тим, що оцінка дається за змістом звукової форми, а не значення слова.

Перший і більш простий варіант розрахунку полягає у визначенні середньої значущості всіх звуків слова:

$$F = \frac{f_1 + f_2 + \dots + f_n}{n}, \quad (1)$$

де f_n — фонетичне значення окремого звуку в слові; n — кількість звуків в слові.

Фонетичне значення звуків — встановлена ймовірнісна величина. На основі проведення експериментів ця величина може бути змінена. Фонетичне значення для кожного звуку встановлюється окремо залежно від шкали, по якій буде проведений аналіз. У табл. 2 наведено приклад фонетичних значень.

Таблиця 2

Фрагмент фонетичного значення звукобукв

	А	Б	В	Г	Д
Хороший — поганий	1,5	2,4	2,9	3,2	2,4
Світлий — темний	2,2	3,2	3,0	3,3	3,2
Красивий — відштовхуючий	2,0	2,6	3,0	2,8	2,4

Так само не варто забувати про ударний звук, він так само виділяється в слові, хоча і не так як перший, тільки двічі.

Це говорить нам про те, що при розрахунку сумарної фонетичної складової всіх звуків слова, вага першого потрібно збільшити в чотири рази, а ударного в два рази.

Але крім розташування літер у слові, не менш важливу роль відіграє зустрічальність букви в словах. Тобто, є літери часто зустрічаються такі як: А, О, Т, Н, а не рідко зустрічаються: Ф, Х. Звідси можна здогадатися, що рідко зустрічаються букви куди більш помітні в словах, ніж часто зустрічаються і звідси випливає висновок, що при розрахунку значущості слова, потрібно брати до уваги зустрічальність букв в словах. Коефіцієнт народження, інакше ж частотність, величина говорить скільки разів буква зустрічається на тисячу звукобукв. Звукобукви же в свою чергу ще діляться на ударні і ненаголошені.

З цього випливає що інформативність (помітність) звуку знаходиться в зворотній залежності від його частотності (тієї, що зустрічається). Тобто найменш інформативний звук з максимальною частотністю, а решта в стільки разів інформативніше, у скільки разів їх частотність менше максимальної для звуків даного слова.

Підводячи підсумок можна сказати, що при розрахунку фонетичної складової звукового комплексу потрібно збільшити вагу середніх оцінок не тільки для першого і ударного звуків, але також і для всіх звуків, крім звуку з максимальною частотою. Інакше кажучи, необхідно спочатку дописати кожного звуку свою вагу в залежності від положення в слові, а тільки після цього обчислювати середнє арифметичне.

Таким чином, можемо скласти формулу для визначення коефіцієнта кожного звуку в слові:

$$k_i = \frac{P_{\max}}{P_i}, \quad (2)$$

де k_i — це коефіцієнт i -го звуку в слові; P_{\max} — максимальна частотність звуку в даному слові; P_i — це табличне значення частотності звукобукви.

Так само не потрібно забувати про положення букв в слові, для цього необхідно збільшити коефіцієнт першого звуку в чотири рази:

$$k_i = 4 \times k_i = 4 \times \frac{P_{\max}}{P_i}, \quad (3)$$

а для ударного в два рази:

$$k_i = 2 \times k_i = 2 \times \frac{P_{\max}}{P_i}, \quad (4)$$

Після отримання необхідних коефіцієнтів (2)–(4), можна вивести формулу для розрахунку фонетичної складової слова:

$$F = \frac{\sum f_i k_i}{\sum k_i}, \quad (5)$$

де F — фонетична складова слова; f_i — фонетична складова кожного i -го звуку слова; k_i — коефіцієнт для кожного i -го звуку.

Метод аналізу інформації заснований на фонетичному аналізі

Фонетичний аналіз слів чимось нагадує семантичний диференціал, результат зводиться до виведення оцінки слова по шкалах [4]. Але в даному методі оцінка проводиться по 20-ти однополярним шкалам на відміну від семантичного диференціалу з 25-ті біполярними шкалами. Такі ознакові шкали краще підходять для характеристики тексту.

Вони наведені у табл. 3, але залежно від завдань, що вирішуються, запропоновані шкали на основі експертних оцінок можуть бути скорочені або розроблені нові.

Таблиця 3

Признаки для фонетичного аналізу

№ з/п	Признак для аналізу	№ з/п	Признак для аналізу
1	Прекрасний	11	Тужливий
2	Бадьорий	12	Радісний
3	Світлий	13	Стрімкий
4	Нижний	14	Похмурий
5	Мінорний	15	Важкий
6	Сумний	16	Піднесений
7	Яскравий	17	Повільний
8	Темний	18	Тихий
9	Сильний	19	Суворий
10	Страхотливий	20	Зловісний

Методика аналізу базується на тому, що людина звикла в розмовній мові до якоїсь частотності звуків і, як встановили психологи, вона визначає цю частотність досить правильно. Відповідно, будь-яке значне відхилення від цієї частотності має бути відмічене підсвідомістю людини. Визначивши, які звуки переважають в тексті, та надавши їм деякі ознакові описи, можна судити про те, який психоемоційний вплив здійснить той або інший текст на підсвідомість людини.

Відхилення значущості слова від середнього значення робить його виразним або схильним до тієї або іншої ознаки. Тому для оцінки значущості слова необхідна таблиця відхилень значущості звуків, яка будується на основі експертних оцінок. Фрагмент такої таблиці відхилень значущості звукобукв наведено в табл. 4.

Таблиця 4

Фрагмент таблиці відхилень значущості звукобукв

Шкала	Буква				
	А	Б	В	Г	Д
Хороший — поганий	+1,5	+0,6	+0,1	-0,8	+0,6
Світлий — темний	+0,8	-0,8	0,0	-0,7	-0,8
Красивий — відштовхуючий	+1,0	+0,4	0,0	+0,2	+0,6

Значущість слова можна отримати шляхом віднімання значень відхилень значущості звукобукви від середнього значення шкали 3,0.

$$k_{\text{знач}} = 3.0 - k_i. \quad (6)$$

Розрахунок фонетичної складової для слова заснований на наступних етапах:

1) переведення слова або послідовності букв в набір звукобукв. На відміну від семантичного диференціалу, послідовність звукобукв не важлива;

2) вибір для кожної звукобукви табличного значення її частотності та значущості відповідно до аналізованого признакового аспекту. Для цього використовуються 2 таблиці. Перша — таблиця частотності звукобукв, з якої завжди вибираються однакові значення незалежно від ознаки по якому проводиться аналіз. Друга — таблиця відхилення значущості звукобукв від норми, яка має 20 (або по кількості шкал оцінювання) різних наборів для кожної звукобукви залежно від признакового аспекту;

3) визначення частоти входження кожної звукобукви в слово на основі підрахунку загального числа звукобукв в аналізованому слові та кількості кожної звукобукви та операції ділення числа входження звукобукви на загальне число звукобукв в слові;

4) визначення відхилення частотності звукобукв від норми. При цьому, нормальна частотність показує, скільки разів повинна зустрітися певна буква в звичайному тексті. Але, як правило, якщо узяти декілька різних текстів, то частотність точно не збігатиметься з табличним значенням. З цього виходить, що нормальна частотність схильна до коливань. Межі коливань визначаються по теорії вірогідності. За одиницю при вимірюванні розмаху коливань приймають величину σ . У теорії вірогідності вважається, що нормальні коливання якої-небудь випадкової величини не повинні перевищувати $+2\sigma$. Поки величина коливається в цих межах, можна вважати, що вона як би «прив'язана» до середньої точки коливання і далеко від цієї точки не відхилиться. Але якщо коливання перевищать значення $+2\sigma$, то вони ненормальні;

5) розрахунок фонетичного значення слова, яким є сумарне значення внесків кожної звукобукви в загальний звуковий тон тексту. Внесок звукобукви — це перемноження величини відхилення частотності від норми на величину відхилення значущості від нейтральної точки, але тільки тих звукобукв, чиє відхилення істотне від норми. Тому для розрахунку буде використовувати формулу:

$$k_{\text{відх}} = \frac{f_{\text{тек}} - f_{\text{норм}}}{\sqrt{f_{\text{норм}} \times (1 - f_{\text{норм}}) / n_{\text{заг}}}}, \quad (7)$$

де $f_{\text{тек}}$ — частота звукобукви в уже згаданому слові; $f_{\text{норм}}$ — нормальна частота звукобукви в промові; $n_{\text{заг}}$ — кількість звукобукв в слові.

Практична реалізація розглянутих підходів

Розглянуті методи реалізовані в автоматизованому програмному забезпеченні, що аналізує джерела інформаційного тексту російською мовою з використанням методів семантико-диференціального та фонетичного аналізу (рис. 2).

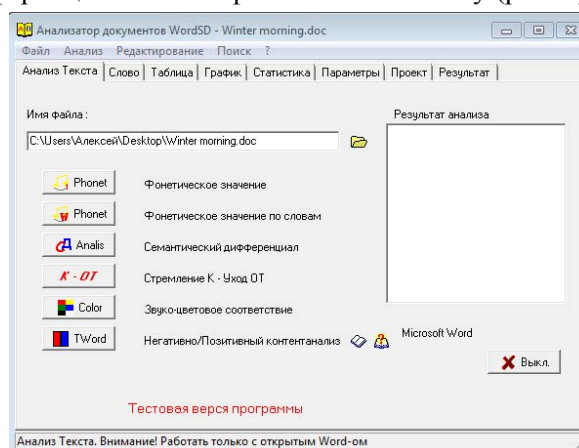


Рис. 2. Головне вікно програми

Програма налаштована на російську мову. У зв'язку з тим, що російська і українська мови належать до слов'янської групи, можна припустити, що якісна оцінка з української мови залишиться без істотних змін. Проводяться додаткові дослідження з адаптації спеціального програмного забезпечення для різних мовних груп.

Таблиці для лінгвістичного аналізу позитивних і негативних слів складаються тільки для тестової версії. Складання повних таблиць, що надаються користувачеві. Автоматизоване складання таблиць може проводитися на основі автоматичного аналізу (за допомогою спеціальної програми, розробленої для цієї мети) груп текстів, представлених експертами і віднесені до певної лінгвістичної (соціальної, професійної тощо) групи. На рис. 3 представлений результат програми у вигляді діаграми результатів характерних аспектів поетичного аналізу Пушкіна А. С. «Зимнее утро».

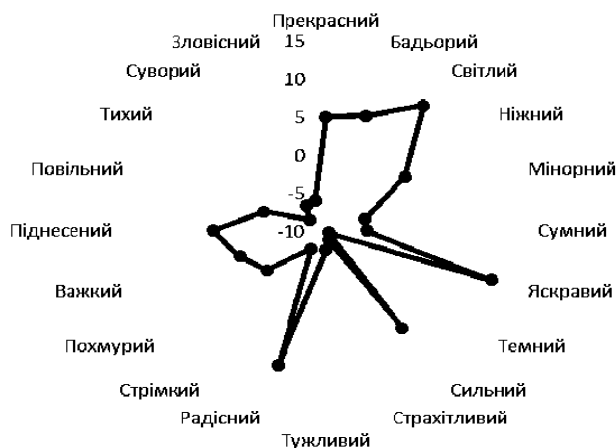


Рис. 3. Діаграма результатів аналізу дослідження

Аналіз діаграми показує, що вірш характеризується такими характерними аспектами: гарний, яскравий, світлий. Всі аспекти мають значні відхилення за шкалою, оскільки вони перевищують значення +5,0.

Найбільш значущим аспектом став знак «яскравий» зі значенням по шкалі +11,21, тобто можна судити про те, що тон вірша досить яскравий і красивий. Що може безпосередньо надати на підсвідомість людини яскравий і красивий емоційний вплив.

Висновки

1. Розглянуто актуальні загрози щодо національної безпеки держави, суспільства та населення. Визначено, що дієвим інструментом впливу на населення інформаційно-психологічний вплив, що має на меті здійснення маніпуляцій зі свідомістю населення.

2. Аналіз існуючих методів визначення інформаційно-психологічного впливу від початку збройної агресії Російської Федерації показав, що дані методи не мають можливості автоматизовано забезпечити інформаційну безпеку суспільства.

3. Розроблені методи, можуть використовуватися для вирішення великого круга завдань з метою виявлення дій сугестій на підсвідомість людини в окремих словах, текстах (документах) цілком і їх різних структурних (складених) елементах. Реалізація даних методів дозволить:

— оцінювати емоційний вплив окремих слів на підсвідомість людини;

— оцінювати емоційний вплив фонетичної структури текстів на підсвідомість людини;

— оцінювати рівень агресивності текстів на основі аналізу позитивного і негативного впливу окремих слів на змістовне значення тексту загалом;

— задавати характеристики бажаного впливу і створювати (коригувати) структури відповідної спрямованості.

ЛІТЕРАТУРА

1. Світова гібридна війна: український фронт: монографія / за заг. ред. В. П. Горбуліна. — К. : НІСД, 2017. — 496 с.

2. Алімпієв А. М. Особливості гібридної війни РФ проти України. Досвід, що отриманий Повітряними Силами Збройних Сил України / А. М. Алімпієв, Г. В. Певцов // Наука і техніка Повітряних Сил Збройних Сил України. — 2017. — № 2. — С. 19–25.

3. Бараннік В. В. Теоретичні основи створення технологій протидії прихованим інформаційним атакам в сучасній гібридній війні / В. В. Бараннік, Т. В. Белікова, С. О. Сідченко. — Х. : ХНУПС Наука і техніка Повітряних Сил Збройних Сил України, 2017. — 133 с.

4. Журавлев А. П. Фонетическое значение / А. П. Журавлев. — Л.: ЛГУ, 1974.

5. Белікова Т. В. Методи виявлення деструктивних сугестивних інформаційно-психологічних операцій в інформаційно-соціальному просторі / Т. В. Белікова // Радиоелектроніка і інформатика. — 2016. — № 3. — С. 62–68.

6. Сідченко С. А. Тестирование семантической составляющей для выявления сугестивного воздействия / С. А. Сідченко, Т. В. Сапрыкина, В. А. Школярченко // Автоматизированные системы управления и приборы автоматики. — 2013. — Вип. 165. — С. 111–117.

Бараннік В. В., Довбенко О. В., Белікова Т. В., Мусієнко О. П.
МЕТОДИ ВИЯВЛЕННЯ ПРИХОВАНИХ СУГЕСТИВНИХ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ВПЛИВІВ В ІНФОРМАЦІЙНИХ РЕСУРСАХ ТЕКСТОВОГО ЗМІСТУ

У статті розглянуто питання, пов'язані з обробкою інформаційних ресурсів, для виявлення прихованих сугестивних впливів. Показано, що інформаційно-психологічний вплив характеризується різною семантичною насиченістю. Тому особливу увагу при обробці інформаційних ресурсів необхідно приділити аналізу сугестивної насиченості, тобто найбільш значимої інформації з прихованим інформаційно-психологічним впливом. Обґрунтовується вибір технології обробки інформаційних ресурсів, при якій вдасться вилучити ключову інформацію. Пропонується створення систем забезпечення інформаційної безпеки держави в інформаційному просторі, а також необхідність використання приведених методів аналізу інформаційних ресурсів для виявлення прихованих сугестивних впливів. Запропоновано варіант спеціального програмного забезпечення з використанням наведених методів.

Ключові слова: інформаційно-психологічний вплив, інформаційна безпека, сугестивний вплив, маніпуляція.

Barannik V. V., Dovbenko O. V., Belikova T. V., Musienko O. P.
METHODS OF DETECTION OF THE HIDDEN INDOCTRINATED INFORMATION AND PSYCHOLOGICAL INFLUENCES IN INFORMATION RESOURCES OF THE TEXT CONTENT

The article deals with issues related to the processing of information resources to identify hidden suggestive effects. It is shown that the information and psychological impact is characterized by different semantic saturation. Therefore, special attention in the processing of information resources should be paid to the analysis of suggestive saturation, that is, the most important information on hidden information and psychological effects. The choice of technology of processing of information resources at which it will be possible to extract key information is proved. It is proposed to create systems to ensure information security of the state in the information space, as well as the need to use these methods of analysis of information resources to identify hidden suggestive effects. The variant of special software using the following methods is proposed.

Keywords: information and psychological impact, information security, suggestive influence, manipulation.

Бараннік В. В., Довбенко О. В., Белікова Т. В., Мусієнко А. П.
МЕТОДЫ ВЫЯВЛЕНИЯ СКРЫТЫХ ВНУШАЕМЫХ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКИХ ВОЗДЕЙСТВИЙ В ИНФОРМАЦИОННЫХ РЕСУРСАХ ТЕКСТОВОГО СОДЕРЖАНИЯ

В статье рассматриваются вопросы, связанные с обработкой информационных ресурсов, для выявления скрытых сугестивных воздействий. Показывается, что информационно-психологическое воздействие характеризуется различной семантической насыщенностью. Поэтому особое внимание при обработке информационных ресурсов необходимо уделить анализу сугестивной насыщенности, то есть наиболее значимой информации по скрытым информационно-психологическим воздействием. Обосновывается выбор технологии обработки информационных ресурсов, при которой удастся извлечь ключевую информацию. Предлагается создание систем обеспечения информационной безопасности государства в информационном пространстве, а также необходимость использования приведенных методов анализа информационных ресурсов для выявления скрытых сугестивных воздействий. Предложен вариант специального программного обеспечения с использованием следующих методов.

Ключевые слова: информационно-психологическое воздействие, информационная безопасность, сугестивное влияние, манипуляция.

Стаття надійшла до редакції 15.09.2018 р.
Прийнято до друку 25.09.2018 р.
Рецензент – д-р техн. наук, проф. Мачалін І. О.

УДК 621.372.852

DOI: 10.18372/2310-5461.39.13090

Ю. П. Бойко, канд. техн. наук
Національний авіаційний університет
orcid.org/ 0000-0003-2344-3632
e-mail: julia_boyko2010@ukr.net

Т. Ю. Приходько, аспірант
Національний авіаційний університет
orcid.org/ 0000-0001-6909-7697
e-mail: tata@mirohost.net

І. О. Басюк, аспірант
Національний авіаційний університет
orcid.org/0000-0002-2666-1136
e-mail: basya2000@gmail.com

ОГЛЯД СУЧАСНИХ ФІЛЬТРУЮЧИХ ПРИСТРОЇВ НВЧ І ЇХ МЕТОДІВ ПОБУДОВИ

Вступ

Добре відомо, яку важливу роль відіграють в радіотехніці коливальні системи. Коливальними системами для діапазону надвисоких частот (НВЧ) є резонатори, що являють собою великий і значний клас пристроїв НВЧ.

При розробці радіотехнічних пристроїв часто доводиться стикатися з труднощами, які викликані суперечностями, а іноді і не сумісністю з вимогами, що ставляться до таких пристроїв.

Пристрій може мати задовільні технічні характеристики, але не задовольняти питанню технологічності під час серійного виробництва, або вимогам комплексної мікромініатюризації, чи навпаки. Тому, як правило, при проектуванні, наприклад, бортових систем вдаються до компромісного рішення у виборі конструкції пристрою.

Це зазвичай відноситься і до проектування фільтруючих систем радіотехнічних пристроїв літальних апаратів, а саме, до вибору елементної бази пристрою.

Постановка завдання дослідження

Провести огляд сучасних фільтруючих пристроїв НВЧ, сучасні уявлення про їх основні властивості та методи побудови, оскільки істотним чинником, що визначає проблеми фільтробудування є те, що перехід до інтегральних схем, які містять елементи з розподіленими параметрами, супроводжується рядом небажаних явищ: добротністю, паразитними смугами пропускання і хвильовими типами коливальних.

Дослідження показало, що оптимізація конструктивних параметрів коливальних систем таким чином, щоб змінювались їх частотні характеристики, призведе до зменшення втрат резонаторів.

Аналіз літературних даних і виклад основного матеріалу

Промисловістю досягнуто значного прогресу в використанні досягнень функціональної мікроелектроніки, яка вирішує завдання фізичної інтеграції селективних кіл. Найбільш перспективними напрямками розвитку мікроелектроніки є: кріоелектроніка, акустоелектроніка, магнітоелектроніка. Розглянемо наведені напрямки.

Кріоелектроніка заснована на використанні явища надпровідності при наднизьких температурах, займається застосуванням явищ в твердих тілах при криогенних температурах нижчих за 120 К у присутності електричних, магнітних і електромагнітних полів для створення електронних приладів і пристроїв, що працюють на основі цих явищ.

Кріоелектроніка, в даний час, швидко розвивається, але промисловістю ще не налагоджено виробництво відповідних розробок [2].

Акустоелектроніка вивчає і використовує взаємодію високочастотних (з частотою вище за 20 кГц) акустичних хвиль з електричним полем і електронами в твердих тілах, вона заснована на використанні різних діелектриків: сегнетоелектриків і п'єзоелектриків. Широке застосування знайшли пристрої на поверхневих акустичних хвилях (ПАХ) [1]. Ці пристрої мають хороші частотно-виборчі властивості, надійні, технологічні, малогабаритні. Найбільш поширеними пристроями на поверхневих акустичних хвилях є резонатори і фільтри. Діапазон роботи найбільш відомих зустрічно-штирьових перетворювачів (використовується для перетворення електромагнітних хвиль в поверхневі акустичні хвилі) становить 0,01 ГГц–2 ГГц і обмежується геометричними розмірами електродів.

У радіоелектронних системах обробки і передачі інформації об'ємні акустичні хвилі використовуються в лініях затримки і кварцових резонаторах для стабілізації частоти.

Після створення термостабільної високочастотної кераміки з малими втратами і високим значенням діелектричної проникності ($\epsilon_r > 100$) широке поширення в діапазоні до 10 ГГц отримали фільтри на діелектричних резонаторах (ДР) [3–8]. Їх перевагами є висока технологічність і малі розміри, а недоліком — виникнення паразитних резонансів на частотах, що перевищують максимальну частоту смуги пропускання.

Основним застосуванням твердотільних резонаторів є використання їх в малогабаритних фільтрах різних конструкцій. На основі діелектричних резонаторів зазвичай створюються мініатюрні смугасто-загороджувальні і смугасто-пропускні фільтри, в тому числі, і в інтегральному виконанні.

Принцип побудови смугасто-загороджувальних фільтрів (СЗФ) заснований на використанні зв'язку діелектричного резонатора з узгодженою лінією передачі. При сильному зв'язку проходження електромагнітної енергії зменшується за рахунок відбиття енергії до входу пристрою.

Перспективними є фільтруючі системи на хвилеподібно-діелектричних резонаторах, які при невеликих розмірах дозволяють отримати дуже вузьку смугу пропускання. У праці [9] описаний фільтр такого типу, що дозволяє в діапазоні 10 ГГц отримати величину габаритного індексу $\delta = 0,49$ при ширині смуги пропускання 0,75 %.

У магнітоелектроніці застосовуються феритові резонатори, що мають малі розміри і дозволяють перебудовувати частоту фільтра в широких межах [10; 11]. Зацікавленість до використання в техніці надвисоких частот намагнічених феритових зразків зумовлена такими їх властивостями, як резонансний характер взаємодії з електромагнітним полем і можливість магнітної перебудови резонансної частоти; різноманітна взаємодія з хвилями, магнітні складові яких поляризовані по колу в протилежних напрямках (невзаємність); залежність магнітних властивостей феритового зразка від амплітуди магнітної складової електромагнітного поля (нелінійність). Однак у бортових фільтруючих системах феритові резонатори не знайшли широкого застосування через великі розміри системи підмагнічування, а також наявності паразитних резонансів.

Крім феритів знаходять застосування магнітодіелектрики [12–13]. У зазначених працях показано їх використання в якості поглиначів електромагнітної енергії. Вони являють собою матері-

ал типу феррит-смола, у який вводять металеві волокна. Величина діелектричної проникності регулюється розмірами волокон. Цей поглинач в одношаровому виконанні можна використовувати для придушення різних типів внутрішніх радіоперешкод. Крім того його можна використовувати при створенні вузькосмугових частотно-виборчих пристроїв [14].

В останні роки отримав розвиток ще один клас фільтруючих систем — фільтри на основі діелектричних брусків, у яких використовуються ті чи інші резонансні елементи. Так, у праці [15] запропоновано фільтр у вигляді металізованого діелектричного паралелепіпеду, у якому резонансні елементи виконані у вигляді наскрізних металізованих отворів, розімкнутих з протилежних сторін. Зв'язок із зовнішніми колами здійснюється за допомогою отворів зв'язку. Для таких фільтрів характерна висока технологічність, хороша термостабільність, малий габаритний індекс. Однак недостатньо розроблені методи розрахунку таких фільтрів, що вимагає складних експериментальних доведень.

Великий інтерес являють собою фільтри на сферах ЖПГ, резонатор НВЧ-діапазону на основі феромагнітного резонансу в залізо-ітрієвому гранаті. Їх перспективність полягає в можливості перебудови частоти в широких межах, високодобротні, однак вони мають складну магнітну систему і складні у виробництві (вимагають наукоємних доведень).

Натепер для виробництва НВЧ апаратури переважно використовуються полоскові лінії передачі, оскільки ці лінії найбільш повно задовольняють вимогам комплексної мікромініатюризації [16]. Полоскові системи стають серйозними конкурентами хвилеподібних вузлів, дозволяючи, в ряді випадків, з вигодою скористатися методом друкованих схем для виробництва елементів радіотехнічних пристроїв. Практично двовимірною конфігурацією полоскової лінії дозволяє конструювати мініатюрні схеми, що виконують складні функції, здійснення яких в хвилеподібному виконанні могло б виявитися технологічно дуже важким, а іноді і нездійсненним завданням.

У пристроях НВЧ, зокрема, в фільтрах, найбільш жорсткі вимоги пред'являються до базових елементів. У зв'язку з цим спроби реалізувати багато видів пристроїв частотної селекції виявилися безуспішними, оскільки мініатюрні резонатори на полоскових лініях зазвичай мають низьку добротність і не дозволяють отримати високі рівні режекції і круті фронти амплітудно-частотних характеристик [1–3]. Істотним фактором, що визначає проблеми фільтробудівництва є те, що перехід до інтегральних схем, з наяв-

тю елементів з розподіленими параметрами, супроводжується рядом небажаних явищ. Що стосується полоскових ліній, то в першу чергу, мова йде про добротність, паразитні смуги пропускання і хвилеподібні типи коливань (вищі типи хвиль). За рахунок збільшення відстані між пластинами або ширини смужки можливе підвищення добротності коливальних систем. Однак існує межа, зумовлена появою хвилеподібних типів коливань. У зв'язку з цими природними фізичними обмеженнями є напівхвильові розміри ширини струмонесучої смужки і відстані між нею і заземленою пластиною (товщина підкладки). Якщо ця вимога не виконується, то вздовж лінії можуть поширюватися вищі типи коливань, створюючи додаткові (паразитні) резонанси, що робить резонатор практично марним.

Зауважимо, що на частотах настільки високих, що довжина хвилі сигналів стає сумірною з розмірами поперечного перетину лінії передачі, виникають нові, відмінні від ТЕМ, типи хвиль. Самі по собі вони не викликають втрату сигналу,

але утворюють небажані фазові спотворення, які обмежують максимальну швидкість.

Найбільшого ефекту слід очікувати від використання полоскових ліній передачі в діапазоні більше 1 ГГц і вище, де у них практично немає конкурентів [3–5]. Функціональні можливості інтегральних мікросхем, що містять елементи на полоскових лініях, досить широкі, оскільки верхня межа застосовності останніх досягає 250 ГГц [38]. Однак, великим недоліком резонансних систем, що виконані на полоскових лініях, розімкнутих на кінці, є наявність втрат на випромінювання. При досить коротких резонаторах близько 90 % втрат зумовлено втратами на випромінювання, а решта 10 % — дисипативними втратами [7].

Виходом з цього положення є включення розімкнутих полоскових резонансних систем на прохід (рис. 1). Виходячи з протиріч, що виникають при конструюванні мініатюрних резонаторів, вони виконуються на напівхвильових і чвертьхвильових відрізках ліній [4].

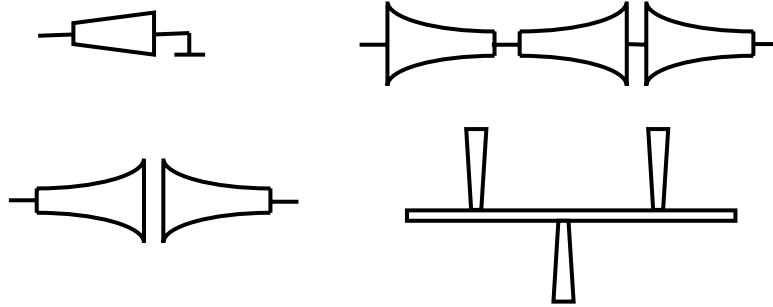


Рис. 1. Приклади включення резонаторів на неоднорідних лініях

Оскільки крім втрат у провіднику і діелектрику максимальна величина добротності полоскової лінії обмежується саме втратами через наявність східчастих неоднорідностей [5; 6], то стає очевидним, що ця обставина є основним фактором, що перешкоджає широкому використанню східчастих резонаторів в частотно-виборчих колах.

В останні роки розвитку теорії і техніки фільтрів на перший план висунуто завдання розробки мініатюрних варіантів резонаторів з поліпшеними електричними характеристиками, такими як висока добротність, необхідна розрядка спектра резонансних частот і т. д., і тим самим підвищеними селективними властивостями [7–9]. Практично вичерпано можливості однорідних (регулярних) ліній в частині створення резонаторів з високими техніко-економічними показниками. Так, центральна частота першої паразитної смуги пропускання досить поширених фільтрів на розімкнутих резонансних відрізках дорівнює подвоєній резонансній частоті, що є істотним недоліком і не дозволяє виконати вимоги ЕМС (електромагнітної сумісності) [13–16]. Дана об-

ставина викликала необхідність впровадження нових методів реалізації кіл з розподіленими параметрами, серед яких можна виділити тенденцію до використання неоднорідних (нерегулярних) ліній передачі. Зміна хвильового опору за координатою дає додатковий степінь вільності при конструюванні кіл різного призначення і дозволяє створити вузли, функціональні можливості яких вище, ніж у аналогічних конструкцій на однорідних лініях [1]. Принципова можливість застосування неоднорідних ліній в якості резонаторів, наприклад, смугасто-пропускних фільтрів з широкими смугами режекції, зумовлена тим, що вони дозволяють отримати збільшену розрядку спектра резонансних частот. Вибором відповідного закону зміни хвильового опору (для полоскових резонаторів — закону зміни ширини провідної смужки уздовж лінії), досягається підвищення добротності резонатора на неоднорідній лінії. Можливі варіанти таких резонаторів і фільтрів показані на рис. 1. Іншим типом фільтруючих систем є фільтри на коаксіальних резонаторах, наведений на рис. 2.

Для підвищення вибіркової фільтрів за рахунок високої добротності резонаторів, найчастіше використовують у вигляді чвертьхвильових короткозамкнених відрізків коаксіальних ліній передачі.

Як правило, вони складаються з декількох резонаторів, короткозамкнених або розімкнених на кінці і пов'язаних між собою індуктивним або ємнісним зв'язком (рис. 2) [9–11]. Для зменшення габаритів резонаторів простір між внутрішнім і зовнішнім провідниками заповнюється діелектричним матеріалом. При цьому габарити резонаторів зменшуються в $\sqrt{\epsilon_r}$ раз.

Такі фільтри мають найменший, з описаних вище, габаритний індекс.

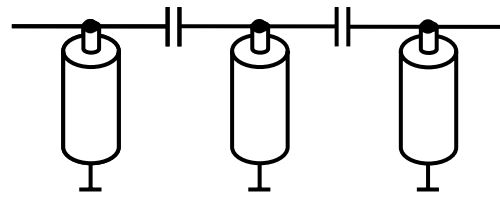


Рис. 2. Коаксіальний фільтр з ємнісними зв'язками

Приклади характеристик фільтрів на коаксіальних резонаторах з різним заповненням наведені в таблиці [12].

Параметри	Резонатор з повітряним заповненням	Резонатор з керамічним заповненням
Частотний діапазон, МГц	300–3000	300–3000
Невантажена добротність резонаторів	1000–1100	750–900
Ширина смуги пропускання на рівні 3 дБ, %	10–15	7–16
Ширина смуги пропускання на рівні 30 дБ, %	20–30	20–40
Внесені втрати, дБ	0,8–1,5	1–1,5
Габарити, мм	150×100×60	40×15×12
Вага, г	450–500	20–25
Вартість, \$	70–80	5–6

Огляд літературних джерел показав, що на сьогодні як діелектрики в основному використовують матеріали з відносною діелектричною проникністю $\epsilon_r = 10 - 300$, що має тангенс кута діелектричних втрат $\text{tg}\delta = 1,5 \times 10^{-4} - 20 \times 10^{-4}$.

Для поліпшення фільтрувальних властивостей резонаторів застосовують резонатори спеціальної ступінчастої форми [1], рис. 3, а, б, що дозволяє змістити першу паразитну смугу на $(6-8) f_0$, де f_0 — перша резонансна частота (основна частота).

Для досягнення цієї самої мети використовують резонатори з плавною зміною діаметра провідників [3], рис. 3, в.

Однак такі резонансні системи складні у виготовленні і застосовуються порівняно рідко. Змінювати хвильовий опір уздовж лінії можна також за рахунок зміни діелектричної проникності уздовж резонатора. На практиці така реалізація зводиться до додавання шайб з різними значеннями діелектричної проникності. Можна домогтися мінімізації втрат в коливальній системі і тим самим отримати максимально можливу добротність, використовуючи переваги обох способів досягнення підвищеної розрядки спектра резонансних частот, а також вибравши оптимальні розміри елементів конструкції резонаторів з урахуванням можливості виникнення вищих типів хвиль.

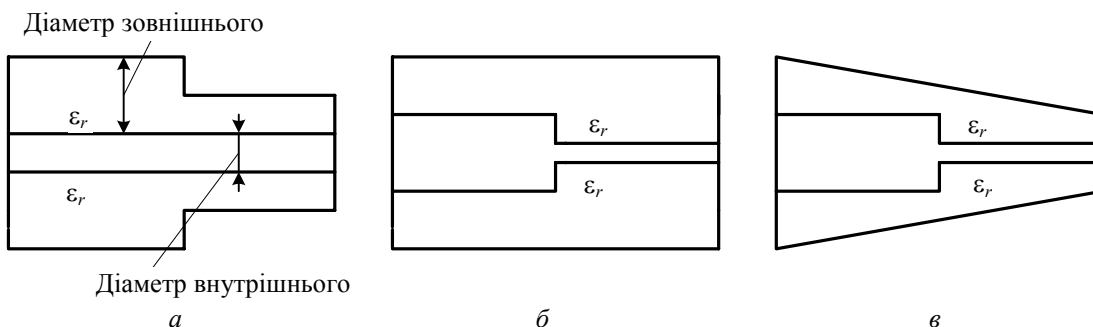


Рис. 3. Резонатори на нерегулярних коаксіальних лініях

При формуванні провідного покриття обирають матеріали, що володіють малими втратами (мідь, срібло, золото). Товщина основного провідного шару обирається залежно від робочої частоти і становить, зазвичай, величину в 3–5 разів більшу товщини скін-шару [4].

Так, у діапазоні частот до 2 ГГц, провідник повинен мати товщину не менше 12–15 мкм, від 2 до 4 ГГц–6–10 мкм.

Недоліком фільтрів на коаксіальних резонаторах є наявність паразитної смуги пропускання, що знаходиться на потроєній резонансній частоті.

Добротність резонатора є визначальною характеристикою будь-якого резонансного елемента. Вона враховує всі фактори теплових втрат і його габаритні розміри. При вирішенні питань мікромініатюризації необхідно чітко уявляти якою ціною доводиться розплачуватися за зменшення розмірів як самих розподілених елементів, так і пристроїв на їх основі. Закономірною, для більшості резонаторів, є залежність власної добротності і частоти від об'єму (об'єми всіх типів резонаторів, крім феритових, обернено пропорційні кубу частоти). Для більш повної і об'єктивної оцінки резонаторів користуються безрозмірним узагальненим параметром якості [11]:

$$K = \frac{10^{-3} Q_0}{V}$$

де Q_0 — навантажена добротність резонатора; V — об'єм резонатора.

Чим більше параметр якості, тим краще характеристики резонатора. У праці [12] для порівняльної оцінки фільтрів вводиться критерій якості, що враховує об'єм і прямі втрати фільтра, а також добротність і кількість резонаторів. Параметри якості відображають суперечливість характеристик резонаторів і фільтрів у тому сенсі, що прагнення в даному типі резонатора поліпшити одну з характеристик, погіршує іншу. Наприклад, збільшення добротності призводить до збільшення габаритів системи.

Отже, остаточний вибір типу резонатора конкретного пристрою визначається всією сукупністю вимог, що пред'являються до цього пристрою, від електричної характеристики системи в яку він повинен бути встановлений, вимог по ефективності придушення перешкод, в тому числі частоти зрізу і верхньої граничної частоти ослаблення, тобто частотних характеристик фільтруючого кола, а також вимог, визначених умовами експлуатації і від реальних обмежень по установці в апаратурі. Всі ці фактори пов'язуються з електричними характеристиками які можна розділити на такі групи:

- вимоги з частотного діапазону;

- вимоги з навантаження;
- вимоги зі струму витоку;
- вимоги щодо послаблення імпульсних перешкод;
- вимоги з стійкості до зовнішніх впливів;
- вимоги до конструкції.

Так, резонатори на відрізках коаксіальних ліній мають високу, порівняно з полосковим резонатором, добротність (отже, і високу вибірковість, малі втрати при відносній ширині смуги пропускання до 5 %), але, як правило, використовується верхня межа їх робочої частоти обмежується 6–8 ГГц. Це обмеження викликано тим, що при постійному діаметрі з підвищенням частоти добротність зростає, однак, коли довжина резонатора стає менше діаметра, виникає небезпека появи вищих коливань (коливань, відмінних від TEM). У зв'язку з цим, при підвищенні частоти одночасно зі зменшенням довжини резонатора необхідно зменшувати і його діаметр, а це в свою чергу призводить до зниження добротності. Аналіз вищевикладеного наштотує на висновок про те, що існують оптимальні параметри конструкції резонатора з точки зору отримання максимальної добротності.

При розробці фільтрів на відрізках неоднорідних полоскових ліній передачі використані далеко не всі можливості підвищення вибірковості резонансних систем з мінімальними втратами. В існуючих в даний час методах розрахунку резонаторів відсутнє урахування впливу втрат, а самі методики, як правило складні і громіздкі. Крім того, вони, як правило, не завершені алгоритмами синтезу коливальних систем. Немає простої і зручної формули розрахунку добротності резонаторів різних типів конструкцій на відрізках неоднорідних ліній.

Висновки

Дослідження показали, що оптимізація конструктивних параметрів коливальних систем таким чином, щоб змінювались їх частотні характеристики, призведе до зменшення втрат резонаторів. З аналізу фільтрувальних систем видно, що виборчі властивості існуючих конструкцій можна підвищити за рахунок оптимізації їх конструктивних параметрів, використовуючи приховані резерви мінімізації втрат з метою відповідності цих систем вимогам ЕМС.

ЛІТЕРАТУРА

1. **Беляков А. Ю.** Расчёт СВЧ полосковых фильтров с частотными характеристиками специального вида / А. Ю. Беляков, Е. В. Петров, В. Е. Попов, А. П. Штейнгарт // *Вестник новгородского государственного университета.* — 2015. — №8. — С. 45–57.

2. **Маттей Г. Л.** Фильтры СВЧ, согласующие цепи и цепи связи / Г. Л. Маттей, Л. Янг, Е. М. Джонс. — Т. 1. — М. : Связь, 1971. — 439 с.

3. **Беляков А. Ю.** Методика проектирования металлокерамических фильтров СВЧ с применением программ 3D-моделирования / А. Ю. Беляков, Е. В. Петров, В. В. Попов, А. П. Штейнгарт // Вестник НовГУ. Сер. : Техн. науки. — 2014. — №81. — С. 26–30.

4. **Atia A. E.** New types of band-pass filters for satellite transponders / A. E. Atia, A. E. Williams // COMSAT Tech. Rev. — 1971. — Vol. 1. — P. 21–43.

5. **Cameron R. J.** Advanced Coupling Matrix Synthesis Techniques for Microwave Filters / Cameron R. J. // IEEE Transactions On Microwave Theory and Techniques. — 2003. — Vol. 51. — №1. — P. 1–10.

6. **Маттей Г. Л.** Фильтры СВЧ, согласующие цепи и цепи связи / Г. Л. Маттей, Л. Янг, Е. М. Джонс. — Т. 2. — М. : Связь, 1972. — 495 с.

7. **Беляков А. Ю.** Методика проектирования металлокерамических фильтров СВЧ с применением программ 3D-моделирования // А. Ю. Беляков, Е. В. Петров, В. В. Попов, А. П. Штейнгарт // Вестник Новгородского государственного университета им. Ярослава Мудрого. — 2014. — №. 81. — С. 26–30.

8. **Cameron R. J.** Advanced coupling matrix synthesis techniques for microwave filters / R. J. Cameron // IEEE Transactions on Microwave Theory and Techniques, 2003 IEEE International Conference. — 2003, vol. 51, no. 1. — P. 1–10.

9. **Gui Y. S.** High sensitivity microwave detection using a magnetic tunnel junction in the absence of an external applied magnetic field / Y. S. Gui et al. // Applied Physics Letters. — 2015. — Т. 106. — №. 15. — С. 152–403.

10. **Koochakzadeh M.** Tunable filters with nonuniform microstrip coupled lines / M. Koochakzadeh, Abbaspour-Tamijani A. // IEEE Microwave and Wireless Components Letters. — V. 18(5). — 2008. — P. 314–316.

11. **Xuan L. M.** Design of dual-stop-band microwave filter based on the magnetoelectric composite / L. M. Xuan, H. M. Zhou, F. Li // Fuzzy Systems and Knowledge Discovery (FSKD), 2011 Eighth International Conference on. — IEEE, 2011. — Т. 4. — С. 2263–2266.

12. **Li-Ming Xuan** Design of dual-stop-band microwave filter based on the magnetoelectric composite / Li-Ming Xuan, Hao-Miao Zhou, Fang Li // Fuzzy systems and knowledge discovery (FSKD), 2011 Eighth International Conference on July IEEE, 2011. — P. 2263–2266

13. **Wang Xu** Tunable microwave filters based on discrete ferroelectric and semiconductor varactors / Wang, Xu, et al. // IET microwaves, antennas & propagation. — V. 5, 7, 2011. — P. 776–782.

14. **Chun Y. H.** Tunable slotted ground structured bandstop filter with BST varactors / Y. H. Chun, J. S. Hong, P. Bao, T. J. Jackson, & Lancaster, M. J. // IET microwaves, antennas & propagation. — 3(5), 2009. — С. 870–876.

15. **Jia-Shiang Fu.** A ferroelectric-based impedance tuner for adaptive matching applications microwave symposium digest / Jia-Shiang FU, Zhu X. A. Phillips, J. D. Mortazawi A. // IEEE MTT-S 2008 International. 2008. — P. 955–958.

16. **Нефедов Е. И.** Полосковые линии передачи: Электродинамические основы автоматизированного проектирования интегральных схем СВЧ / Е. И. Нефедов, А. Т. Фиалковский. — М. : Изд-во «Наука», 1980. — С. 468.

Бойко Ю. П., Приходько Т. Ю., Басюк І. О.

ОГЛЯД СУЧАСНИХ ФІЛЬТРУЮЧИХ ПРИСТРОЇВ НВЧ І ЇХ МЕТОДІВ ПОБУДОВИ

Добре відомо, яку виключно важливу роль відіграють в радіотехніці коливальні системи. Коливальними системами для діапазону надвисоких частот є резонатори, що представляють великий і значний клас пристроїв НВЧ. У статті проведено огляд сучасних фільтруючих пристроїв НВЧ, сучасні уявлення про їх основні властивості та методи побудови. Істотним чинником, що визначає проблеми фільтробудування є те, що перехід до інтегральних схем, що містять елементи з розподіленими параметрами, супроводжується рядом небажаних явищ: добротність, паразитні смуги пропускання і хвильові типи коливань. Дослідження показало, що оптимізація конструктивних параметрів коливальних систем таким чином, щоб змінювались їх частотні характеристики, призведе до зменшення втрат резонаторів.

Ключові слова: НВЧ, фільтр, фільтрація, лінія передачі, смуга пропускання, хвиля, хвилевід.

Бойко Ю. П., Приходько Т. Ю., Басюк И. А.

ОБЗОР СОВРЕМЕННЫХ ФИЛЬТРУЮЩИХ УСТРОЙСТВ СВЧ И ИХ МЕТОДОВ ПОСТРОЕНИЯ

Хорошо известно, какую важную роль играют в радиотехнике колебательной системы. Колебательными системами для диапазона сверхвысоких частот является резонаторы, представляющие большой и значительный класс устройств СВЧ. В статье проведен обзор современных фильтрующих устройств СВЧ, современные представления об их основных свойствах и методы построения. Существенным фактором, определяющим

проблемы фильтростроения является то, что переход к интегральным схемам, содержащим элементы с распределенными параметрами, сопровождается рядом нежелательных явлений: добротность, паразитные полосы пропускания и волновые типы колебаний. Исследование показало, что оптимизация конструктивных параметров колебательных систем таким образом, чтобы менялись их частотные характеристики, приведет к уменьшению потерь резонаторов.

Ключевые слова: СВЧ, фильтр, фильтрация, линия передачи, полоса пропускания, волна, волновод.

Boyko Y., Prikhodko T., Basiuk I.

REVIEW OF MODERN MICROWAVE FILTERING DEVICES AND THEIR METHODS OF CONSTRUCTION

It is well known that oscillatory systems play an extremely high role in radio engineering. The resonators are oscillatory systems for the ultrahigh frequency range that representing a large and significant class of superhigh frequency devices. The article provides an overview of modern superhigh frequency filtering devices, recent interpretations about their main properties and methods of construction. An important factor that defines an issue of filter composition is the transition to integrated circuits containing elements with distributed parameters which accompanied by a number of undesirable phenomena: Q -factor, parasitic bandwidth and wave types of oscillations. The research has shown that the optimization of the design factors of oscillatory systems in such a way that their frequency characteristics are changed, will reduce the losses of the resonators.

Keywords: superhigh frequency devices, filtering devices, transmission line, bandwidth, wave, waveguide.

Стаття надійшла до редакції 18.09.2018 р.

Прийнято до друку 25.09.2018 р.

Рецензент – д-р техн. наук, проф. – Козловський В. В.

А. В. Ільєнко, канд. техн. наук, доц.
Національний авіаційний університет
orcid.org/0000-0001-8565-1117
e-mail: ilyenko.a.v@nau.edu.ua

С. С. Ільєнко, канд. техн. наук, доц.
Національний авіаційний університет
orcid.org/0000-0002-0437-0995
e-mail: ilyenko.s.s@nau.edu.ua

ПРОГРАМНИЙ МОДУЛЬ З ВИКОРИСТАННЯМ ПРОЦЕДУРИ ФОРМУВАННЯ ТА ВЕРИФІКАЦІЇ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПISУ

Вступ

Сьогодні в Україні активно розвивається інформаційне суспільство, однією з характеристик якого можна назвати орієнтацію на інтереси людей. У 1993 р. сутність інформаційного суспільства була розкрита Комісією ЄС: «Інформаційне суспільство — це суспільство, у якому діяльність людей здійснюється на основі використання послуг, що надаються за допомогою інформаційних технологій та технологій зв'язку». В такому суспільстві кожний громадянин має можливість створювати і накопичувати інформацію та знання, мати до них вільний доступ, користуватися та обмінюватися ними і, таким чином, реалізовувати свій у потенціал у сфері забезпечення особистого розвитку та підвищення якості життя.

Проблема збереження електронних документів від копіювання, модифікації і підробки потребує для свого вирішення специфічних засобів і методів захисту. Одним з поширених в світі засобів такого захисту є електронний цифровий підпис, який за допомогою спеціального програмного забезпечення підтверджує достовірність інформації документу, його реквізитів і факту підписання конкретною особою. Програма електронного документообігу з використанням електронно-цифрового підпису (ЕЦП) на сьогодні активно впроваджується в державних установах і органах державної влади, що істотно розширює можливості застосування ЕЦП і розвиток електронного документообігу в Україні.

Постановка завдання дослідження

Завданням даної роботи є характеристика теоретичних основ алгоритмів формування та верифікації ЕЦП з метою розробки програмного модуля для реалізації захисту інформаційних ресурсів, а саме забезпечення цілісності та конфіденційності інформації на базі удосконаленої схеми

ДСТУ 4145-2002. Також проведення оцінювання ефективності отриманої модифікації алгоритму ДСТУ 4145-2002, що ґрунтується на перетвореннях в групі точок еліптичної кривої, з умови надання їй можливості відновлювати інформаційне повідомлення за допомогою обраного криптографічного алгоритму.

Теоретичні основи класифікації алгоритмів формування та верифікації ЕЦП

Існують різні класифікації сучасних схем електронного цифрового підпису. Їх можна класифікувати за механізмом побудови (симетричні та асиметричні), з відновленням повідомлення чи без, одноразові та багаторазові, детерміновані та ймовірнісні, за проблемою, що покладена у їх основу.

Усі схеми ЕЦП також можна розділити на два великих класи: звичайні цифрові підписи (з доповненням) та електронні цифрові підписи з відновленням повідомлення. В ЕЦП з відновленням частина або повне повідомлення можуть бути відновленими з цифрового підпису, тобто для перевірки цифрового підпису необхідно знати тільки цифровий підпис та, можливо, сертифікат відкритого ключа. В ЕЦП з додаванням – цифровий підпис приєднується до повідомлення та зберігається і передається з ним, а для перевірки ЕЦП потрібно обов'язково мати сертифікат відкритого ключа [1].

Теоретичне обґрунтування та практичні дослідження ЕЦП з відновленням повідомлення були виконані, порівняно з ЕЦП з доповненням, пізніше. Значною мірою вони з'явилися, коли виникла необхідність в ЕЦП для коротких повідомлень. У 2003 р. був прийнятий міжнародний стандарт ISO/IEC 15946-4.

До нього було включено п'ять незалежних алгоритмів ЕЦП з відновленням повідомлення

(ECNR, ECMR, ECAO, ECPV, ECKNR), криптографічні перетворення в якому базуються на еліптичних кривих. У подальшому цей стандарт було удосконалено, і він був прийнятий в 2006 р. як ISO/IEC 9796-3 [2] на заміну існуючому. Стандарт ISO/IEC 9796-3 поширює й уточнює алгоритми, що вказані в ISO/IEC 15946-4, і з 2008 р. є основним стандартом підписів з відновленням повідомлення. Підписи мають спільну загальну схему Німберга–Руппеля, але в них використовують для оптимального використання r -компоненти модифікованого алгоритму передпідпису [3]. Додатково до нього був включений алгоритм ЕЦП, що ґрунтується на перетворенні в полі Галуа.

Схеми ЕЦП з відновленням повідомлення доцільно використовувати в інформаційних системах і протоколах з чітко визначеними повідомленнями. Це є принциповою особливістю з погляду їх застосування. Схема ЕЦП з відновленням повідомлення дає перевагу при застосуванні повідомлень невеликого розміру. Електронно-цифровий підпис, розроблений за такою схемою, може ефективно використовуватися в інфраструктурах з відкритими ключами, у протоколах з малим розміром повідомлення, наприклад, електронних магазинах для захисту товарів і послуг тощо.

Схеми з відновленням мають характерну особливість: зменшення розміру підпису за рахунок маскуванню у зворотній компоненті. Зменшення підпису має й негативні наслідки – підпис може мати менший розмір за рахунок зменшення збитковості, але це робить його потенційно більш вразливим до екзистенційної підробки.

Підпис з відновленням повідомлення, порівняно з підписом з доповненням, надає додаткову послугу безпеки — конфіденційність. Також для невеликих обсягів повідомлення можливо зробити таємною всю інформацію, що передається, у самому підписі. Відновити повідомлення можливо у разі відтворення передпідпису, що у загальному випадку можливо тільки при перевірці ЕЦП.

Таким чином, можна стверджувати, що повідомлення можна відновити лише за наявності відкритого ключа.

У відкритих системах така схема не має сенсу з надання послуг конфіденційності, але у разі, якщо циркуляція відкритих ключів в системі є контрольованою, є сенс у використанні цієї власливості схем з доповненням [4].

Окрім алгоритмів, зазначених в ISO/IEC 9796-3, до схем з відновленням інформаційного повідомлення належать схеми RSA, p-NEW, Zhang.

Особливо необхідно відзначити, що усі підписи з відновленням повідомлення є асиметричними з погляду складності обчислення й перевіряння ЕЦП. Указане має бути враховано при обчисленні та перевірянні ЕЦП в реальному масштабі часу.

При порівнянні схем без відновлення повідомлення були виявлено, що алгоритми RSA та El-Gamal при однаковому розмірі ключа матимуть однакову криптостійкість (приблизно $2,7 \cdot 10^{28}$ для ключа 1024 біта). Але алгоритм El-Gamal є набагато швидшим за RSA при підписуванні документа, але поступається у швидкості при верифікації. Перевагою схеми El-Gamal є те, що при заданому рівні стійкості алгоритму цифрового підпису цілі числа, що беруть участь в обчисленнях, мають запис на 25 % коротше (в RSA множники повинні бути від 1024 біт, а в El-Gamal від 512 біт), що зменшує складність обчислень майже в два рази і дозволяє помітно скоротити обсяг використовуваної пам'яті. Крім того, процедура формування підпису за схемою El-Gamal не дозволяє обчислювати цифрові підписи під новими повідомленнями без знання секретного ключа. Проте схема El-Gamal поступається схемі RSA у неможливості відновлювати повідомлення та у тому, що довжина цифрового підпису в 1,5 рази більша, а це збільшує час її обчислення [6].

Перевагою алгоритмів DSA та ECDSA є менший розмір підпису, ніж в RSA та El-Gamal (у середньому 320 біт), тому що основні параметри системи мають розмірність 160 біт за замовчанням. Також при перевірці підпису більшість операцій з числами також проводиться за модулем числа довжиною 160 біт, що скорочує обсяг пам'яті і час обчислення [5]. Проте вважається, що ECDSA є більш криптостійким через складність проблеми дискретного алгоритмування по точках еліптичної кривої. Крім того, секретний ключ в ECDSA є унікальним, а не лише випадковим, як у DSA, що покращує надійність алгоритму. Алгоритм DSA має і недолік в тому, що він призначений лише для підписування/верифікації електронних документів, а не для їх шифрування/дешифрування, на відміну від усіх інших розглянутих алгоритмів. Але його перевагою може бути відносно нескладна реалізація та невелика затрата ресурсів.

Перевагою та особливістю схем з відновленням повідомлення є те, що наявна можливість не тільки переконатися у правдивості повідомлення, а ще й з тіла цифрового підпису автоматично отримати безпосередньо саме повідомлення. Це дозволяє ЕЦП зберігати не тільки цілісність переданого повідомлення, а й конфіденційність.. Схеми NR/ECNR зазвичай ефективні для роботи

з повідомлення невеликої довжини, тому що в такому випадку буде відновлюватися все повідомлення. Але варіант підписання великого повідомлення даними алгоритмами також передбачений, у такому випадку за допомогою збитковостей буде знаходитися частина повідомлення, що не зможе відновитися, і буде передаватися разом з підписом, а після перевірки ця та відновлена частина поєднаються, і можна буде отримати початкове повідомлення. Також дані алгоритми мають перевагу в криптостійкості та складності математичних проблем, на яких вони засновані. А застосування функцій знаходження збитковостей може гарантувати менші обсяги підпису на коротких повідомленнях. Окрім цього, завдяки тому, що схема ECNR діє з використання еліптичних кривих, це дає змогу використовувати параметри та ключі менших обсягів (а це оптимізує об'єм використовуваної пам'яті та збільшує швидкість при передачі даних). Саме тому найбільш ефективним та оптимальним був обраний алгоритм ECNR.

Сучасні схеми цифрового підпису можуть бути класифіковані відповідно до складної матема-

тичної проблеми, що лежить у їх основі та забезпечує їхню безпеку, а саме проблема дискретного логарифму в групі точок еліптичної кривої (ПДЛЕК); проблема дискретного логарифму (ПДЛ); проблема факторизації цілих чисел (ПФЧ).

За критерієм проблеми, що лежить в основі, можна зробити висновок, що найбільш криптостійкими будуть алгоритми, що ґрунтуються на ПДЛЕК.

До алгоритмів, заснованих на проблемі знаходження дискретного логарифму в групі точок еліптичної кривої над простим полем, можна віднести ECDSA, EC-KDSA, ECSS, ECNR.

У 2013 р. були досліджені та порівняні алгоритми, засновані на даних проблемах, для значення 10^{11} MIPS (величина, що показує число мільйонів інструкцій, які виконуються процесором за одну секунду під час деякого штучного тесту) років необхідних для злому закритого ключа [7]. Як порівнювальні характеристики, були взяті мінімальні ознаки, за яких реалізується дана криптостійкість.

Результати порівняння зафіксовані в табл. 1.

Таблиця 1

Характеристики математичних проблем під час створення ЕЦП

Проблема, що лежить в основі алгоритму	ПФЧ	ПДЛ	ПДЛЕК
Розмір системних параметрів (біт)	1024	2208	481
Розмір підпису (біт)	1024	320	320
Розмір відкритого ключа (біт)	1088	1024	161
Розмір закритого ключа (біт)	2048	160	160

З цього випливає, що для того, щоб досягти нормального рівня безпеки при ПФЧ та ПДЛ необхідно використовувати ключ розміром 1024 біт, у той час як для алгоритму с ПДЛЕК достатньо ключа розміром 160 біт. Використання ключів меншої довжини зменшує кількість даних, які потребують обробки, зберігання та передачі по каналам зв'язку, а з поширенням технологій ЕЦП на мобільні пристрої, смарт-карти та інші пристрої з жорсткими обмеженнями обчислювальної спроможності, об'єму пам'яті та використовуваного трафіку, дана характеристика може стати вирішальною при виборі алгоритму ЕЦП. Крім того, було проаналізовано зміну розміру ключа відповідно до збільшення криптостійкості. На рис. 1 можна побачити, що для алгоритмів з ПДЛЕК розмір ключа не так швидко та стрімко зростає, на відміну від алгоритмів з ПФЧ або ПДЛ.

Порівняння трьох складних математичних проблем, на яких базуються відомі асиметричні криптосистеми підпису, виявило той факт, що

жодна з них не є доказово надійною. Роки інтенсивних досліджень призвели до загальноприйнятого переконання, що ПДЛЕК значно складніша ніж проблема факторизації цілих чисел та ПДЛ, оскільки невідомо алгоритму загального спрямування з субекспоненційним часом виконання. І крім того алгоритм з ПДЛЕК при менших розмірах параметрів, що використовуються в обчисленнях та передаються по каналу зв'язку, здатний забезпечити більшу криптостійкість порівняно з іншими алгоритмами ЕЦП.

Важливим є розгляд основного Державного стандарту України, який установлює механізм цифрового підписування, що ґрунтується на властивостях груп точок еліптичних кривих над полями $GF(2^m)$.

Необхідність його дослідження та подальшого використання полягає в тому, що саме в ньому встановлено механізм побудови ЕЦП та правила його застосування, які діють та застосовуються в більшості організацій та підприємств різних рівнів на території України.

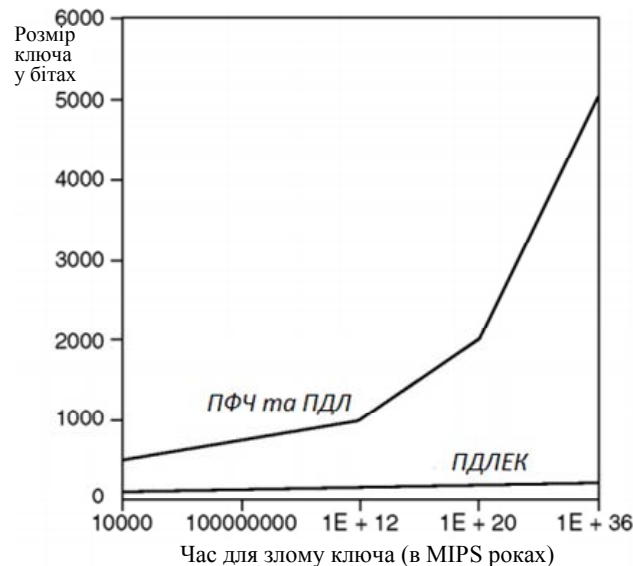


Рис. 1. Порівняння розмірів ключів відповідно до рівнів безпеки для різних схем створення ЕЦП

ДСТУ 4145-2002 (повна назва: «ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка») — національний стандарт України, що описує алгоритми формування та перевірки електронного цифрового підпису. Затверджено та надано чинності наказом Державного комітету України з питань технічного регулювання та споживчої політики від 28 грудня 2002 р. № 31.

Цей стандарт установлює механізм цифрового підписування, оснований на властивостях груп точок еліптичних кривих над полями $GF(2^m)$, та правила застосування цього механізму до повідомлень, що пересилаються каналами зв'язку та/або обробляються у комп'ютеризованих системах загального призначення. Застосування цього стандарту гарантує цілісність підписаного повідомлення, автентичність його автора та неспростовність авторства [8, с. 6]. Стандарт гнучкий, стосовно вибору параметрів безпеки (наприклад, для нього можна обирати будь-яку функцію гешування, а не тільки ту, що зазначена в самому стандарті). Це дозволяє використовувати та підлаштовувати його майже під будь-яке апаратне та програмне середовище. Окремо треба відмітити те, що існують відкриті бібліотеки на мовах C/C++ та Java, у яких реалізовані основні криптопримітиви зі стандарту. Найбільшими перевагами є невеликий обсяг відкритого ключа (а це забезпечує досить швидко передачу та процес верифікації) та математична проблема, що покладена в основу механізму дії алгоритму. Найбільше переваг (висока криптостійкість та малі розміри параметрів) було знайдено в схемах з ПДЛЕК.

Модифікація стандарту ДСТУ 4145-2002 для надання йому можливості відновлювати інформаційне повідомлення за допомогою алгоритму ECNR

У попередній роботі було визначено теоретичні основи подальших шляхів удосконалення схеми ЕЦП відповідно до ДСТУ 4145-2002 з можливістю відновлення повідомлення, що дозволяє ввести додаткову послугу забезпечення конфіденційності та цілісності інформаційного повідомлення [9–12].

Обидва алгоритми ДСТУ 4145-2002 та ECNR засновані на математичній проблемі дискретного логарифмування в групі точок еліптичної кривої, а при детальному розгляданні можна побачити, що обидві схеми мають ще й майже однакову структуру. Тому алгоритм ECNR ідеально підходить для модифікації ДСТУ 4145-2002 та дана процедура потребувала мінімальних змін. Головною відмінністю стала заміна функції гешування на функцію маскування з використанням геш-токену, що робить процедуру підписання та верифікації оберненими та надає змогу відновлювати повідомлення з r -компоненти підпису.

Так, наприклад, загальні параметри цифрового підпису та спосіб їх формування є однаковими для обох алгоритмів.

Також незмінним буде обчислення ключової пари, тому даний етап повністю відтворюємо зі стандарту ДСТУ 4145-2002, а тому зобразимо їх на схемі (рис. 2).

Зауваження. У схемі не зазначено, але якщо поле задане поліноміальний базис, то необхідно зробити перевірку многочлена $f(t)$ на примітивність (перед перевіркою коефіцієнтів A та B)..

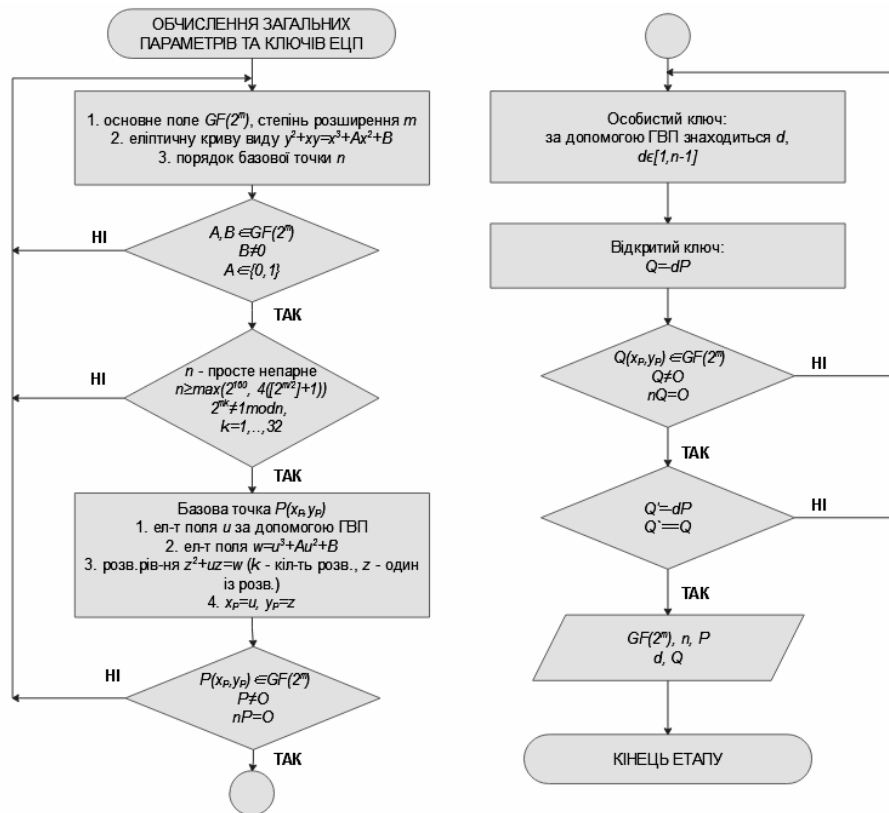


Рис. 2. Обчислення загальних параметрів ЕЦП та генерація ключової пари

По закінченню даного етапу маємо такі параметри: степiнь розширення m ; еліптична крива виду $y^3 + xy = x^3 + Ax^2 + B$; базова точка еліптичної кривої $P(x_P, Y_P)$; порядок базової точки n ; закритий ключ d ; відкритий ключ Q .

Етап формування підпису для модифікованого розглянемо детальніше. Зауважимо, що на відміну від звичайного ДСТУ 4145-2002 будемо використовувати не переведення параметрів до двійкового рядка, а їх перетворення на октети. Таким чином, будуть використовуватися такі функції: I2OSP — примітив перетворення цілих чисел в октетові рядки; OS2IP — примітив перетворення октетових рядків в цілі числа; EC2OSP — примітив перетворення еліптичної кривої в октетові рядки; OS2ECP — примітив перетворення октетових рядків в еліптичну криву.

Дані примітиви є обов'язковими складовими в бібліотеках для створення програмного забезпечення у сфері ЕЦП. Зручно одразу їх використовувати в описі наступних етапів, тому що вони будуть застосовані під час проектування програмного модуля. Повністю етап формування підпису зображений на рис. 3.

Отже, отриманий підпис має такі особливості, а саме в звичайному ДСТУ 4145 це (iH, M, D) ,

хоч перший параметр і не обов'язковий, а при модифікації з відновленням отримуємо (M_{clr}, r, s) , де M_{clr} буде використовуватися лише в одиничних випадках, а пара (r, s) і являє собою підпис D . Тобто, можна сказати, що при повідомленнях невеликої довжини, алгоритм з відновленням підпису буде ще й значно меншим за розміром порівняно з такими самими параметрами алгоритму без відновлення. Крім цього, після створення підпису запропонованим способом додається та забезпечується послуга конфіденційності даних, а також підвищується криптостійкість. Та необхідно вказати й недолік подібної модифікації — через додання математичних операцій (розщеплення повідомлення та його маскування) зменшується швидкість підписування.

Таким чином, відбувається модифікація ДСТУ 4145-2002 за допомогою алгоритму ECNR для надання йому функції відновлення повідомлення [9].

Це додає послугу конфіденційності, зменшує обсяг підпису, збільшує криптостійкість, проте сповільняє процедуру підпису/верифікації за однакових початкових параметрах.

Тепер можна перейти до верифікації підпису (рис. 4).

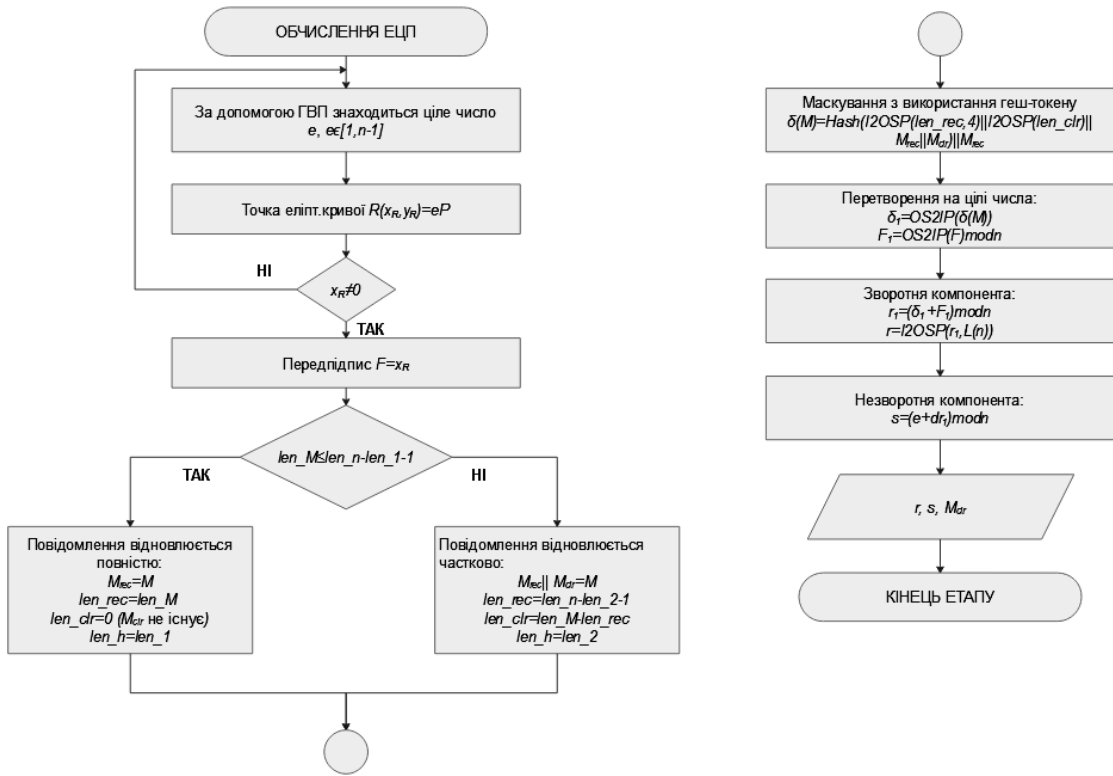


Рис. 3. Підписання повідомлення за модифікованим алгоритмом

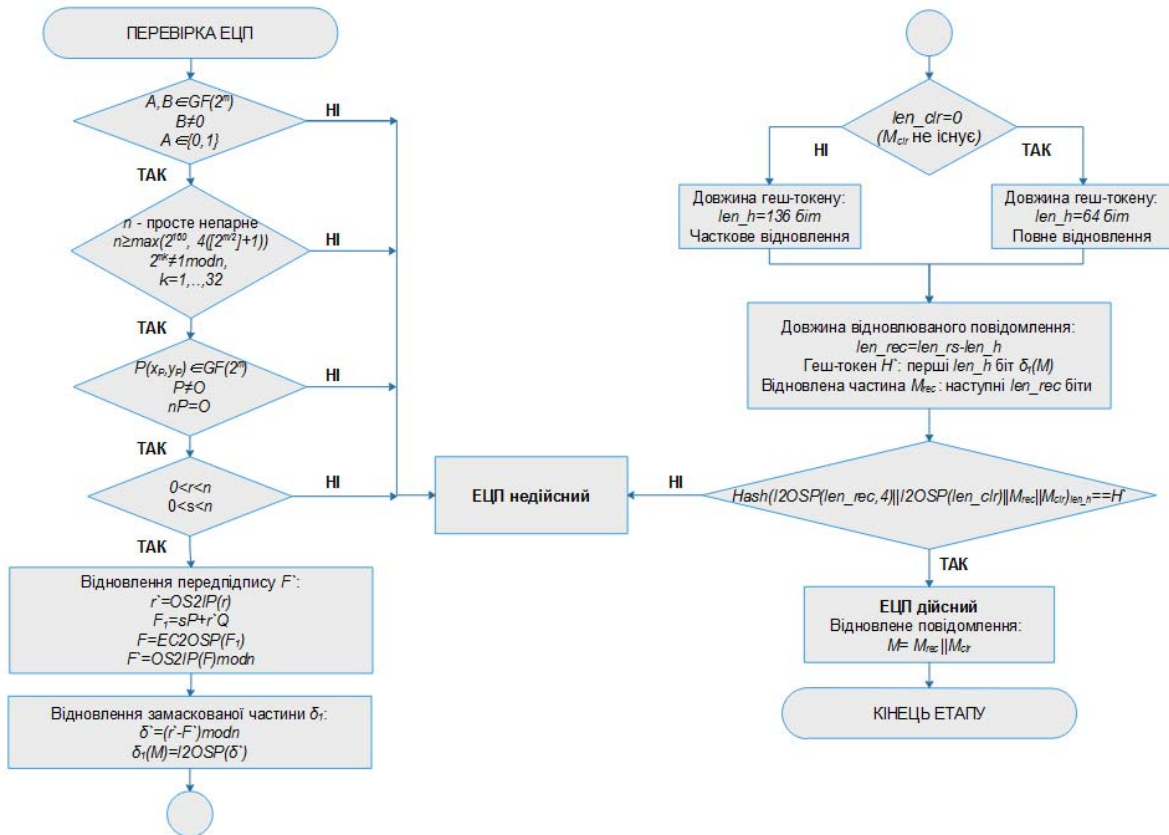


Рис. 4. Верифікація ЕЦП за модифікованим алгоритмом

Таким чином для підписання повідомлення необхідно лише обрати необхідний файл, який містить повідомлення, та параметри ключа (162, 256 або 512 біт). Програма автоматично згенерує ключі та підпише файл. У результаті користувач отримує файл *.key та *.sign з відкритим ключем та підписом відповідно. Для того, щоб перевірити ЕЦП, користувачеві необхідно мати файл з підписом та файл з відкритим ключем. Вони обидва є обов'язковими і в разі їх відсутності верифікації проводитися не буде. Якщо ж обидва файли обрані, то програма відтворює процедуру верифікації. У випадку вірності ЕЦП, користувачеві буде запропоновано відновити початкове повідомлення. При натисканні «Так» відкриється вікно, у якому міститиметься інформаційне повідомлення. Крім того було перевірено роботу програми у випадках зміни файлу *.sign або використанні іншого відкритого ключа. Як очіку-

валося, програма правильно реагує на подібні варіанти та сповіщає про недійсність ЕЦП.

Отже, було створено програмний модуль, який здатний підписувати повідомлення, формувати ключі та зберігати відкритий, перевіряти підпис, і в разі його вірності відновлювати інформаційне повідомлення. Це відбувається за алгоритмом ДСТУ 4145 з модифікаціями зі схеми ECNR, що заснована на проблемі дискретного логарифму в групі точок еліптичної кривої.

Оцінювання ефективності програмного модуля формування та верифікації ЕЦП на базі модифікованого алгоритму ДСТУ 4145-2002

Провівши необхідні операції для перетворення схеми ДСТУ 4145-2002 без відновлення повідомлення на схему з відновленням, можна провести їх аналіз та порівняти. Висновки та результати, отримані у попередньому підрозділі зафіксовано у табл. 2.

Таблиця 2

Порівняння звичайної та модифікованої схем ДСТУ 4145-2002

Параметри	ДСТУ 4145-2002	Модифікація ДСТУ 4145-2002
Забезпечення послуг	Цілісність	Цілісність Конфіденційність
Відновлення повідомлення	Ні	Так
Перетворення початкового повідомлення	Функція гешування	Функція маскування (+знаходження надлишковості)
Відкритий ключ, біт	163-768	112-768
Довжина підпису/Мінімальна довжина	Дайждест повідомлення + (r,s)/256 біт	(r,s) або (r,s,M _{clr})/162 біта
Час створення підпису, мс	1,24	1,98
Час перевірки підпису, мс	1,67	2,83

Отже, як можна побачити, разом з відновленням повідомлення модифікована версія ДСТУ 4145-2002 отримала змогу забезпечувати конфіденційність інформації, що передається. Також можна стверджувати, що у модифікованому варіанті можна використовувати відкритий ключ меншого розміру без загрози зменшення криптостійкості. Окрім цього, необхідно зазначити, що в разі повідомлення невеликої довжини (коли є можливість його повного відновлення), розмір підпису буде меншим і складатиметься всього з двох компонентів. Проте змінений алгоритм поступається звичайному у швидкості при однакових початкових параметрах. Та даний недолік не є критичним та звичайні користувачі майже не помітять зменшення швидкості підписання/верифікації.

Висновки

Отже, в статті була наведена повна характеристика модифікації Національного стандарту для

створення та перевірки ЕЦП – ДСТУ 4145-2002 та знайдені його переваги та недоліки.

З огляду на те, що схеми ДСТУ 4145 та ECNR є схожими, обрана модифікація не потребувала значних змін.

Головна відмінність — заміна функції гешування на функцію маскування з використання геш-токену, що робить процедуру підписання та верифікації оберненими та надає змогу відновлювати повідомлення з r -компоненти підпису.

Крім цього, було передбачено випадок підписання великого повідомлення, коли відновлюватися зможе тільки його частина.

Для цього було використано штучні збитковості повідомлення.

У результаті це додає схемі ДСТУ 4145-2002 послугу конфіденційності, зменшує обсяг підпису, збільшує криптостійкість, проте сповільняє процедуру підпису/верифікації за однакових початкових параметрах.

ЛІТЕРАТУРА

1. ISO/IEC 9796-3:2006: Information technology — Security techniques — Digital signature schemes giving message recovery — Part 3: Discrete logarithm based mechanisms, 2006. — URL:<http://www.iso.org>, doi.org/10.3403/30117202 (eng).
2. **Schneier В.** Applied cryptography: protocols, algorithms, and source code in C. — 2007, doi.org/10.1002/9781119183471 (eng).
3. **Горбенко Ю. І.** Аналіз властивостей та об'ластей застосування цифрових підписів стандарту ISO/IEC 9796 – 3:2006 / Ю.І. Горбенко, А. А. Шевчук // Прикладная радиоэлектроника. — 2009. — Т.8, №3. — С. 304–314.
4. **Шевчук А. А.** Особливості ЕЦП з відновленням повідомлення / А. А. Шевчук // Прикладная радиоэлектроника. — 2010. — Т.9, №3. — С. 489–492.
5. **Молдовян Д. Н.** Новый механизм формирования подписи в схемах ЭЦП, основанных на сложности дискретного логарифмирования и факторизации / Д. Н. Молдовян // Вопросы защиты информации. — 2005. — №4 (71). — С. 81–93.
6. **Алгулиев Р. М.** Исследование международных и национальных стандартов цифровой подписи на эллиптических кривых / Р. М. Алгулиев, Я. Н. Имамвердиев // Вопросы защиты информации. — 2005. — №2 (69). — С. 2–7.
7. **Полторак В. П.** Підвищення швидкодії процедури множення точки на число у алгоритмах електронного цифрового підпису на еліптичних кривих / В. П. Полторак, В. Б. Голков // Вісник НТУУ «КПІ»: Інформатика, управління та обчислювальна техніка. — К., 2013. — №57. — С. 155–163.
8. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка. — К. : Держстандарт України, 2003.
9. **Ільєнко А. В.** Сучасні шляхи удосконалення процедури формування та верифікації електронно-цифрового підпису / А. В. Ільєнко, Г. О. Миронова // Наукоємні технології. — № 1 (37). — 2018. — С. 61–66, doi.org/10.18372/2310-5461.37.12370 (ukr).
10. **Чунарьова А. В.** Практичні схеми реалізації алгоритмів електронного цифрового підпису / А. В. Чунарьова // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні: наук.-техн. зб. — К. : НТУУ «КПІ», 2013. — № 1 (25). — С. 81–88.
11. **Ільєнко А. В.** Сучасні методи гомоморфного шифрування інформаційних ресурсів / А. В. Ільєнко // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні: наук.; техн. зб. — К. : НТУУ «КПІ», 2015. — № 2 (30). — С. 52–57.
12. **Ільєнко А. В.** Оцінка ефективності оптимізованої криптосистеми Гентрі з умови забезпечення конфіденційності інформації / А. В. Ільєнко // Наукоємні технології. — № 1 (33). — 2017. — С. 41–45, doi.org/10.18372/2310-5461.33.11557(ukr).

Ільєнко А. В., Ільєнко С. С.

ПРОГРАМНИЙ МОДУЛЬ З ВИКОРИСТАННЯМ ПРОЦЕДУРИ ФОРМУВАННЯ ТА ВЕРИФІКАЦІЇ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПISУ

У статті проведено дослідження сучасних теоретичних основ класифікації алгоритмів формування та верифікації електронно-цифрового підпису. На основі проведеного аналізу та класифікації визначено, що в загальному за своєю структурою всі схеми електронно-цифрового підпису можна поділити на два великих класи: звичайні цифрові підписи (з доповненням) та електронні цифрові підписи з відновленням повідомлення. Проведені дослідження дозволили визначити, що схеми з відновленням повідомлення відрізняються від схем з доповненням тим, що вони не ґешують повністю повідомлення, а замість них користуються функціями маскування та знаходження збитковостей повідомлення. Також визначено, що за критерієм проблеми, що лежить в основі формування та верифікації електронно-цифрового підпису, найбільш криптостійкими будуть алгоритми, що ґрунтуються на проблемі дискретного логарифму в групі точок еліптичної кривої. Також описаний підхід щодо забезпечення цілісності та конфіденційності інформації на основі ЕЦП на базі еліптичних кривих з використанням стандарту ДСТУ 4145-2002 та схеми Німберга–Руппеля, що надає можливість відновлення повідомлення. Головною відмінністю стала заміна функції ґешування на функцію маскування з використанням ґеш-токену, що робить процедуру підписання та верифікації оберненими та надає змогу відновлювати повідомлення з r -компоненти підпису. Описано програмний модуль реалізації електронно-цифрового підпису за національним стандартом ДСТУ 4145-2002 з модифікацією на базі алгоритму ECNR, що заснована на проблемі дискретного логарифмування в групі точок еліптичної кривої та проведено оцінювання ефективності програмної реалізації з умови забезпечення конфіденційності та цілісності.

Ключові слова: електронно-цифровий підпис, верифікація, конфіденційність, еліптичні криві, ґеш-токен, дискретне логарифмування

Ильенко А. В., Ильенко С. С.

ПРОГРАММНЫЙ МОДУЛЬ С ИСПОЛЬЗОВАНИЕМ ПРОЦЕДУРЫ ФОРМИРОВАНИЯ И ВЕРИФИКАЦИИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

В статье проведено исследование современных теоретических основ классификации алгоритмов формирования и верификации электронно-цифровой подписи. На основе проведенного анализа и классификации определено, что, в общем, по своей структуре все схемы электронно-цифровой подписи можно разделить на два больших класса: обычные цифровые подписи (с дополнением) и электронные цифровые подписи с восстановлением сообщения. Проведённые исследования позволили определить, что схемы с восстановлением сообщения отличаются от схем с дополнением тем, что они не хешируют полностью сообщения, а вместо них используются функциями маскировки и нахождения избыточности сообщения. Также определено, что по критерию проблемы, лежащей в основе формирования и верификации электронно-цифровой подписи, наиболее криптостойкими будут алгоритмы, основанные на проблеме дискретного логарифма в группе точек эллиптической кривой. Также описан подход по обеспечению целостности и конфиденциальности информации на основе ЭЦП на базе эллиптических кривых с использованием стандарта DSTU 4145-2002 и схемы Нимберга-Руппеля, что даёт возможность восстановления сообщения. Главным отличием стала замена функции хеширования на функцию маскировки с использованием хэш-токена, что делает процедуру подписания и верификации обратными и даёт возможность восстанавливать сообщения с r-компоненты подписи. Описаны программный модуль реализации электронно-цифровой подписи с национальным стандартом DSTU 4145-2002 с модификацией на базе алгоритма ECNR, основанной на проблеме дискретного логарифмирования в группе точек эллиптической кривой и проведено оценивание эффективности программной реализации из условия обеспечения конфиденциальности и целостности.

Ключевые слова: электронно-цифровая подпись, верификация, конфиденциальность, эллиптические кривые, хэш-токен, дискретное логарифмирование

Ilyenko A. V, Ilyenko S. S

PROGRAM MODULE USING THE PROCEDURE FOR THE FORMATION AND VERIFICATION OF ELECTRONIC DIGITAL SIGNATURE

In the article the research of modern theoretical bases of classification of algorithms of formation and verification of electronic digital signature is carried out. Based on the analysis and classification, it has been determined that, in general, all electronic signature schemes can be divided into two large classes by their structure: ordinary digital signatures (with the addition) and electronic digital signatures with message recovery. The studies conducted have made it possible to determine that the message recovery schemes differ from the schemes with the addition that they do not completely hash the messages, but instead use the masking and redundancy features of the message. It is also determined that according to the criterion of the problem underlying the formation and verification of an electronic digital signature, algorithms based on the problem of a discrete logarithm in the group of points of an elliptic curve will be most crypto-resistant. Also described is the approach to ensuring the integrity and confidentiality of EDS-based information on the basis of elliptic curves using the standard DSTU 4145-2002 and the Niemberg-Ruppel scheme, which enables the recovery of the message. The main difference was the replacement of the hash function with the hash token function, which makes the signature and verification procedure reversed and allows you to retrieve messages from the signature r-component. The software module for implementing digital signatures with the national standard DSTU 4145-2002 with ECNR algorithm based on the problem of discrete logarithm in the group of points of the elliptic curve is described and the effectiveness of the software implementation from the condition of securing confidentiality and integrity has been evaluated.

Keywords: digital signature, verification, confidentiality, elliptical curves, hash token, discrete logarithm

Стаття надійшла до редакції 04.09.2018 р.
Прийнято до друку 18.09.2018 р.
Рецензент – д-р техн. наук, проф. Оксіюк О. Г.

УДК 003.26:004.056.55 DOI: 10.18372/2310-5461.39.13092

Р. С. Одарченко, канд. техн. наук, доц.
Національний авіаційний університет
orcid.org/0000-0002-7130-1375
e-mail: odarchenko.r.s@ukr.net

Є. О. Самойлик
Національний авіаційний університет
orcid.org/0000-0003-4090-8681
e-mail: sea110913@gmail.com

А. О. Абакумова, аспірант
Національний авіаційний університет
orcid.org/0000-0002-2844-096X
e-mail: nastia.abakumova@gmail.com

МЕТОД ПОБУДОВИ СЕМАНТИЧНОГО СЛОВНИКА У СКЛАДІ ДОСКОНАЛО СТІЙКОЇ КРИПТОСИСТЕМИ ЗАХИСТУ ТЕКСТОВОЇ ІНФОРМАЦІЇ

Вступ

Розвиток нових інформаційних технологій і впровадження комп'ютерних систем в усі сфери людської діяльності стали причиною різкого зростання зацікавленості широкого кола користувачів до проблеми інформаційного захисту. Провідна роль у забезпеченні інформаційної безпеки в інформаційно-телекомунікаційних системах відводиться криптографії, одним із головних завдань якої є: забезпечення конфіденційності, цілісності та автентичності даних, що передаються. Зважаючи на це в рамках сьогодення питання використання, удосконалення та розроблення досконало стійких криптографічних систем (криптосистем), які забезпечують різноманітний рівень криптостійкості, є досить актуальним.

Аналіз останніх досліджень і публікацій

На сьогодні багатьма вченими розроблено різноманітні практично стійкі криптографічні системи, що знайшли застосування для вирішення широкого спектру прикладних задач, де необхідно забезпечити надійний захист від порушень конфіденційності інформації, що передається відкритими каналами зв'язку [1–5]. Тим не менш, ці криптосистеми не гарантують формальну, теоретично доведену неможливість їхнього злому [4–7]. Згідно з цим існує проблема недовіри до надійності цих систем в задачах передавання інформації, що характеризуються високими рівнями секретності.

Водночас численні дослідження багатьох авторів указують на відносно невеликі значення відстані єдиності при шифруванні повідомлень, складених із символів алфавіту будь-якої із природних мов [8; 9]. Відтак це призводить до необ-

хідності частоті зміни ключової інформації, що є проблемою для багатьох застосувань.

Постановка завдання

З урахуванням вище зазначеного можна стверджувати, що створення нових методів побудови досконало стійких криптосистем, які забезпечують більш великі значення відстані єдиності або, взагалі, забезпечують можливість шифрування скільки завгодно великих обсягів текстових, зокрема голосових, повідомлень незалежно від значень відстані єдиності являє актуальне завдання.

За таких умов для вирішення даного завдання в першу чергу необхідно розробити метод побудови семантичного тезаурусу, придатного для використання у складі досконало стійкої криптосистеми захисту текстової інформації. А саме: увести показники семантичних зв'язків між смисловими конструкціями мови відображення прикладної області, насамперед показники правдоподібності, і на цій основі здійснити синтез структури тезаурусу.

Структура тезаурусу смислових образів

Неодмінним елементом будь-якої досконало стійкої криптосистеми, що заснована на застосуванні певним чином побудованої лексикографічної системи, є тезаурус бази захисту інформації у прикладній системі, де ця криптосистема використовується. У даному випадку тезаурус — це семантичний словник, структура якого відображає структуру семантичних зв'язків між смисловими конструкціями мови відображення прикладної області його застосування. У досконало стійких криптосистемах структура семантичних зв'язків між елементами тезаурусу має бути відображена на формальному рівні.

В першу чергу визначимо на формальному рівні структуру тезаурусу смислових образів мови відображення області розумової діяльності суб'єкта. Будемо вважати, що тезаурус будь-якої мови взагалі TZ_M або будь-якого суб'єкта окремо TZ_S має ієрархічну прошаркову (рос. — слоистую) структуру і за ступенем абстрагування відображення смислових образів розподіляються на i рівнів, де $i = 1, 2, \dots, I$ — кількість рівнів абстрагування відображення смислових образів, якими оперує колективний інтелект носіїв цієї

мови взагалі або індивідуальний інтелект суб'єкту розумової діяльності окремо, а I_{\max} — максимальна кількість рівнів абстрагування відображення SO , що є доступною інтелекту. Так що, простір смислових образів, доступний суб'єкту (або групі суб'єктів), тобто його тезаурус TZ_S , є дискретним, кінцево-мірним, який щодо рівнів абстрагування представлення образів має прошаркову коренево-подібну структуру (рис. 1).

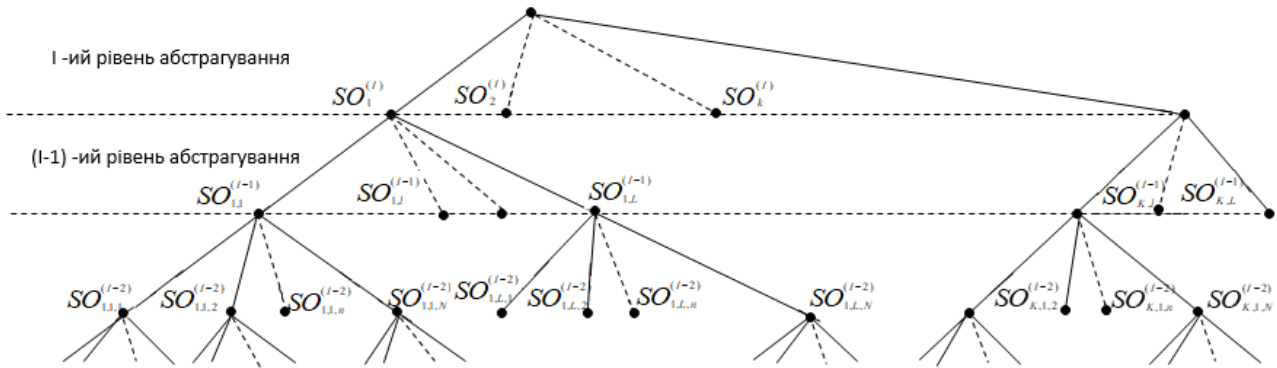


Рис. 1. Прошаркова коренево-подібна структура простору смислових образів, що складають тезаурус

За таким визначенням будь-який тезаурус TZ (зокрема, TZ_M або TZ_S) складається із сукупності підтезаурусів семантичних одиниць усіх доступних для розуміння рівнів абстрагування $TZ^{(i)}$, де $i = 1, 2, \dots, I$. При цьому підтезауруси у складі TZ розташовані прошарками у вигляді гілкоподібної кореневої системи, що розростаються зверху вниз. В основі кореня лежить семантичний образ $SO^{(I+1)}$ з максимальним $(I+1)$ -м рівнем абстрагування відображення SO , що є доступним інтелекту у конкретній області розумової діяльності.

У загальному випадку структуру тезаурусу TZ можливо представити у вигляді рекурентної коренево-подібної схеми як

$$TZ \in \{ TZ^{(I)}_k \},$$

$$\text{де } TZ^{(I)}_k \in \{ TZ^{(I-1)}_{k,l} \}, \text{ де } TZ^{(I-1)}_{k,l} \in \{ TZ^{(I-2)}_{k,l,n} \},$$

$$\text{де } TZ^{(I-2)}_{k,l,n,\dots,p} \in \{ SO^{(1)}_{k,l,n,\dots,j} \}. \quad (1)$$

У виразі (1) прийняті такі позначення:

$TZ^{(I)}_k$ — тезаурус I -го рівня абстрагування представлення SO ; $I \in \{1, 2, \dots, i, \dots, I_{\max}\}$ — кількість рівнів абстрагування відображення SO , що доступна інтелектові; $k \in \{1, 2, \dots, K\}$ — порядковий номер елемента $TZ^{(I)}_k$ у множині тезаурусів, що у сукупності визначають простір смислових образів I -го рівня абстрагування; K — кількість тезаурусів I -го рівня абстрагування відображення SO , що входять до складу TZ ;

$TZ^{(I-1)}_{k,l}$ — тезаурус $(I-1)$ -го рівня абстрагування представлення SO , що конкретизує смислові образи $TZ^{(I)}_k$, де $l \in \{1, 2, \dots, L\}$ — порядковий номер тезаурусу $(I-1)$ -го рівня абстрагування у множині тезаурусів, які у сукупності визначають простір смислових образів $(I-1)$ -го рівню абстрагування у рамках тезаурусу $TZ^{(I)}_k$; L — кількість тезаурусів $(I-1)$ -го рівня абстрагування відображення SO , що входять до складу $TZ^{(I)}_k$; $TZ^{(I-2)}_{k,l,n}$ — тезаурус $(I-2)$ -го рівня абстрагування представлення SO , що конкретизує смислові образи $TZ^{(I-1)}_{k,l}$, де $n \in \{1, 2, \dots, N\}$ — порядковий номер тезаурусу $(I-2)$ -го рівня абстрагування у тезаурусі $TZ^{(I-1)}_{k,l}$; N — кількість тезаурусів $(I-2)$ -го рівня абстрагування відображення SO , що входять до складу $TZ^{(I-1)}_{k,l}$; $TZ^{(2)}_{k,l,n,\dots,p}$ — тезаурус другого рівня абстрагування представлення SO , що конкретизує смислові образи $TZ^{(3)}_{k,l,n,\dots,s}$, де $p \in \{1, 2, \dots, P\}$ — порядковий номер тезаурусу другого рівня абстрагування у складі тезаурусу третього рівня абстрагування $TZ^{(3)}_{k,l,n,\dots,s}$, де $s \in \{1, 2, \dots, S\}$ — порядковий номер тезаурусу третього рівня абстрагування; P — кількість тезаурусів другого рівня абстрагування, що входять до складу $TZ^{(3)}_{k,l,n,\dots,s}$; S — кількість тезаурусів третього рівня абстрагування, що входять до складу відповідного тезаурусу четвертого рівня абстрактності і т. д. уздовж ланцюгу тезаурусів із зростанням значення індексу i ; $SO^{(1)}_{k,l,n,\dots,j}$ — семантичний словник, що відображає тезаурус $TZ^{(2)}_{k,l,n,\dots,p}$; J — кількість слів у тезаурусі $TZ^{(2)}_{k,l,n,\dots,p}$.

Отже, структура тезаурусу TZ представляється у вигляді розгалуженого кореня підтезаурусів $TZ^{(i)}$, де $i \in \{1, 2, \dots, I_{\max}\}$.

Якщо розглядати структуру тезаурусів мови відображення будь-якої прикладної області відповідно до розтину за рівнями абстрагування відображення смислових образів (рис. 1), то у загальному випадку доцільно задати таку ієрархію її семантичних одиниць:

$$\begin{aligned} & \text{прикладна область (напрямок знань)/} \\ & \text{тема/сценарій/ситуація/} \\ & \text{фраза/слово/символ алфавіту/} \\ & \text{код символу алфавіту} \end{aligned} \quad (2)$$

Зокрема, у багатьох сферах прикладних застосувань, які у подальшому назвемо областями активності, доцільно призначити таку ієрархію смислових одиниць, що відображають логічно завершені думки певного рівня абстрагування, де убунання ступеню абстрагування прийнято зліва направо:

$$\text{сценарій/ситуація/фраза/слово} \quad (3)$$

У цьому випадку, у виразі (1) $I = 4$, тобто будемо мати чотирьох ступеневу ієрархічну структуру у вигляді розгалуженого кореня тезаурусів з різним рівнем абстрагування представлення смислових образів. Значення параметрів K, L, M, N, S та P у виразі (1) необхідно визначати, виходячи із феноменології заданої області активності.

Під сценарієм (або темою у рамках визначеної області активності) розуміється упорядкована щодо смислу послідовність ситуацій, під ситуацією — упорядкована щодо смислу послідовність фраз, під фразою — упорядкована щодо смислу послідовність слів. А під словом (письмової мови) — упорядкована щодо смислу послідовність символів обраного алфавіту.

Область активності — це область розумової діяльності, яка відображається заданим простором смислових образів (які, у свою чергу, відображаються відповідним простором мовних одиниць усіх рівнів абстрагування у рамках обраної мови). Бажано, щоб цей простір повною мірою відображав визначену область активності. Однак створення такого простору через його велику розмірність потребує занадто великих ресурсних витрат. На практиці область активності обмежується визначеною сферою прикладних застосувань.

Формальне відображення семантики текстової інформації

Відобразимо зразок текстової послідовності на рівні семантичних одиниць i -го рівню абстрагування так:

$$SO^{(i)}_{k(1)}, SO^{(i)}_{k(2)}, \dots, SO^{(i)}_{k(n)}, \dots, SO^{(i)}_{k(Ni)}, \quad (4)$$

де k — порядковий номер семантичної одиниці $TZ^{(i)}$ у тезаурусі $TZ^{(i+1)}$, тобто $k = 1, 2, \dots, K$.

Значення індексу k генеруються інтелектом суб'єкта підчас формування смислового образу тексту і залежить від порядкового номеру n семантичної одиниці у тексті, $n = 1, 2, \dots, Ni$. Параметр Ni визначає розмірність зразка текстової послідовності.

Зрозуміло, що запис (4) буде справедливим, якщо для будь-якого елемента зразка $SO^{(i)}$ знайдеться відповідний тезаурус $TZ^{(i)}$ у тезаурусі $TZ^{(i+1)}$, тобто якщо $SO^{(i)} \equiv TZ^{(i)}$, де символ \equiv означає відношення смислової ідентичності.

У свою чергу, кожен елемент випадкової послідовності (4) може бути представлений послідовністю більш конкретного змісту — на рівні семантичних одиниць $(i-1)$ -го рівня абстрагування:

$$SO^{(i)}_k \rightarrow SO^{(i-1)}_{k, l(1)}, SO^{(i-1)}_{k, l(2)}, \dots, SO^{(i-1)}_{k, l(Ni)}, \quad (5)$$

а кожен елемент випадкової послідовності (5) має бути представлений послідовністю ще більш конкретного змісту — на рівні семантичних одиниць $(i-2)$ -го рівня абстрагування:

$$SO^{(i-1)}_{k, l} \rightarrow SO^{(i-2)}_{k, l, m(1)}, SO^{(i-2)}_{k, l, m(2)}, \dots, SO^{(i-2)}_{k, l, m(Nm)}. \quad (6)$$

Отже, найбільш конкретний рівень представлення смислу текстових повідомлень здійснюється тоді, коли кожен елемент другого рівню абстрагування буде являти собою послідовність слів, тобто послідовність семантичних елементів першого рівню абстрагування:

$$SO^{(2)}_{k, l, n, \dots, p} \rightarrow SO^{(1)}_{k, l, n, \dots, j(1)}, SO^{(1)}_{k, l, n, \dots, j(2)}, \dots, SO^{(1)}_{k, l, n, \dots, j(Nj)}. \quad (7)$$

Надані вище семантичні відношення можливо визначити між смисловими одиницями, що відображають логічно завершені думки певного рівня абстрагування, зокрема на рівні ситуацій, на рівні фраз або на рівні слів.

Смислові відношення між семантичними одиницями

Метод побудови досконало стійкої крипто-системи базується на використанні лексикографічних ефектів, що пов'язані з такою властивістю текстової (голосової чи письмової) інформації як можливість її неоднозначного сприйняття суб'єктом. Механізми такої крипто-системи мають забезпечити створення умов, за яких зашифровані зразки текстової інформації сприймаються крипто-аналітиком як правдоподібні з невідзначеною ймовірністю їхньої появи у шифрограмі, що не дає йому змогу відрізнити вихідні відкриті зразки повідомлень, що були зашифровані, від інших правдоподібних відображень цих повідомлень, що утворились у результаті шифрування. Отже, щоб побудувати будь-яку крипто-семантичну систему захисту, необхідно надати формальні визначення таким смисловим відно-

шенням між семантичними одиницями як *смілова ідентичність*, *смілова відмінність*, сумнівна *смілова ідентичність* (або *правдоподібність*), сумнівна *смілова відмінність* (або *фальшиво-подібність*).

Побудована вище модель розуміння мови та створений на основі цієї моделі формалізм структури тезаурусів, яким оперує суб'єкт під час розумової діяльності, дозволяють визначити вищезазначені показники наступним чином:

- *Обмеження щодо області визначення смислових відношень*

Смислові відношення у даній роботі визначаються за таких умов:

1) семантичні одиниці, між котрими визначаються смислові відношення, мають належати одному і тому самому тезаурусу мови, що відображає певним чином обрану область активності;

2) смислові відношення визначаються між семантичними одиницями будь-якого, але однакового рівню абстрагування

- *Відношення смислової ідентичності*

Якщо серед множини семантичних одиниць, що представляють тезаурус TZ , існує кілька одиниць, що є ідентичними за сутністю змісту, то ці одиниці щодо смислу знаходяться у відношенні смислової ідентичності (синоніми). Тобто, будь-які дві семантичні одиниці будь-якого, але однакового рівня абстрагування $TZ_a^{(i)_k}$ та $TZ_b^{(i)_k}$ із множини $\{TZ^{(i)_k}\} \rightarrow TZ$ знаходяться у відношенні смислової ідентичності

$$TZ_a^{(i)_k} \equiv TZ_b^{(i)_k}, \quad (8)$$

якщо є ідентичними за сутністю змісту.

Позначка \rightarrow означає приналежність будь-якого тезаурусу $TZ^{(i)_k}$ із множини тезаурусів i -го рівня абстрагування до тезаурусу обраної мови TZ , а у виразі (8) позначка \equiv означає відношення смислової ідентичності.

Зрозуміло, якщо

$$TZ_a^{(i)_k} \equiv TZ_b^{(i)_k}, \text{ а } TZ_b^{(i)_k} \equiv TZ_c^{(i)_k}, \text{ то } TZ_a^{(i)_k} \equiv TZ_c^{(i)_k}. \quad (9)$$

Зрозуміло також, що

$SO^{(i)_k} \equiv TZ^{(i)_k}$ для будь-яких значень i та k (10) тобто, будь-який елемент будь-якого тезаурусу, що входить до складу тезаурусу будь-якої мови будь-якої області активності відображає відповідний смисловий образ

- *Відношення смислової відмінності*

Якщо серед множини семантичних одиниць, що представляють тезаурус TZ , існує кілька одиниць, що не є ідентичними за сутністю змісту, то ці одиниці щодо смислу знаходяться у відношенні смислової відмінності. Тобто, семантична одиниця i -го рівню абстрактності $TZ_a^{(i)_k}$ із множини $\{TZ^{(i)_k}\} \rightarrow TZ$ та семантична одиниця

$TZ_b^{(i)_l}$ із множини $\{TZ^{(i)_k}\} \rightarrow TZ$ знаходяться у відношенні смислової відмінності

$$TZ_a^{(i)_k} \triangleq TZ_b^{(i)_l}, \quad (11)$$

якщо не є ідентичними за сутністю змісту. Позначка \triangleq означає смислову відмінність.

Зрозуміло, що різні гілки будь-якого, але одного рівня абстрагування представлення SO у корені, що представляє структуру TZ (рис. 1), знаходяться у стані смислової відмінності.

- *Відношення правдоподібності*

Якщо порівнювальні смислові образи сприймаються суб'єктом як ідентичні щодо смислу, але у нього існують небезпідставні сумніви щодо істинності такого сприймання, то у цьому випадку доцільно визначити смислове відношення як правдоподібне. Тобто, якщо в якості позначки відношення правдоподібності обрати символ \wedge та врахувати, що $SO^{(i)_k} \equiv TZ^{(i)_k}$ для будь-яких значень i та k , то будь-які дві семантичні одиниці будь-якого, але однакового рівня абстрагування $TZ_a^{(i)_k}$ та $TZ_b^{(i)_k}$ із множини $\{TZ^{(i)_k}\} \rightarrow TZ$ знаходяться у відношенні смислової правдоподібності

$$TZ_a^{(i)_k} \wedge TZ_b^{(i)_k}, \quad (12)$$

якщо ймовірність того, що $TZ_a^{(i)_k} \equiv TZ_b^{(i)_k}$ є меншою, ніж 1.

Відносно семантичних одиниць I -го (найвищого у даній мові даної області активності) рівня абстрагування буде справедливим таке твердження:

$$SO^{(i)_1} \wedge SO^{(i)_2} \wedge \dots \wedge SO^{(i)_k} \wedge \dots \wedge SO^{(i)_K},$$

$$\text{якщо } \{TZ^{(i)_k}\} \rightarrow TZ, \quad (13)$$

за умови $SO^{(i)_k} \equiv TZ^{(i)_k}$, для будь-яких значень I та K (14)

У виразі (13) позначка \rightarrow означає приналежність будь-якого тезаурусу $TZ^{(i)_k}$ із множини тезаурусів I -го рівня абстрагування до тезаурусу обраної мови TZ , а у виразі (14) позначка \equiv означає відношення смислової ідентичності.

- *Відношення фальшиво-подібності*

Якщо порівнювальні смислові образи сприймаються суб'єктом як відмінні щодо смислу, але у нього існують небезпідставні сумніви щодо істинності такого сприймання, то у цьому випадку доцільно визначити смислове відношення як фальшиво-подібне. Тобто, якщо в якості позначки відношення фальшиво-подібності обрати символ ∇ та врахувати, що $SO^{(i)_k} \equiv TZ^{(i)_k}$ для будь-яких значень i та k , то будь-які дві семантичні одиниці будь-якого, але однакового рівня абстрагування $TZ_a^{(i)_k}$ із множини $\{TZ^{(i)_k}\} \rightarrow TZ$ та $TZ_b^{(i)_l}$ із множини $\{TZ^{(i)_l}\} \rightarrow TZ$ знаходяться у відношенні смислової фальшиво-подібності

$$TZ_a^{(i)_k} \nabla TZ_b^{(i)_l}, \quad (15)$$

якщо ймовірність того, що $TZ_a^{(i)_k} \triangleq TZ_b^{(i)_l}$ є меншою, ніж 1.

Структура тезаурусу бази захисту

Структура тезаурусу прикладної системи TZ_{PS} відображена на рис. 1 і є рекурентною схемою (1). Як бачимо, тезаурус TZ_{PS} містить усі можливі семантичні образи на всіх заданих рівнях абстрагування, що в сукупності складають мову відображення цієї прикладної області. Оскільки будь-який лексикографічний метод захисту текстової інформації базується на випадковій заміні істинного смислового образу повідомлення на інший правдоподібний смисловий образ, то користування тезаурусом TZ_{PS} для здійснення таких заміन не уявляється можливим. Лексикографічна система у складі досконало стійкої криптосистеми має спиратися на тезаурус, усі елементи котрого пов'язані між собою відношенням правдоподібності, коли будь-яка заміна одного семантичного образу на інший не порушує відношення правдоподібності.

Такий тезаурус назвемо тезаурусом бази захисту інформації TZ_{BZ} у прикладній системі, що відображається тезаурусом TZ_{PS} (рис. 2).

Для захисту смислу текстових повідомлень пропонується такий методологічний підхід, що заснований на використанні відношень смислової правдоподібності. Для того, щоб криптоаналітик ні за яких умов не мав можливостей скласти будь-яке уявлення щодо істинності смислу перехоплених текстових повідомлень, необхідно і достатньо замінити смисл SO , що входять до складу вихідних відкритих текстових повідомлень, на правдоподібні їхні відображення, що беруться із тезаурусу бази захисту інформації TZ_{BZ} обраної області активності з тезаурусом TZ_{PS} .

Для здійснення такої заміни в автоматичному режимі необхідно мати формальні позначення місць розташування відображень SO у структурі TZ_{BZ} , тобто необхідно локалізувати мовні одиниці у структурі тезаурусу TZ_{BZ} .

Аналізуючи структуру TZ_{BZ} на рис. 2, можливо формалізувати цю структуру таким чином, щоб параметри локалізації були представлені в явному вигляді, наприклад:

$$SO^{(i)}_k \in \left\{ \begin{array}{l} SO^{(i-1)}_{k,1,1}; SO^{(i-1)}_{k,1,2}; \dots; SO^{(i-1)}_{k,1,n}; \dots; SO^{(i-1)}_{k,1,N(l=1)} \\ SO^{(i-1)}_{k,2,1}; SO^{(i-1)}_{k,2,2}; \dots; SO^{(i-1)}_{k,2,n}; \dots; SO^{(i-1)}_{k,2,N(l=2)} \\ \dots \\ \dots \\ SO^{(i-1)}_{k,l,1}; SO^{(i-1)}_{k,l,2}; \dots; SO^{(i-1)}_{k,l,n}; \dots; SO^{(i-1)}_{k,l,N(l)} \\ \dots \\ \dots \\ SO^{(i-1)}_{k,L,1}; SO^{(i-1)}_{k,L,2}; \dots; SO^{(i-1)}_{k,L,n}; \dots; SO^{(i-1)}_{k,L,N(L)} \end{array} \right. \quad (16)$$

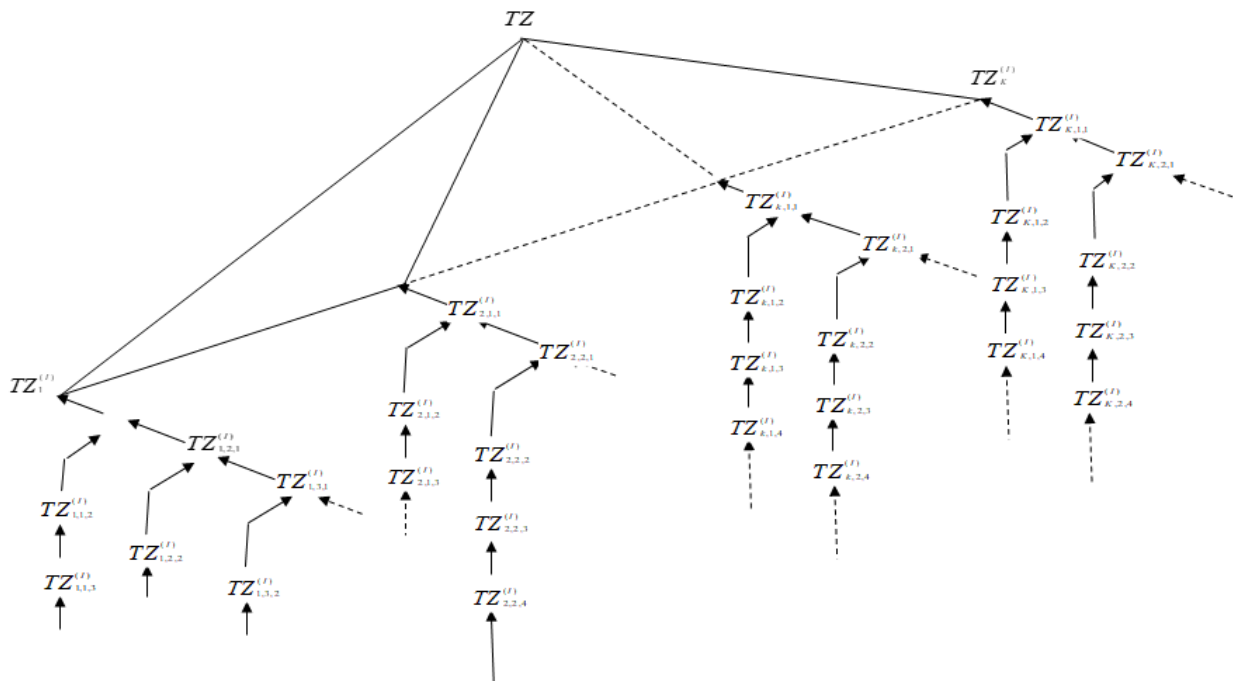


Рис. 2. Структура тезаурусу бази захисту текстової інформації TZ_{BZ} у прикладній системі, що відображається тезаурусом TZ_{PS}

Поточні значення нижніх індексів у позначеннях семантичних одиниць у виразі (16) однозначно визначають місця розташування цих семантичних одиниць у структурі TZ_{BZ} .

Отже, будь-яка семантична одиниця $TZ_k^{(l)}$ із множини семантичних одиниць l -го рівню абстрагування, що входять до складу тезаурусу мови обраної області активності TZ_{PS} , під час криптоаналізу сприймається суб'єктом як можливий кандидат на смислову ідентичність із вихідною семантичною одиницею відкритого тексту $TZ_l^{(l)}$.

Щодо смислової правдоподібності між семантичними одиницями $(l-1)$ -го рівня абстрагування за аналогією буде справедливим наступне твердження:

$$SO_{k,1}^{(l-1)} \wedge SO_{k,2}^{(l-1)} \wedge \dots \wedge SO_{k,l}^{(l-1)} \wedge \dots \wedge SO_{k,L}^{(l-1)},$$

$$\text{якщо } \{TZ_{k,l}^{(l-1)}\} \rightarrow TZ_k^{(l)}, \quad (17)$$

за умови $SO_k^{(l-1)} \equiv TZ_k^{(l-1)}$, для будь-яких значень $(l-1)$, k та l . (18)

Аналогічно за рекурентною схемою можна записати вирази щодо відношень між смисловими одиницями для будь-яких інших більш деталізованих рівнів абстрагування представлення смислових образів. Із виразів (16)–(18) випливає, що семантичні одиниці, що входять до складу будь-якої однієї гілки у структурі тезаурусу TZ_{BZ} , знаходяться між собою у відношенні семантичної правдоподібності.

Висновки

Таким чином розроблено метод побудови семантичного словника, який за рахунок уведення в прикладну лексикографічну систему показників семантичних зв'язків між смисловими конструкціями мови відображення прикладної області застосування задає семантичну структуру словника прикладної області, що дає можливість використати його у складі досконало стійкої криптосистеми захисту текстової інформації.

Водночас показано, що для побудови будь-якої досконало стійкої лексикографічної криптосистеми системи захисту текстової інформації необхідно мати формальні визначення таких смислових відношень між семантичними одиницями як смислова ідентичність, смислова відмінність, правдоподібність, фальшиво-подібність.

Нарешті, на закінчення запропоновано методологічний підхід до захисту смислу текстових повідомлень, що заснований на використанні відношень смислової правдоподібності.

Перспективи подальших досліджень

Перспективи дослідження полягають у технічній реалізації крипто-семантичного метода захисту текстових даних, що буде заснований на використанні прикладного тезаурусу смислових образів, який дозволить забезпечити режим досконалої стійкості у рамках конкретно визначених прикладних систем.

Технічне рішення дасть можливість забезпечити досконалу стійкість захисту для умов, коли обсяги зашифрованих семантичних одиниць обраної мови представлення смислових образів не обмежуються відстанню єдиності та довжиною ключової інформації, що сприяє усуненню проблеми розповсюдження ключів шифрів.

ЛІТЕРАТУРА

1. **Смарт Н.** Криптографія / С. А. Кулешова (пер. с англ.). — М. : Техносфера, 2006. — 519 с.
2. **Мессі Дж. Л.** Введение в современную криптологию. Малый тематический выпуск «Защита информации». ТИИЭР, 1988, № 5.
3. Encyclopedia of cryptography and security / ed.-in-chief Henk C. A. van Tilborg. New York : Springer, cop. 2005. — X 684.
4. **Тилборг Ван Х. К. А.** Основы криптологии. Профессиональное руководство и интерактивный учебник. — М. : Мир, 2006. — 471 с.
5. **Грездов Г. Г.** Современные методы защиты информации; под ред. чл.-корр. НАН Украины В. В. Васильева. — К., 2002. — 32с. (Препринт / НАН Украины. Отделение гибридных моделирующих и управляющих систем в энергетике ИПМЭ; №01/2001).
6. **Соломаа А.** Криптография с открытым ключом: пер. с англ. — М. : Мир, 1995. — 318 с.
7. **Щербаков Л. Ю., Домашев А. В.** Прикладная криптография. Использование и синтез криптографических интерфейсов. — М. : Издательско-торговый дом «Русская редакция», 2003. — 416 с.
8. **Заєць В. В., Чуприн В. М.** Визначення стійкості криптостеганографічних методів захисту інформації // Збірник наукових праць Інституту проблем моделювання в енергетиці ім. Г. Є. Пухова. — Київ: ІПМЕ ім. Г.Є.Пухова НАН України, 2007. — № 44. — С. 9–19.
9. **Заєць В. В., Чуприн В. М.** Розрахунок ефективності криптосемантичної системи захисту інформації // Збірник наукових праць «Управління розвитком». — Харків : ХНЕУ, 2008. — №6 — С. 68–70.

Одарченко Р. С., Самойлик Є. О., Абакумова А. О.

МЕТОД ПОБУДОВИ СЕМАНТИЧНОГО СЛОВНИКА У СКЛАДІ ДОСКОНАЛО СТІЙКОЇ КРИПТОСИСТЕМИ ЗАХИСТУ ТЕКСТОВОЇ ІНФОРМАЦІЇ

У статті розроблено формальну структуру тезаурусу смислових образів для будь-якої мови взагалі або для будь-якого суб'єкту окремо. Показано, що у багатьох прикладних сферах доцільно призначити наступну ієрархію смислових одиниць, що відображають логічно завершені думки певного рівня абстрагування, де убуння ступеню абстрагування прийнято зліва направо: сценарій/ситуація/фраза/слово. Одночасно зазначалося, що для побудови будь-якої досконало стійкої лексикографічної крипто-семантичної системи захисту текстової інформації необхідно мати формальні визначення таких смислових відношень між семантичними одиницями як смислова ідентичність, смислова відмінність, сумнівна смислова ідентичність (або правдоподібність), сумнівна смислова відмінність (або фальшиво-подібність). Відповідно з цим, запропоновано методологічний підхід до захисту смислу текстових повідомлень, що заснований на використанні відношень смислової правдоподібності. На закінчення представлено формальні відображення семантики текстової інформації, що дозволяє автоматизувати процес створення семантичних словників.

Ключові слова: криптосистема; захист; тезаурус; семантичний словник; текстова інформація.

Odarchenko R. S., Samoilyk Ye. O., Abakumova A. O.

METHOD OF CONSTRUCTING A SEMANTIC DICTIONARY CONSISTING OF A PERFECTLY STABLE CRYPTOSYSTEM OF TEXT INFORMATION PROTECTION

The article describes the formal structure of semantic images thesaurus for any language in general or for any subject separately. It is shown that in many applied spheres it is advisable to assign the following hierarchy of semantic units that reflect logically completed thoughts of a certain level of abstraction, where the degree of abstraction is reduced from left to right: script/situation/phrase word. At the same time, it was noted that for the construction of any perfectly stable lexicographic crypto-semantic protection system of text information it is necessary to have formal definitions of such semantic relations between semantic units as semantic identity, semantic difference, questionable semantic identity (or plausibility), questionable semantic difference (or false similarity). Accordingly, a methodological approach is proposed to protect the meaning of text messages, which is based on the use of semantic plausibility relations. In conclusion, the formal representation of textual information semantics is presented, which allows automating the process of creating semantic dictionaries.

Keywords: cryptosystem; protection; thesaurus; semantic dictionary; text information.

Одарченко Р. С., Самойлик Е. О., Абакумова А. А.

МЕТОД ПОСТРОЕНИЯ СЕМАНТИЧЕСКОГО СЛОВАРЯ В СОСТАВЕ СОВЕРШЕННО УСТОЙЧИВОЙ КРИПТОСИСТЕМЫ ЗАЩИТЫ ТЕКСТОВОЙ ИНФОРМАЦИИ

В статье разработано формальную структуру тезауруса смысловых образов для любого языка вообще или для любого субъекта в отдельности. Показано, что во многих прикладных сферах целесообразно назначить следующую иерархию смысловых единиц, отражающих логически завершённые мысли определённого уровня абстрагирования, где убывания степени абстрагирования принято слева направо: сценарий/ситуация/фраза/слово. Одновременно отмечалось, что для построения любой совершенно устойчивой лексикографической крипто-семантической системы защиты текстовой информации необходимо иметь формальные определения таких смысловых отношений между семантическими единицами как смысловая идентичность, смысловое отличие, сомнительная смысловая идентичность (или правдоподобие), сомнительное смысловое отличие (или фальшиво-сходство). Согласно с этим, предложено методологический подход к защите смысла текстовых сообщений, основанный на использовании отношений смыслового правдоподобия. В заключение представлены формальные отображения семантики текстовой информации, что позволяет автоматизировать процесс создания семантических словарей.

Ключевые слова: криптосистема; защита; тезаурус; семантический словарь; текстовая информация.

Стаття надійшла до редакції 26.06.2018 р.

Прийнято до друку 28.08.2018 р.

Рецензент – д-р техн. наук, проф. Коначович Г. Ф.

Malikov E., Doctoral candidate,
National Aviation Academy, Az 1045, Baku, Bina 25,
orcid.org/0000-0001-5169-4813
e-mail: emin757-200@rambler.ru

INFLUENCE OF "AT WINGLETS" WINGTIP TYPE ON THE AERODYNAMIC CHARACTERISTICS OF WINGS

Introduction

Inductive drag of the wing is associated with the finiteness of the wing span and arises from the flow of air through the end sections, perpendicular to the main one - in front of the incoming flow. Being inversely proportional to the wing span, it decreases with increasing span. When designing the constructors in every way try to reduce the drag of the aircraft, which leads to an increase in the aerodynamic quality of the device. In this case, a decrease in the inductive drag of the wing is also one of the first to occur in thought. This, at least, can be achieved by increasing the wing span, or by preventing the flow of air through the end sections of the wing. Thus, the idea of using wing tips (winglets) arose. The wing tips have been used in aviation since the seventies of the last century, and bring tremendous fuel savings for the year. However, theoretical studies in this field began in 2012 in Azerbaijan in the National Aviation Academy [1–3]. In the mentioned studies, the influence of vertical wing tips (VWT) on the inductive drag is investigated. Various mathematical models have been constructed that reflect the influence of the VWT on aerodynamic characteristics. In the present study, similar questions are being solved for a wing with "Advantage Technology winglets" wingtip type.

Formulation of the problem

We take the following coordination system. We place the beginning of the coordinates in the middle of the wing, direct the axis of Oz along the span to the right, the axis Oy 's directed upwards and Ox axis on the undisturbed flow. We define all the forces influencing on the aircraft with winglets type "Advantage Technology winglets" at a steady level flight. Due to equilibrium of these forces we determine the influence of aerodynamic forces of wingtip on the inductive drag of the wing.

The solution of the problem

The following forces effect the plane in level flight [4–6]:

- The power of the weight G — always directed vertically down to the center of the earth;
- Lift of the aircraft Y — is perpendicular to the direction of the undisturbed flow;
- Drag force of the aircraft Q — aimed in the direction opposite to the movement of aircraft;
- Thrust P — is generally directed towards the aircraft movement motion, along the axis;
- Full aerodynamic force created by the upper wingtips. The force created by the upper left wingtip is symbolized \vec{R}_l^g , but the force created by the right wingtip is symbolized \vec{R}_r^g ;
- Complete aerodynamic forces created by the lower wingtips. They are symbolized respectively, the left \vec{R}_l^g and the right force \vec{R}_r^g .

The angle between the true velocity and the free-flow speed for a wing with wingtips α_z equals to the angle between the vector of the total aerodynamic force generated by the upper left wingtip \vec{R}_l^g and the longitudinal axis of the wing, as the sides of these angles are perpendicular to each other.

Then the projection of the full aerodynamic force of the left wingtip will have the form:

$$\vec{R}_l^g = \{R_{lx}^g, R_{ly}^g, R_{lz}^g\},$$

Where

$$R_{lx}^g = R_l^g \cos \varphi \sin \alpha_z$$

Longitudinal force created by the upper left wingtip, φ -angle of wingtip camber (the angle between the vertical plane of aircraft symmetry and the tangent plane to the wingtip surface at the point of its center of pressure),

$$R_{ly}^e = R_l^e \sin \varphi$$

lift force created by the upper left wingtip,

$$R_{lz}^e = R_l^e \cos \varphi \cos \alpha_z$$

the lateral force generated by the upper left wingtip.

Here, R_l^e is the vector unit of \vec{R}_l^e ,

$$R_l^e = \sqrt{R_{lx}^{e2} + R_{ly}^{e2} + R_{lz}^{e2}}.$$

This force is applied to the center of the wingtip pressure. The total aerodynamic force of right upper wingtip differs from it only with the mark of the third component, so it can be written as

$$\vec{R}_n^e = \{R_n^e \cos \varphi \sin \alpha_z, R_n^e \sin \varphi, -R_n^e \cos \varphi \cos \alpha_z\}.$$

Obviously, $R_n^e = \sqrt{R_{nx}^{e2} + R_{ny}^{e2} + R_{nz}^{e2}} = R_n^e$

therefore, the lower indices that indicate the left and right wingtips will be removed in the future.

Then, the right and left upper part of the wingtips together create a force with components

$$2\vec{R}^e = \vec{R}_n^e + \vec{R}_l^e = \{2R^e \cos \varphi \sin \alpha_z, 2R^e \sin \varphi, 0\}. \quad (1)$$

Now we define the forces created by the lower part of wingtips (projections) (Fig 1).



Fig. 1. The AT winglet wingtip of the Airbus A319

Since, under the wing the air pressure is much higher than in the environment, it can be assumed that the lower left wingtip pressure force is applied to the center of pressure of the wingtip, normal to its surface. Lower wingtip camber is indicated by the letter φ , and the twist angle of the center of pressure is indicated by the letter β .

Then, with the same above mentioned argumentation, we can write

$$2\vec{R}^h = \vec{R}_n^h + \vec{R}_l^h = \{2R^h \cos \varphi \sin \beta, 2R^h \sin \varphi, 0\}. \quad (2)$$

Thus

$$2R_{lx}^e = 2R_l^e \cos \varphi \sin \alpha_z$$

the longitudinal is force generated by the lower parts of wingtip, but

$$2R_y^h = 2R^h \sin \varphi$$

lift force is created by them.

Because of symmetry, the lateral forces created by the left and right wingtips, balance each other.

The amount of power generated by all four parts of the wingtips “Advantage Technology winglets”, is indicated by the vector \vec{R}_z . Thus

$$\vec{R}_z = \{R_{zx}, R_{zy}, R_{zz}\},$$

Where

$$R_{zx} = 2R^e \cos \varphi \sin \alpha_z + 2R^h \cos \varphi \sin \beta \quad (3)$$

the longitudinal component of the vector of total aerodynamic wingtip force, which obviously reduces any drag force, and, of course, is added to the force of traction motors,

$$R_{zy} = 2R^e \sin \varphi + 2R^h \sin \varphi, \quad (4)$$

the vertical component of the vector of total aerodynamic wingtip force, which is added to the lift of the wing, and the lateral component of the vector of the total aerodynamic force due to the symmetry of wingtips equals to zero $R_{zz} = 0$.

Now, considering the formulas (3) and (4), we can write the equilibrium equations of steady motion of the aircraft with wingtips type “AT winglets” in level flight in the form of

$$\left. \begin{aligned} P + R_{zx} - Q &= 0 \\ Y + R_{zy} - G &= 0 \end{aligned} \right\}. \quad (5)$$

From the first equation of the system (5) it follows that the thrust of the engine P balances the force $Q - R_{zx}$. Since the force $Q = Q_{pr} + Q_i$ consists of the sum of the profile and inductive drag and the profile resistance is almost unchanged, the force R_{zx} reduces the inductive drag of the wing of the finite span without wingtips, i.e.

$$\Delta Q_i = R_{zx}$$

or, the reduced part of the inductive drag force equals to

$$\Delta Q_i = 2R^e \cos \varphi \sin \alpha_z + 2R^h \cos \varphi \sin \beta.$$

Heading in the direction of flight, this force increases the thrust of the engines and reduces the drag of the wing. In the case when the angles of collapse $\varphi = 0$ and $\beta = 0$ it has the greatest value, and when $\varphi = \beta = \pi/2$ — it turns to zero. Angles α and β are usually small enough. The latter case is a consequence of the fact that when $\varphi = \beta = \pi/2$ the tip turns into a wing extension with large sweep angles, in comparison with the wing itself, it also disappears. It turns out a longer wing without wingtips.

From the second equation of system (5) it follows that

$$Y + R_{zy} = G.$$

As follows from this equality, the lift Y is less than the weight of the aircraft, and the weight of the aircraft is balanced by the lifting forces created by the wing and the tips together. The quantities on the left side of this equation for wings without wingtips, with upper endings and with double endings, will be indicated, respectively, by the indices 0, 1 and 2 from above. Since the weight of the aircraft is constant and $R_{zy}^0 = 0$, then it can be written as follows:

$$Y^0 = Y^1 + R_{zy}^1 = Y^2 + R_{zy}^2 = G.$$

Following from formula (4)

$$0 < R_{zy}^1 < R_{zy}^2.$$

Then from the preceding chain of equations, it follows that

$$Y^0 > Y^1 > Y^2.$$

Thus, provided the weight of the aircraft is constant, the lift of the wing with the tips is reduced, and the smallest is obtained for the wing with double wingtips of the "AT winglets" type. The remaining part of the lifting force creates aerodynamic wingtips. In this regard, the distribution of the lifting force over the entire wing span with the "AT winglets" wingtip is more even. And this leads to a decrease in the amplitude of wing oscillations and noise during flight. Note that the tip itself is also a profiled winglet and from its end there is a flow of air towards the fuselage at the upper wingtips and from the fuselage at the lower wingtips. These currents, forming with the main flow of air against motion, create vortices of relatively low intensity, flowing from the ends of the tips. The inductive drag of the wing is affected only by the longitudinal component of the total aerodynamic force of the tips, defined by formula (3).

Power R_{zx} can be represented through the high-speed head,

$$R_{zx} = \bar{C}_{zx} q_{\infty} S_z = C_{zx} q_{\infty} S$$

where

$$q_{\infty} = \frac{\rho V_{\infty}^2}{2}$$

is velocity head, S wing area without wingtips, and C_{zx} the coefficient of longitudinal force of the wingtips. The coefficient of this force is

$$\bar{C}_{zx} = C_{zx} \frac{S}{S_z}$$

where S_z is the sum of the areas of the wingtips.

Then the force ΔQ_i can be written in the form

$$\Delta Q_i = C_{zx} q_{\infty} S.$$

The coefficient of inductive drag of the wing with the tips is written in the form of the difference in the inductive drag of the wing without the tip and the force factor ΔQ_i :

$$C_{zxi} = \frac{C_y^2}{\pi \lambda} (1 + \delta) - C_{zx}.$$

We express this expression in the following form

$$C_{zxi} = \frac{C_y^2}{\pi \lambda} (1 + \delta) \left[1 - \frac{\pi \lambda}{C_y^2 (1 + \delta)} C_{zx} \right]$$

or

$$C_{zxi} = \frac{C_y^2}{\pi \lambda} (1 + \delta)$$

where

$$\tilde{\lambda} = \lambda \left[1 - \frac{\pi \lambda}{C_y^2 (1 + \delta)} C_{zx} \right]^{-1}.$$

Aspect ratio of the wing. As can be seen the value of the aspect ratio makes it possible to record the inductive drag of the wing with the tips in the usual form. It is easy to see the inequality, which shows a decrease in the inductive drag of the wing under the influence of the wingtips.

Since

$$\frac{\pi \lambda C_{zx}}{C_y^2 (1 + \delta)} < 1$$

then a square bracket with negative degree is the sum of a geometric progression

$$1 + \frac{\pi \lambda C_{zx}}{C_y^2 (1 + \delta)} + \left(\frac{\pi \lambda C_{zx}}{C_y^2 (1 + \delta)} \right)^2 + \left(\frac{\pi \lambda C_{zx}}{C_y^2 (1 + \delta)} \right)^3 + \dots$$

Substituting this into the expressions for the effective elongation and leaving only the first two terms, we have

$$\tilde{\lambda} = \lambda \left[1 + \frac{\pi \lambda C_{zx}}{C_y^2 (1 + \delta)} \right]$$

or, taking into account the coefficient of inductive drag of the wing without wingtips,

$$\tilde{\lambda} = \lambda \left(1 + \frac{C_{zx}}{C_{xi}} \right).$$

Taking into account the following formula

$$C_{zx} = 2C_{zx}^e \cos \varphi \sin \alpha_z + 2C_{zx}^h \cos \varphi \sin \beta$$

we get the following

$$\tilde{\lambda} = \lambda \left(1 + \frac{2C_{zx}^e \cos \varphi \sin \alpha_z + 2C_{zx}^h \cos \varphi \sin \beta}{C_{xi}} \right).$$

This is an approximate expression of the wing aspect ratio with double tips.

The relative ratio of the wing is in the following form

$$\frac{\Delta \lambda}{\lambda} = \frac{C_{zx}}{C_{xi}}. \tag{6}$$

This result can be obtained in another way. We transform the expression for the aspect ratio

$$\begin{aligned} \tilde{\lambda} &= \lambda \left[1 - \frac{\pi \lambda}{C_y^2 (1 + \delta)} C_{zx} \right]^{-1} = \lambda \frac{1}{1 - \frac{C_{zx}}{C_{xi}}} = \\ &= \lambda \frac{C_{xi}}{C_{xi} - C_{zx}} = \lambda \frac{C_{xi}}{C_{zxi}}. \end{aligned}$$

Thus

$$\tilde{\lambda} = \lambda \frac{C_{xi}}{C_{zxi}}$$

or

$$\tilde{\lambda} C_{zxi} = \lambda C_{xi}.$$

With the following formula $C_{zx} = C_{zx}^e + C_{zx}^h$, the last equation can be extended

$$\tilde{\lambda} C_{zxi} = \tilde{\lambda}^e C_{zxi}^e = \lambda C_{xi}. \tag{7}$$

Here both $\tilde{\lambda}^e$ and C_{zxi}^e are aspect ratio, and the inductive drag of the wing with some upper wingtips. As can be seen, the product of effective lengthening of the wings with double and only upper tips on their coefficients of inductive drag is equal to the product of the wing extension without the wingtip to its coefficient of inductive drag. Thus, with increasing effective lengthening of the wing, its inductive drag decreases and vice versa.

This fundamental result can also be said as follows: when the weight of the aircraft is constant, the product of the effective wing aspect ratio with its wingtips to its coefficient of inductive drag is constant.

Alternatively, provided the weight of the aircraft is constant, the ratio of effective wing extensions is equal to the inverse ratio of their inductive drag coefficients.

We also must note the following proof of this result. From the expression for the coefficient of inductive drag for all wings

$$C_{zxi} = \frac{C_y^2}{\pi \lambda} (1 + \delta)$$

we get the following

$$\tilde{\lambda} C_{zxi} = \frac{C_y^2}{\pi} (1 + \delta)$$

which is constant with a constant weight of the aircraft.

Assuming the effective wing aspect ratio is known, from formulas (1.7) it is possible to determine the loss of inductive drag

$$\Delta C_{xi} = C_{xi} - C_{zxi} = C_{xi} - \frac{\lambda}{\tilde{\lambda}} C_{xi} = \frac{\tilde{\lambda} - \lambda}{\tilde{\lambda}} C_{xi} = \frac{\Delta \lambda}{\lambda} C_{xi}.$$

Conclusion

1. The aerodynamic forces created by the AT winglet wingtips during the flight are determined.

2. A system of algebraic equations containing all the forces acting on an airplane with a steady horizontal flight, which constitutes the mathematical model of the problem under investigation, is recorded.

3. It is shown that the wing tips reduce the inductive drag.

4. The aspect ratio of the wing is determined.

5. It is shown that, when the weight of the aircraft is constant, the product of the aspect ratio of the wing with its ends to its coefficient of inductive drag is constant.

REFERENCE

1. **Jafarzade R. M., Ilyasov M. H., Huseynli J. N.** Analysis of a finite span rectilinear winglets influence on its induced drag by the distributed vortex method. Transactions of National Academy of Sciences of Azerbaijan, series of physics-technical and mathem-l sciences, vol. The XXXV, № 1, 2015, pp. 120–126.
2. **Jafarzade R. M., Ilyasov M. H., Huseynli J. N.** Influence of wingtips on induced drag force of rectangular wing. "SAEQ" issue 6, 28 Mart's 2014, № 15, pp. 12–15.
3. **Jafarzade R. M., Ilyasov M. H., Huseynli J. N.** The analysis of a finite span rectilinear winglets influence on its induced drag by the distributed vortex method. Research work of the National Academy of Aviation, № 1, 2015, pp. 63–77.
4. **Arzhanika N. S., Maltsev V. N.** Aerodynamics, Moscow. 2011, pp. 483.
5. **Krasnov N. F.** Aerodynamics. Part 1. Theory basics. Aerodynamics of wing and its profile, Moscow, 2010, pp. 496.
6. **Krasnov N. F.** Aerodynamics. Part 2. Aerodynamic calculation methods. Moscow, 2010, pp. 368.

Malikov E.

INFLUENCE OF "AT WINGLETS" WINGTIP TYPE ON THE AERODYNAMIC CHARACTERISTICS OF WINGS

In this article by the method of equations of steady horizontal flight the impact «AT winglets» wingtips on the wing aerodynamic quality is explored. The total aerodynamic force, created by all four parts of the wingtips is determined. The vector of the total aerodynamic force of the wingtips is represented in the form of components of a linked coordinate system. Equilibrium equations for the steady motion of an aircraft with «AT winglets» type wing tips in a horizontal flight are recorded. From these equations it is obtained that, in the direction of motion, the longitudinal component of the vector of the total aerodynamic force of the tips reduces the inductive drag of the wing (increases the thrust of the engines), the vertical component is added to the lifting force of the wing and increases it, and the lateral components, due to the symmetry of the wing, are in balancing state. It is shown that the lifting force created by the «AT winglets» type wingtips is larger compared to the same ones created by the upper wingtips. An important consequence is that the distribution of the lifting force over the wing span with double tips is more uniform in comparison with the wing without a wingtip or with a wing with the upper wingtip. The expression for the effective aspect ratio of the wing with the tips is defined, which is greater than the inductive drag of the wing without the tip. An important consequence is obtained: at the constant weight of the aircraft, the product of effective wing aspect ratio with the «AT winglets» wingtips and only the upper wingtips by their coefficients of inductive resistance is equal to the product of the wing aspect ratio without a tip by its coefficient of inductive drag.

Keywords: AT winglet, a mathematical model, the aerodynamic characteristics, effective aspect ratio, steady motion.

Меликов Е. Т.

ВПЛИВ ЗАКІНЦІВОК «AT WINGLETS» НА АЕРОДИНАМІЧНІ ХАРАКТЕРИСТИКИ КРИЛА

У статті методом системи рівнянь устатовленого горизонтального польоту досліджується вплив закінцівок «AT winglets» на аеродинамічні характеристики крила. Визначається повна аеродинамічна сила, що створюється всіма чотирма частинами крила. Вектор повної аеродинамічної сили закінцівок уявляється у вигляді компонент у зв'язаній системі координат. Наводяться рівняння рівноваги устатовленого руху літака із закінцінками крила типу «AT winglets» у горизонтальному польоті. З цих рівнянь отримано, що прямуючи у бік руху, подовження компонента вектора повної аеродинамічної сили закінцівок зменшує індуктивний опір крила (збільшує силу тяги двигунів), вертикальна компонента додається до підйомної сили крила і збільшує її, а бічні компоненти, за рахунок симетрії крила, знаходяться в балансувальному стані. Показано, що частка підйомної сили, яка створена закінцінками типу «AT winglets», більша у порівнянні з тими ж, які створені верхніми закінцінками. Зроблено важливе слідство про те, що розподіл підйомної сили за розмахом крила з подвійними закінцінками більш рівномірний порівняно з крилом без закінцівок або ж з крилом з верхніми закінцінками. Визначається вираз ефективного подовження крила з закінцінками, яке більше індуктивного опору крила без закінцівок. Показано, що за умови сталості ваги літака, множення ефективного подовження крила з закінцінками і коефіцієнта індуктивного опору крила є величина постійна.

Ключові слова: AT winglets, математична модель, аеродинамічні характеристики, ефективно подовження, індуктивний опір, усталений рух.

Меликов Э.Т.

ВЛИЯНИЕ ЗАКОНЦОВОК «AT WINGLETS» НА АЭРОДИНАМИЧЕСКИЕ ХАРАКТЕРИСТИКИ КРЫЛА

В статье методом системы уравнений устатовившегося горизонтального полета исследуется влияние законцовок «AT winglets» на аэродинамические характеристики крыла. Определяется полная аэродинамическая сила, созданная всеми четырьмя частями законцовок. Вектор полной аэродинамической силы законцовок представляется в виде компонент в связанной системе координат. Приводятся уравнения равновесия устатовившегося движения самолета с законцовками крыла типа «AT winglets» в горизонтальном полете. Из этих уравнений получено, что направляясь в сторону движения, продольная компонента вектора полной аэродинамической силы законцовок уменьшает индуктивное сопротивление крыла (увеличивает силу тяги двигателей), вертикальная компонента прибавляется к подъемной силе крыла и увеличивает ее, а боковые компоненты, за счет симметрии крыла, находятся в балансирующем состоянии. Показано, что доля подъемной силы, созданная законцовками типа «AT winglets» больше по сравнению с теми же, созданными верхними законцовками. Сделано важное следствие о том, что распределение подъемной силы по размаху крыла с двойными законцовками более равномерное по сравнению с крылом без законцовок или же с крылом с верхними законцовками. Определяется выражение эффективного удлинения крыла с законцовками, которое больше индуктивного сопротивления крыла без законцовок. Показано, что при условии постоянства веса самолета, произведение эффективного удлинения крыла с законцовками и коэффициента индуктивного сопротивления крыла есть величина постоянная.

Ключевые слова: AT winglets, математическая модель, аэродинамические характеристики, эффективное удлинение, индуктивное сопротивление, устатовившееся движение.

Стаття надійшла до редакції 03.09.2018 р.
Прийнято до друку 10.09.2018 р.
Рецензент – д. т. н., проф. Абдуллаєв П. Ш.

І. О. Козлюк, д-р техн. наук, проф.
Національний авіаційний університет
orcid.org/0000-0001-4937-2756
e-mail: avia_ira@ukr.net

Ю. Б. Коваленко, докторант
Національний авіаційний університет
orcid.org/0000-0002-6714-4258
e-mail: yleejulee22@gmail.com

МЕТОДИ ОЦІНКИ ПОКАЗНИКІВ НАДІЙНОСТІ АВІАЦІЙНОЇ ТЕХНІКИ ЗА РЕЗУЛЬТАТАМИ ВИПРОБУВАНЬ ТА ТЕХНІЧНОЇ ДІАГНОСТИКИ

Вступ

Проблема забезпечення надійності розроблюваних систем управління обладнанням авіаційної техніки, що включає засоби обчислювальної техніки, сучасну радіоелектронну і автоматичну апаратуру, передбачає вирішення таких основних завдань:

1) прогнозування надійності розроблюваних функціональних систем (ФС) повітряних суден (ПС) на всіх етапах проектування з виявленням слабких місць і видачею своєчасних рекомендацій щодо забезпечення надійності;

2) контроль досягнутого рівня надійності на кінцевих етапах розробки на підставі результатів випробувань ПС;

3) оптимізація надійності розроблюваних ПС, програмними і апаратно-програмними засобами.

Підвищення точності апріорних оцінок проектованої надійності сприяє підвищенню якості, продуктивності та конкурентоспроможності розроблюваних ПС.

Аналіз останніх досліджень і публікацій

Існуючі інженерні аналітичні методи розрахунку показників надійності ПС зазвичай засновані на використанні однопараметричного експоненціального розподілу напрацювання елементів до відмови. При цьому передбачається, що протягом терміну експлуатації елементи не піддаються старінню і зносу, а при черговій відмові елементів ПС повністю відновлюється через надійність. Таке грубе моделювання надійності елементів ПС призводить до великих методичних похибок оцінок шуканих показників надійності ПС [7]. На сьогодні практично всі вирішення різноманітних складних завдань надійності отримані на підставі використання експоненціального закону, тобто на основі використання статистичної моделі надійності. Статистичний підхід до дослідження надійності ряду ПС стає практично неможливим через відсут-

ність статистики відмов через високу надійність ПС або наявності одиничних прикладів. Крім того, відсутність зв'язку показників надійності з фізичними характеристиками ПС і зовнішніми умовами експлуатації не дає можливості ефективно управляти проектуванням і забезпеченням необхідного рівня надійності ПС, що розробляються та експлуатуються [2]. Інший шлях встановлення кількісних показників надійності, на відміну від строго ймовірнісного підходу, заснований на вивченні механо-фізико-хімічних властивостей і деяких фізичних параметрів ПС, які характеризують технічний стан останніх. А саме, встановлення кількісних показників надійності засноване на визначенні аналітичного зв'язку показників надійності з закономірностями зносу, зокрема зі швидкістю протікання фізико-хімічних процесів. У цьому випадку найбільш ефективним і загальним є підхід, заснований на використанні в якості моделей зносу випадкових процесів та стохастично кінетичних рівнянь, що призводить до законів розподілу відмов. Даний підхід називається ймовірнісно-фізичним, оскільки він безпосередньо встановлює зв'язок імовірності відмови і фізичного параметра, що викликає відмову. Внаслідок цього параметри одержуваного ймовірнісного розподілу відмов мають певний фізичний сенс. Розподіл відмов (розподіл наробітку до відмови), параметри якого мають конкретну фізичну інтерпретацію, прийнято називати ймовірнісно-фізичним розподіленням відмов. Під визначальними параметрами в цьому випадку мають на увазі такі початкові фізичні параметри: скупчення дислокацій та інших дефектів, пластичні і пружні деформації, механічний знос, провідність контактуючих, суцільних провідників струму та n - p переходів та ін., перевищення якими певних граничних значень призводить до відмови.

Мета статті. Необхідно перевірити та підтвердити, що в сучасних умовах суворого дефі-

циту часу і незначної статистики відмов тільки ймовірно-фізичний підхід, який додатково використовує інформацію про фізичний знос ПС, здатний ефективно вирішувати необхідні для інженерної практики завдання надійності, в тому числі розрахунків надійності обладнання ПС. У цій статті представлені сучасні методи вирішення основних завдань надійності на основі ймовірно-фізичної теорії надійності.

Виклад основного матеріалу

Ймовірно-фізичні моделі мають більшу перевагу перед суворо ймовірнісними моделями надійності в тому, що їх параметри можуть бути оцінені на підставі, як статистики відмов, так і аналізу фізичного зносу. Для багатьох ПС завдання оцінки надійності можна вирішити в результаті вимірювання деяких визначальних параметрів в процесі випробувань, які не доводять ПС до стадії руйнування.

Відмови елементів ПС викликають значні втрати коштів, сил і часу через руйнування обладнання ПС, необхідність проведення відновлювальних робіт і пов'язаних з ними простоїв ПС, шкоди від невиконання певних завдань.

Крім того, недостатня надійність ПС негативно впливає на безпеку їх експлуатації [9].

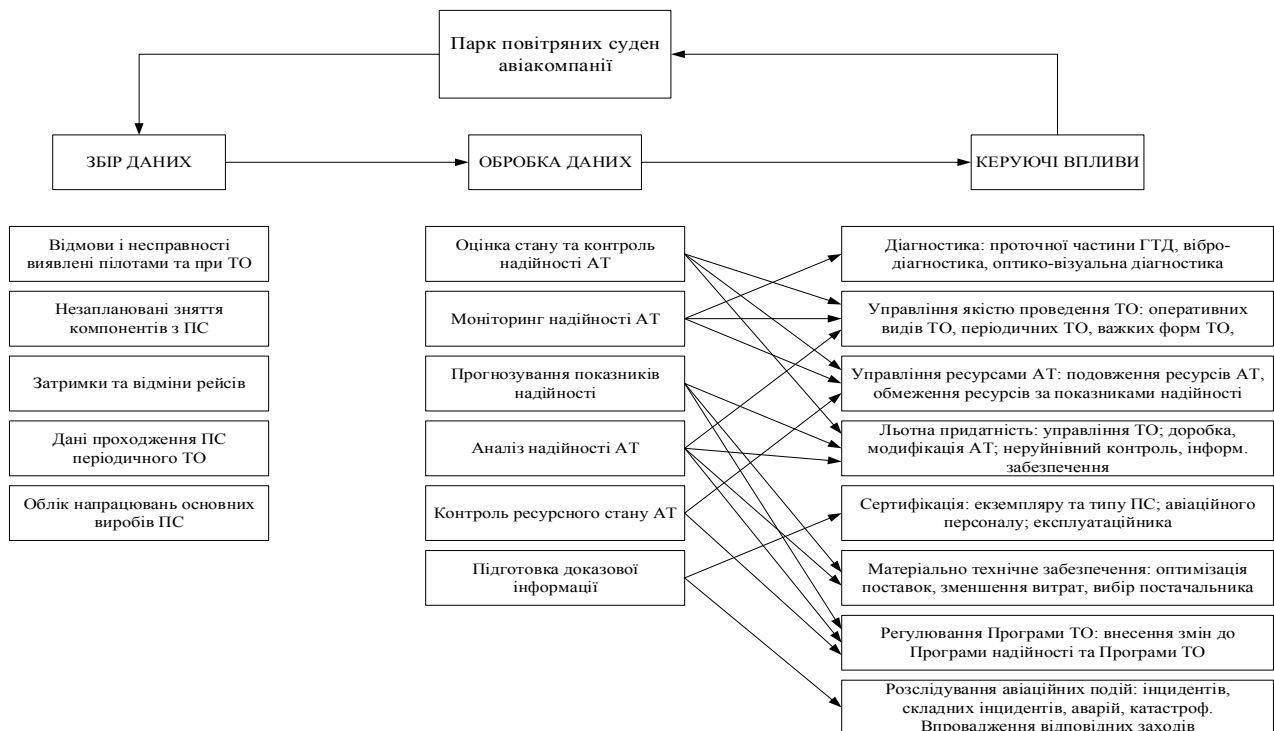
Значимо, в авіакомпанії основними заходами, спрямованими на збільшення прибутку, є

оптимізація процесів технічного обслуговування та матеріально-технічного забезпечення, своєчасна сертифікація екземплярів, типів ПС, персоналу і експлуатаційника та забезпечення льотної придатності парку ПС.

Усі ці заходи засновані на даних з надійності. Важливим питанням є правильна організація системи збору інформації з надійності, причому необхідно зазначити, що авіакомпанія експлуатує авіаційну техніку і за станом, і за ресурсами. Тобто потрібно враховувати дані по відмовам, наробіткам та ресурсам компонентів авіаційної техніки (АТ).

Для управління надійністю ПС в авіакомпанії розроблено загальний контур управління експлуатацією ПС показано на рисунку, основними складовими якого є збір, обробка даних та керуючі впливи.

На основі даних про відмови і несправності, виявлені екіпажем у польоті та наземними службами при ТО, незаплановані зняття компонентів з ПС, затримки та відміни рейсів, даних проходження ПС періодичного ТО, обліку напрацювань основних виробів ПС проводиться оцінка стану та контроль надійності компонентів АТ, моніторинг, прогнозування показників надійності, контроль і аналіз ресурсного стану АТ та підготовка доказової інформації [6; 8].



Загальний контур управління надійністю ПС в авіакомпанії

Результати обробки даних використовуються для інформаційної підтримки процесів регулю-

вання Програм надійності і технічного обслуговування ПС, діагностування, управління якістю

проведення ТО, управління ресурсами АТ, забезпечення льотної придатності, сертифікації, матеріально-технічного забезпечення та розслідування авіаційних подій.

При зміні стану надійності проводиться управління процесом введення нових процедур з діагностики та контролю АТ для раннього виявлення та попередження відмов. На основі отриманих даних з надійності проводиться планування та зміна періодичності оглядів та проведення ТО з ціллю раннього попередження відмов.

На основі результатів з обробки даних про надійність проводиться управління якістю ТО. Аналізуються якість робіт виконаних окремими працівниками, бригадами, змінами та цехами, які проводять оперативне, періодичне ТО та важкі форми ТО. Спираючись на аналіз, вводяться штрафні або заохочувальні санкції, проводиться збір доказової інформації про рівень кваліфікації персоналу для його сертифікації.

Під час управління ресурсами, залежно від значення розрахованих показників надійності та його впливу на безпеку польотів, компоненти авіаційної техніки переводяться на відповідні методи технічного обслуговування за станом або за ресурсом.

Для обслуговування за ресурсом важливими питаннями управління є подовження або обмеження ресурсів компонентів АТ.

Досягнутий рівень надійності та безпеки польотів визначає стан забезпечення льотної придатності авіаційної техніки. Тому процеси управління надійністю направлені на підвищення та забезпечення льотної придатності ПС.

Проведення сертифікації експлуатанта, екземпляру та типу ПС, авіаційного персоналу, багато в чому засновано на даних про надійність АТ. На основі цієї інформації в авіакомпаніях готуються необхідні звіти та доказова інформація на основі якої визначається стан льотної придатності кожного екземпляру та парку типів ПС авіакомпанії, рівень кваліфікації обслуговуючого персоналу [2; 4].

Процес управління матеріально-технічним забезпеченням авіакомпанії, що базується на даних про відмови, наробітки та ресурси комплектуючих виробів ПС та наявності запасних частин і витратних матеріалів на складах та пунктах комплектуваннях, включає вирішення задач оптимізації поставок запасних частин, вибору постачальників, у яких умови закупки та якість компонентів АТ кращі.

Якщо при розслідуванні авіаційних подій, інцидент стався з технічної причини, проводиться ряд заходів, складаються бюлетені, направлені на підвищення надійності типу ПС [7].

Регулювання Програми ТО та програми надійності проводиться шляхом внесення необхідних змін до програми технічного обслуговування, поопераційних відомостей. Ці зміни направлені на підвищення рівня надійності та зменшення витрат на технічне обслуговування АТ, забезпечення заданого рівня льотної придатності та безпеки польотів. Отже, в основу автоматизованої системи для визначення стану надійності парку ПС авіакомпанії покладені такі показники безвідмовності:

- середній наробіток на відмову

$$T = \sum_{i=1}^N \frac{t_i}{n}$$

де N — загальне число компонентів ПС (двигунів, систем, комплектуючих виробів); t_i — наробіток i -го компонента ПС за розглянутий календарний період; n — число відмов компонентів ПС за цей період;

- середнє значення параметра потоку відмов

$$\omega_{k,r,v,j} = \frac{\sum_{j=1}^l \Delta n_{k,r,j}}{\sum_{j=1}^l t_{\text{сум},k,r,j}}$$

де $\Delta n_{k,r,j}$ — кількість відмов r -го виду елемента k -го типу в j -му інтервалі наробітку; $t_{\text{сум},k,r,j}$ — сумарний наробіток v -го виду елемента k -го типу за j -й контрольний період; l — число інтервалів наробітку;

– імовірність справної роботи елементів за умови, що значення наробіток між відмовами і несправностями розподіляється за експонентним законом:

$$P_{k,r,j} = \exp(-\omega_{k,r,j} t),$$

де t — задана величина наробітку.

Тобто оцінка якості проведення ТО обслуговуючим персоналом визначається за такими показниками:

- початкові оцінки якості:

$$H_{K_n} = \frac{N_1}{N} 100\% = \frac{N-T}{N} 100\% = \left(1 - \frac{T}{N}\right) 100\%,$$

де N — кількість пред'явлених робіт; N_1 — кількість прийнятих з першого пред'явлення робіт; T — кількість оформлених талонів другого пред'явлення;

- узагальнені показники якості:

$$R_{K_s} = H_{K_s} K_{CH} K_W K_{\Gamma},$$

де

$$K_{CH} = 1_1^{n_1} 1_2^{n_2} \dots 1_z^{n_z} = \prod_z 1_1^{n_1},$$

$$K_W = \frac{a_{\Phi}}{a_0}, K_{\Gamma} = \frac{W_{\Phi}}{W_0}.$$

де 1_i^n — коефіцієнти перерахунку початкової оцінки якості; z — кількість перерахувань; a_ϕ і a_0 — фактичний виробіток і встановлений норматив на даний період на одного виконавця; W_ϕ і W_0 — фактичний і запланований об'єми робіт з технічного обслуговування для ділянки зміни; K_r — коефіцієнт гарантії; s — індекс того виду продукції, для якого визначалися всі розглянуті величини; $s = 1, 2, \dots, S$;

– індекси якості:

$$I_R = \frac{W_1 \frac{R_{K_1}}{R_{K_1^0}} + W_2 \frac{R_{K_2}}{R_{K_2^0}} + W_S \frac{R_{K_S}}{R_{K_S^0}}}{W_1 + W_2 + \dots + W_S} = \frac{\sum_{s=1}^S W_s \frac{R_{K_s}}{R_{K_s^0}}}{\sum_{s=1}^S W_s},$$

де W_s — об'єм продукції s -го виду, тобто об'єм технічного обслуговування по ділянці, цеху; $s = 1, 2, \dots, S$, $R_{K_s^0}$ — базові значення узагальнених показників якості технічного обслуговування;

– загальний рівень якості:

$$R_{3AT} = \frac{W_1 R_{K_1} + W_2 R_{K_2} + W_S R_{K_S}}{W_1 + W_2 + \dots + W_S} = \frac{\sum_{s=1}^S W_s R_{K_s}}{\sum_{s=1}^S W_s}.$$

Зазначимо, що при постійному значенні потоку відмов відновлювальних елементів АТ, використовується метод контролю та прогнозування надійності на основі розподілу Пуассона. Спочатку в методі визначається середнє значення параметра потоку відмов

$$\overline{\omega}_{oye} = \frac{1}{k} \sum_{j=1}^k (\omega_{oye})_j,$$

де $(\omega_{oye})_j$ — параметр потоку відмов елемента за j -й період експлуатації (місяць, квартал, рік), що передує контрольованому, з номером k .

Допустиме число відмов елемента $n_{доп k}$ за контрольований період знаходиться з рішення рівняння $P(n_{доп k}, \overline{\omega}_{oye}, t_{сум k}) = P_{доп}$, яке при Пуассонівському потоці відмов, має вигляд:

$$P_{доп} = \sum_{n=0}^{n_{доп k}} \frac{(\overline{\omega}_{oye} t_{сум k})^n}{n!} \exp(-\overline{\omega}_{oye} t_{сум k}),$$

де $P(\cdot)$ — закон розподілу ймовірності безвідмовної роботи; $t_{сум k} = m \sum t_i k$ (при $i = \overline{1, m}$) — сумарний наробіток елемента за контрольований період; t_{ik} — наробіток i -го елемента за контрольований період; m — кількість однотипних елементів на ПС; $P_{доп}$ — припустима ймовірність безвідмовної роботи елемента, що зазвичай

приймається рівною $P_{доп} = 0,975, 0,9$, або $0,75$. Значення $0,75$ ймовірності безвідмовної роботи елемента визначено як оптимальне, якщо час поставки (закупки) елемента незначний.

Якщо фактичне число відмов $n_{фк}$ за контрольований період перевищує отриману з рішення рівняння величину $n_{доп k}$, тобто

$$n_{фк} > n_{доп k},$$

то необхідно розробити заходи по підвищенню рівня надійності АТ.

Припустиме число відмов елемента $n_{доп in}$ за прогнозований період експлуатації визначається шляхом рішення рівняння типу відносно n :

$$P_{доп} = \sum_{n=0}^{n_{доп+пр}} \frac{(\overline{\omega}_{oye} t_{сум пр})^n}{n!} \exp(-\overline{\omega}_{oye} t_{сум пр}),$$

де $t_{сум пр}$ — передбачуваний сумарний наробіток елемента за період прогнозу, що приблизно можна оцінити за допомогою співвідношення

$$t_{сум пр} \approx t_{сум k} \left(1 + \frac{N_H - N_C}{N} \right).$$

Тут N_H — число ОВ, що надходять в експлуатацію в прогнозований період; N_C — кількість ОВ, що підлягають списанню в той же період.

За необхідності забезпечення експлуатації відновлювальних виробів на заданому інтервалі $[0, t_k]$, якщо інтервал експлуатації виробу є досить великим порівняно з середнім часом між відмовами, приймається розподіл відмов по закону, близькому до нормального. При цьому число відмов визначається як

$$m(t) = \frac{t}{T} + u_\alpha \frac{\sigma \sqrt{t}}{T^{3/2}},$$

де $m(t)$ — прогнозована кількість елементів, $u_{1-\alpha}$ — квантиль нормального розподілу для ймовірності, рівної $(1 - \alpha)$; T — середній час між відмовами; σ^2 — дисперсія часу між відмовами, t — поточний наробіток.

Для прийняття правильних рішень з управління експлуатацією ПС необхідно оперувати достовірною інформацією з надійності авіаційної техніки [3; 4; 5]. Для цього була розроблена автоматизована система, на основі якої реалізується блок обробки даних загального контуру управління надійністю парку ПС.

До автоматизованої системи вводяться дані з надійності, які беруться з журналів пілотів, цехів оперативного і періодичного ТО, планово-диспет-

черського відділу — загальна інформація про літак, у якому виявлено несправності, опис відмов та вжитих заходів для їх усунення, дані по знятих та встановлених агрегатах, постачальникам цих агрегатів, облік напрацювань агрегатів, інформація по затримкам, відмінам рейсів, інцидентах, відкладеному ТО та ін. На основі цих даних визначаються фактичні показники надійності та проводиться:

- контроль рівня надійності парку типів ПС авіакомпанії;
- моніторинг показників надійності ПС авіакомпанії;
- визначення загальної статистики відмов, затримок рейсів, інцидентів, повторних дефектів, відкладеного ТО парку ПС авіакомпанії;
- визначення загальної статистики замінив двигунів ПС авіакомпанії з різних причин;
- визначення стану надійності комплектуючих виробів, систем і основних виробів ПС авіакомпанії;
- прогнозування запасу комплектуючих виробів ПС авіакомпанії;
- аналіз якості виконання важких форм ТО;
- контроль за проведенням випробувань допоміжної силової установки (ДСУ) при висотному старті та системи автоматичної посадки.

На основі загальних статистичних даних з надійності, проводиться моніторинг відмов в польоті та на землі, затримок рейсів, інцидентів, повторних дефектів, відкладеного ТО парку ПС авіакомпанії за обраний період експлуатації. Для кожного типу та екземпляру ПС також проводиться моніторинг напрацювання в годинах, польотних циклах, середньої тривалості польоту та добового нальоту.

Визначаються загальні статистичні дані по запланованим та незапланованим зняттям двигунів з ПС та вимкненням двигунів в повітрі.

Прогнозування надійності проводиться для матеріально-технічного забезпечення авіакомпанії необхідними запасними частинами, оптимізації процесу поставок, зменшення витрат та вибору того постачальника, у якого якість товару та умови закупки кращі. Аналіз якості виконання важких форм ТО проводиться шляхом оцінки стану надійності АТ за 40-денний період експлуатації після ремонту та його порівняння з середніми показниками за попередній рік.

На основі отриманих даних вводяться штрафні або заохочувальні санкції бригадам та цехам, або підрядним організаціям, що проводили ремонт.

Дослідження відмов ПС, наприклад, на основі експоненціального розподілу, є однопараметрична функція, яка широко використовувалася

по теперішній час в теорії надійності завдяки простоті моделі. Однак необхідно критично підходити до застосування цієї моделі, оскільки однопараметричність моделі накладає на неї ряд істотних обмежень, робить її грубо наближеною і призводить до дуже великих похибок, як при розрахунку надійності, так і при експериментальній оцінці.

Звідси, всі відомі методи показників надійності, засновані на використанні строго ймовірнісних моделей розподілу відмов (експоненціального, Вейбулла та ін.), допускається тільки два можливих стану елементів системи — справний і несправний, імовірності поєднання яких визначає також двопозиційний стан системи в цілому — працездатний або непрацездатний.

Метод розрахунку, заснований на використанні ймовірнісно-фізичної моделі, відрізняється від строго ймовірнісних методів тим, що він розглядає безперервну множину станів елементів і системи з безперервним часом і називається *ймовірнісно-фізичним методом*.

За результатами дослідження певних параметрів, що характеризують технічний стан ПС, можна відшукати параметр, який інформує про витрачання ресурсу ПС, і, оцінивши швидкість його зміни і знаючи його граничне значення, можна прогнозувати всі необхідні кількісні показники надійності ПС.

Основним завданням теорії надійності є розробка кількісних методів оцінки надійності та визначення найбільш раціональних методів забезпечення необхідного рівня надійності ПС, які створюються і вводяться в експлуатацію. Застосування кількісних методів дослідження надійності забезпечує:

- наукове обґрунтування вимог до новостворюваних зразків ПС;
- проектування обладнання ПС з необхідним рівнем надійності;
- планування обсягів, термінів і способів відпрацювання ПС для досягнення заданого рівня надійності;
- обґрунтування шляхів зниження економічних витрат і скорочення часу на розробку ПС;
- вибір і обґрунтування найбільш ефективних заходів забезпечення надійності на етапах проектування, конструкторського відпрацювання, виготовлення і експлуатації ПС;
- об'єктивну оцінку технічного стану ПС, які знаходяться в експлуатації;
- розробку науково обґрунтованих рекомендацій, спрямованих на поліпшення авіаційної техніки і методів її експлуатації.

Через складність фізичних процесів, що призводять до відмови, і неможливості врахувати всі

початкові умови, а також випадковий вплив навантажень в процесі експлуатації, в даний час загальноприйнято вважати появу відмови випадковою подією в тому сенсі, що задана структура авіаційного обладнання та умови його експлуатації не визначають точно моменти і місце виникнення відмов. Прийняття цієї концепції зумовлює математичний апарат, який повинен бути використаний для визначення показників надійності і побудови на їх основі теорії надійності. Як відомо, кількісною характеристикою випадкової події є її ймовірність, яка приблизно дорівнює частоті появи події в достатньо довгій послідовності спостережень за незмінних умов.

Теоретичне дослідження надійності та практичні оцінки показників надійності ПС можна віднести до двох етапів, які відрізняються один від одного і постановками задач, і вихідними даними, і використовуваними математичними апаратами [11; 12; 13].

Перший етап дослідження надійності називають *апріорним аналізом надійності*. Існують ще кілька визначень цього етапу оцінки надійності: аналітичні методи розрахунку надійності ПС, що розробляються, проектна оцінка надійності. Апріорний аналіз надійності проводиться на стадії проектування системи, коли конструкторами намічено кілька конкуруючих структурних схем ПС. Цей аналіз передбачає апріорі повністю відомими кількісні характеристики надійності всіх використовуваних елементів ПС. Насправді ж на стадії проектування зазначені апріорні дані конструктор має лише для тих типів елементів ПС, які тривалий час перебували в експлуатації. Для нових елементів ПС немає достовірних кількісних характеристик надійності, і їх можна задавати за аналогією з показниками надійності елементів ПС, що застосовуються або по інтуїції.

Таким чином, апріорний аналіз базується на апріорних (імовірнісних) характеристиках надійності, які лише приблизно і неповно відображають дійсні процеси в ПС. Проте, для порівняння показників надійності декількох структурних схем ПС використання апріорного аналізу може бути дуже корисним. Цей аналіз дозволить виявити на стадії проектування слабкі з точки зору надійності місця в конструкції і вжити необхідні заходи до їх усунення, а також відкинути незадовільні варіанти побудови ПС.

Саме в даному сенсі апріорний аналіз надійності, не претендуючи на видачу достовірних кількісних характеристик, має істотне значення в практиці проектування, і тому становить невід'ємну частину технічних проектів ПС.

Оскільки апріорний аналіз передбачає цілком визначеними ймовірнісні характеристики надій-

ності, то для його здійснення використовують методи теорії ймовірності та теорії випадкових процесів.

Другий етап дослідження і оцінки показників надійності вже розроблених і виготовлених ПС називають *апостеріорним аналізом надійності* (експериментальна оцінка). Його проводять на підставі статистичної обробки експериментальних даних про працездатність і відновлюваність ПС, отриманих в процесі її налагодження, випробувань і експлуатації. Метою випробувань на надійність і збору експлуатаційних даних про надійність є оцінка досягнутого рівня надійності ПС.

У даному випадку завдання апостеріорного аналізу полягає, перш за все, в оцінці невідомих параметрів за результатами спостережень і в подальшому розрахунку за допомогою цих оцінок показників надійності.

Визначальні випробування ПС на надійність проводять для визначення фактичних показників надійності ПС із заданою точністю і достовірністю.

При плануванні визначальних випробувань ПС для кожного показника, який визначається, повинні бути вказані:

- очікуване значення показника надійності повітряних суден — A_0 ;
- очікуване значення коефіцієнта варіації напруження до відмови v_0 ;
- достовірність (довірча ймовірність q) і точність (відносна помилка δ) оцінки показника надійності повітряних суден;
- тип плану випробувань (з відновленням, заміною або без заміни, певною тривалістю або до певного числа відмов повітряних суден).

Вибір довірчої ймовірності q (двосторонньої), а також відносної помилки δ оцінки показників надійності ПС здійснюють за погодженням із замовником відповідно до вимог стандартів (загальнотехнічних і галузевих).

За результатами визначальних випробувань на надійність за кожним показником надійності обчислюють точкову оцінку A , нижню \underline{A} і верхню \overline{A} довірчі кордони, відповідні заданій довірчій ймовірності. Зв'язок між односторонньою p і двосторонньою q довірчими ймовірностями така:

$$\beta = \frac{1+q}{2}.$$

План випробувань на надійність ПС встановлює число випробувань, порядок проведення випробувань (з відновленням працездатного стану ПС після відмови, заміною ПС, що відмовило або без заміни і відновлення) і критерій їх припинення.

Випробуванням піддаються однотипні ПС, що не мають конструктивних або інших відмінностей, виготовлені за єдиною технологією і випробувані в ідентичних умовах. Тривалість або обсяг роботи (напрацювання) ПС залежно від їх типу і умов експлуатації може вимірюватися в годинах або циклах.

Реалізація запропонованої методології з оцінки рівня надійності здійснювалася на підприємстві на п'яти виробках одного типу.

Проведено оцінку рівня надійності комплексуючих виробів (КВ) повітряних суден за результатами їх експлуатації із застосуванням методів експлуатації за технічним станом. Оцінка проводилася за даними, представленим користувачами ПС за певний період експлуатації.

Оцінка кожного чергового етапу формувалася шляхом обробки повного обсягу даних з початку експлуатації парку ПС. Повний обсяг даних для обробки формувалася на основі наявного обсягу даних попереднього етапу, доповненого і відкоригованого за даними, отриманими на оцінюючому етапі. При цьому, за рахунок збільшення обсягу статистичних даних, на кожному новому етапі обробки, вироблялося уточнення як складу даних, так і оцінок значень даних, оцінок параметрів, отриманих на попередньому етапі. При зростанні напрацювання КВ, також проводилася оцінка параметрів з напрацювання КВ.

Для проведення робіт формувалася база вихідних даних про хід експлуатації повітряних суден і КВ, його функціональних систем для всього парку ПС, які в міру надходження нових даних доповнювалися і відповідним чином коригувалися. Зміст бази даних проходив процедуру обов'язкової періодичної звірки з даними відповідного користувача. За результатами звірки проводилося необхідне коригування змісту бази даних, на основі якої в подальшому проводилася оцінка рівня надійності і необхідний аналіз.

Для побудови оцінки рівня надійності використовувався такий склад вихідних даних:

– по повітряним суднам — напрацювання по кожному польоту (дата, тривалість) кожного ПС за весь період експлуатації;

– щодо комплектуючих виробів:

1) належності кожного КВ повітряному судну;

2) на якому ПС встановлено;

3) дата установки, дата демонтажу;

4) напрацювання за час кожної чергової установки;

5) дата відмови;

6) напрацювання КВ — сумарне при кожному демонтажі,

7) напрацювання КВ на момент оцінки: сумарне, після чергової установки,

8) визначався склад КВ, що експлуатувалися на повітряному судні,

9) для кожного КВ визначалися дані по пп. 1–7.

Оцінка проводилася із застосуванням контролю рівня надійності кожного КВ. При цьому розглядалися умови виникнення деяких ситуацій польоту ПС, в тому числі: особлива ситуація (ОС); катастрофічна ситуація (КС); аварійна ситуація (АС); складна ситуація (СС); ускладнення умов польоту (УУП).

Особлива ситуація — аварійна подія, що характеризує як «ускладнення умов польоту», «складну ситуацію», «аварійну ситуацію», «катастрофічну ситуацію», виникнення якої, пов'язане з можливістю впливу несприятливих факторів, або їх поєднання на будь-якому з етапів польоту, що приводить до зниження безпеки польоту.

Катастрофічна ситуація — особлива ситуація, при виникненні якої, запобігання загибелі людей або втрати ПС виявляється практично неможливим.

Аварійна ситуація — особлива ситуація, що характеризується значним підвищенням психофізіологічних навантажень на екіпаж, погіршення льотних характеристик, стійкості, керованості, яка веде до досягнення (підвищення) граничних обмежень і розрахункових умов польоту.

Складна ситуація — особлива ситуація, що характеризується помітним підвищенням психофізіологічних навантажень на екіпаж або погіршенням льотних характеристик, стійкості, керованості льотних характеристик, або виходом одного або декількох параметрів польоту за експлуатаційні обмеження, але без досягнення граничних обмежень і розрахункових умов польоту.

Ускладнення умов польоту — особлива ситуація, що характеризується незначним збільшенням психофізіологічних навантажень на екіпаж або незначне погіршення характеристик стійкості, керованості або льотних характеристик.

Розрахунок виконувався інтервальний — для кожних 1000 год нальоту парку. Завданням контролю було — перевірити, чи є зростання за інтенсивністю відмов і, якщо є — визначити на якому напрацюванні блоку відбувається таке зростання. При цьому виявлялися випадки збільшення інтенсивності в два і більше разів. Вид контролю рівня надійності, встановлений при сертифікації з результатами оцінки для кожного КВ.

Висновки

Проведено обробку даних про надійність КВ повітряних суден за певний період експлуатації. Початкова обробка даних первинний етап оцінки була виконана для початкового і подальшого періоду експлуатації. Обробка чергового етапу

проводилася шляхом додавання до обсягу даних попереднього етапу нових даних, отриманих на етапі, який оцінюється коригуванням змісту бази даних попереднього періоду (за необхідності), і повторного розрахунку нових значень параметра $\omega_{\text{ср}}$.

Розрахунок значень параметра $\omega_{\text{ср}}$ (потік відмов) проводився для кожного КВ, яке експлуатується за методом «відмов», за умови, що статистичних даних досить для виконання розрахунку (зафіксовано три і більше відмови).

Для оцінки наявності змін $\omega_{\text{ср}}$ в міру зростання напрацювання КВ, виконувався розрахунок для не менше ніж двох інтервалів напрацювання КВ.

Проводився порівняльний аналіз результатів оцінки $\omega_{\text{ср}}$:

- для порівняльної оцінки рівня надійності, отриманого за результатами експлуатації (значення $\omega_{\text{ср}}$ на періоді, що оцінюється) і значення контрольного рівня;

- для порівняльної оцінки $\omega_{\text{ср}}$ на попередньому етапі та етапі, що оцінюється;

- для порівняльної оцінки $\omega_{\text{ср}}$ по інтервалах напрацювання КВ.

За результатами аналізу результатів обробки встановлено:

- значення $\omega_{\text{ср}}$ на етапі, що оцінюється, не перевищують встановлених значень для контрольного рівня надійності,

- істотного зростання $\omega_{\text{ср}}$ в міру збільшення напрацювання КВ не виявлено;

- істотного зростання значення $\omega_{\text{ср}}$ при напрацюваннях, які перевищують установлені значення ресурсу до першого ремонту або призначеного не виявлено.

Таким чином, даних, що потребують зміни складу (переліку) КВ, що експлуатуються за методом «відмов», не виявлено.

Перспективи подальших досліджень

Отримання кількісних показників по ресурсу і надійності КВ дозволяє порівняно просто прогнозувати очікуване залишкове напрацювання (ресурс, термін експлуатації) на будь-який момент експлуатації як на стадії проектування, коли використовується та сама інформація, що і для прогнозування початкового напрацювання (ресурсу, терміну експлуатації), так і на стадії

випробувань і експлуатації, коли є можливість уточнення початкових оцінок шляхом використання додаткової інформації.

ЛІТЕРАТУРА

1. **Воробьев В.** Надежность и техническая диагностика авиационного оборудования: учебник / В. Воробьев, В. Константинов. — М. : МГТУ ГА, 2010. — 440 с.

2. **Бургаев Ю., Острейковский В.** Статистический анализ надежности объектов по ограниченной информации. — М. : Энергоатомиздат, 1995. — 240 с.

3. ДСТУ 2860-94. Надійність техніки. Терміни та визначення. — К. : Держстандарт України, 1995. — 91 с.

4. ДСТУ 2861-94. Надійність техніки. Аналіз надійності. Основні положення. — К. : Держстандарт України, 1995. — 32 с.

5. ДСТУ 2862-94. Надійність техніки. Методи розрахунку показників надійності. — К. : Держстандарт України, 1995. — 39 с.

6. **Дзиркал Э.** Задание и проверка требований к надежности сложных изделий / Э. Дзиркал. — М. : Радио и связь, 1981. — 176 с.

7. **Diccio T., Efron B.** Bootstrap Confidence Intervals, Statistical Science. — Vol. 11, №. 3, 1996. — P. 189–228.

8. **Креденцер Б. П.** Прогнозирование надежности систем с временной избыточностью / Б. П. Креденцер. — К. : Наук. думка, 1978. — 240 с.

9. **Кучер О.** Контроль та аналіз стану надійності систем і агрегатів повітряних суден в експлуатації / О. Кучер, П. Власенко // Наукоємні технології. — К. : НАУ, №1(15), 2010. — С. 15–26.

10. **Міляев Ю.** Основы надійності технічних систем: навч. посібник / Ю. Міляев, О. Нечипоренко. — К. : Видавн.-полігр. центр Акад. муніцип. управління, 2008. — 246 с.

11. Надійність техніки. Методи оцінки показників надійності за експериментальними даними : ДСТУ 3004-95. [Чинний від 1995-01-25]. — К. : Держспроживстандарт України, 1995. — 51 с.

12. **Топольский М.** Методы максимального использования эксплуатационной информации о надежности / М. Топольский // Вопросы экспериментальной оценки показателей надежности. — М. : Знание, 1979. — С. 56–88.

13. **Скрипник В.** Анализ надежности технических систем по цензурированным выборкам / В. Скрипник, А. Назин, Ю. Приходько, Ю. Благовещенский. — М. : Радио и связь, 1988. — 184 с.

Козлюк І. О. Коваленко Ю. Б.

МЕТОДИ ОЦІНКИ ПОКАЗНИКІВ НАДІЙНОСТІ АВІАЦІЙНОЇ ТЕХНІКИ ЗА РЕЗУЛЬТАТАМИ ВИПРОБУВАНЬ ТА ТЕХНІЧНОЇ ДІАГНОСТИКИ

У статті пропонуються методи визначення характеристик показників надійності функціональних систем авіаційної техніки, засновані на використанні експоненціального розподілу ймовірно-фізичної моделі відмов. Дана оцінка методу, визначає довірчу ймовірність і точність оцінки показника надійності функціональних систем. Оцінка рівня надійності та його аналіз представлений за результатами випробувань і технічної діагностики авіаційної техніки. Також проведено обробку даних про надійність комплектуючих виробів повітряних суден за певний період експлуатації. Початкова обробка даних первинний етап оцінки була виконана для початкового і подальшого періоду експлуатації. Обробка чергового етапу проводилася шляхом додавання до обсягу даних попереднього етапу нових даних, отриманих на етапі, який оцінюється коригуванням змісту бази даних попереднього періоду, і повторного розрахунку нових значень.

Ключові слова: ймовірно-фізичний розподіл відмов; апіорний і апостеріорний аналіз; механо-фізико-хімічні параметри; експоненціальний розподіл; визначальні випробування; математична статистика; експериментальна оцінка.

Kozlyuk I. O. Kovalenko Y. B.

METHODS OF PRODUCTS RELIABILITY EVALUATION BASED ON THE RESULTS OF TESTS AND OPERATION

The article proposes methods for determining the characteristics of reliability indicators of functional systems of aviation equipment, based on the use of the exponential distribution, the probability-physical model of failures. This evaluation of the method determines the confidence probability and the accuracy of the evaluation of the reliability index of functional systems. The assessment of the level of reliability and its analysis are presented based on the results of tests and diagnostics of aviation equipment. Also, the data processing reliability components of aircraft for a certain period of operation. The initial data processing, the initial stage of evaluation, was performed for the initial and subsequent period of operation. The processing of the next stage was carried out by adding to the data volume of the preliminary stage new data obtained at the stage estimated by adjusting the content of the previous period database and recalculating the new value.

Keywords: statistically physical distribution of failures; a priori and a posteriori analysis; mechanical- physical-chemical parameters; exponential distribution; determinative tests; mathematical statistics; experimental evaluation.

Козлюк И. О. Коваленко Ю. Б.

МЕТОДЫ ОЦЕНКИ ПОКАЗАТЕЛЕЙ НАДЕЖНОСТИ АВИАЦИОННОЙ ТЕХНИКИ ПО РЕЗУЛЬТАТАМ ИСПЫТАНИЙ И ТЕХНИЧЕСКОЙ ДИАГНОСТИКИ

В статье предлагаются методы определения характеристик показателей надежности функциональных систем авиационной техники, основанные на использовании экспоненциального распределения, вероятностно-физической модели отказов. Данная оценка метода, определяет доверительную вероятность и точность оценки показателя надежности функциональных систем. Оценка уровня надежности и его анализ представлен по результатам испытаний и диагностики авиационной техники. Также проведена обработка данных надежности комплектующих изделий воздушных судов за определенный период эксплуатации. Начальная обработка данных первичный этап оценки, была выполнена для начального и последующего периода эксплуатации. Обработка очередного этапа проводилась путем добавления к объему данных предварительного этапа новых данных, полученных на этапе, который оценивается корректировкой содержания базы данных предыдущего периода, и повторного расчета новых значений.

Ключевые слова: вероятностно-физическое распределение отказов; апіорний и апостеріорний аналіз; механо-фізико-хімічні параметри; експоненціальне розподілення; визначаючі випробування; математична статистика; експериментальна оцінка.

Стаття надійшла до редакції 03.09.2018 р.

Прийнято до друку 17.09.2018 р.

Рецензент – д-р техн. наук, проф. Конахович Г. Ф.

УДК 519.233.2: 621.391.83 (045)

DOI: 10.18372/2310-5461.39.13095

О. В. Соломенцев, д-р техн. наук, проф.
Національний авіаційний університет
orcid.org/0000-0002-3214-6384
e-mail: avsolomentsev@ukr.net

М. Ю. Заліський, канд. техн. наук
Національний авіаційний університет
orcid.org/0000-0002-1535-4384
e-mail: maximus2812@ukr.net

Т. С. Герасименко, аспірантка
Національний авіаційний університет
orcid.org/0000-0002-8504-2001
e-mail: milusga@meta.ua

АНАЛІЗ ЕФЕКТИВНОСТІ ПРОЦЕДУРИ ВИЯВЛЕННЯ РОЗЛАДНАННЯ В СИСТЕМАХ ЕКСПЛУАТАЦІЇ НАЗЕМНИХ ЗАСОБІВ АЕРОНАВІГАЦІЇ

Вступ

Під час аеронавігаційного обслуговування використовують наземні засоби аеронавігації (НЗА), до яких належать засоби зв'язку, навігації, спостереження, автоматизовані системи керування повітряним рухом тощо. Надійна робота НЗА значною мірою залежить від функціонування системи експлуатації НЗА. Ця система містить такі складові як: засоби НЗА; технологічні процеси (технічного обслуговування, ремонту, продовження ресурсу, наземних та льотних перевірок тощо); персонал; нормативні документи та ін. В процесі функціонування НЗА та їх систем експлуатації (СЕ) можливі випадки невідповідності встановленим вимогам, що може призвести до зайвих витрат, порушення безпеки та нерегулярності польотів тощо.

У загальному випадку процеси зміни технічного стану НЗА та інших елементів СЕ є нестаціонарними та випадковими. При цьому можуть бути інтервали квазістаціонарності, що мають різні значення статистичних розподілів або параметрів на відповідних інтервалах. Причинами нестабільності процесів зміни стану НЗА та інших елементів СЕ можуть бути: процеси старіння елементної бази НЗА, несвоєчасні та невірні керуючі впливи з боку адміністративних органів, умови навколишнього середовища, неякісні дії обслуговуючого персоналу, причини обумовлені електромагнітною несумісністю тощо. В науково-технічній літературі задачі пов'язані з

аналізом нестаціонарних процесів розглядаються як задачі дослідження «розладнання» [1; 2].

Розробка процедур виявлення розладнання в реалізації процесів, що характеризують стан НЗА та їх СЕ, є актуальною науково-практичною задачею, оскільки додаткова інформація щодо тренду нестаціонарного процесу дає можливість сформулювати та своєчасно реалізувати керуючі та запобіжні дії персоналом СЕ.

Аналіз публікацій

Питання розробки та модернізації системи експлуатації технічних систем широко висвітлюються в науково-технічній літературі [3]. Предметними сферами є задачі аналізу цілісності аеронавігаційної системи, аналізу телеметричних даних, деградаційних процесів технічних комплексів, виявлення кіберзагроз тощо.

При цьому питання статистичної обробки нестаціонарних випадкових процесів змін технічного стану НЗА та складових СЕ приділяється недостатньо уваги. Це може негативно вплинути на ефективність СЕ та надійність роботи НЗА, а далі знизити ефективність системи аеронавігаційного обслуговування. Крім того, під час аналізу стратегій технічного обслуговування НЗА за станом з контролем рівня надійності в [4–8] не розглядають моделі опису трендів змін стану НЗА у вигляді показників надійності.

Постановка проблеми

Узагальнена структурна схема СЕ може бути представлена у наступному вигляді (рис. 1).

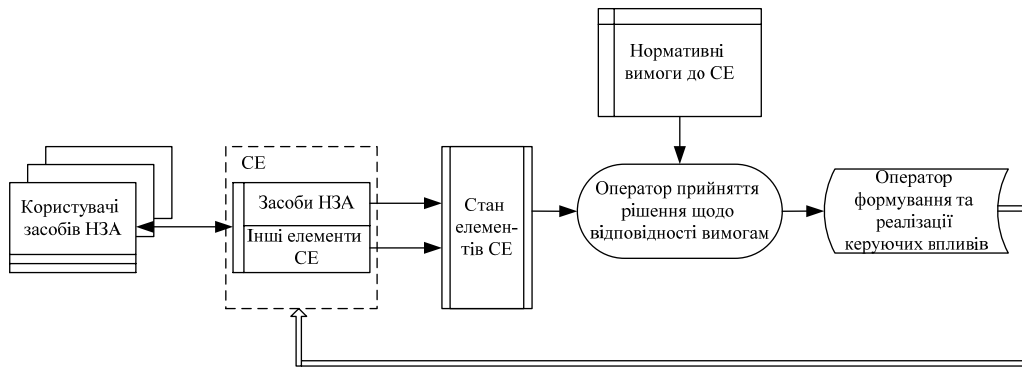


Рис. 1. Узагальнена структурна схема CE

Структурна схема характеризує CE як систему формування та реалізації керуючих впливів щодо НЗА та інших елементів CE з метою забезпечення надійності роботи НЗА та ефективності функціонування CE. Керуючі впливи повинні бути своєчасними та вірними для зменшення ризиків та можливих витрат, обумовлених випадками зміни технічного стану НЗА та інших елементів CE. Відомо, що для цього доцільно використовувати процедури прогнозування стану об'єктів керування. При цьому прогнозування є ефективним у разі справедливості гіпотези щодо збіжності моделей розвитку трендів на етапах збору даних та в межах періоду екстраполяції. Якщо розглядати моделі трендів визначальних параметрів та характеристик у вигляді моделей з розладнанням, тоді для забезпечення ефективності процедур прогнозування доцільно використовувати процедури визначення фактів розладнання та оцінки параметрів їх протікання.

Основними моментами під час розгляду процедур виявлення є моделі даних, що підлягають обробці, методи синтезу та аналізу ефективності процедур, синтез процедури обробки даних та її аналіз, показники та критерії ефективності. У рамках такого методичного підходу в статті вирішується задача синтезу та аналізу процедури виявлення розладнання в тренді нестационарного випадкового процесу, що характеризує зміни стану засобу НЗА для заданої моделі опису випадкового процесу.

Сформулюємо математичну постановку задачі дослідження на рівні функціоналів та операторів. У загальному випадку показник ефективності CE може бути визначений як функціонал типу

$$Ef = f(t_d, t_{\Sigma}, D, P_{fa}, U, C / \vec{A}),$$

де \vec{A} — це множина алгоритмів статистичної обробки експлуатаційних даних, у тому числі виявлення розладнання; t_d — це інтервал часу від моменту виникнення розладнання до момен-

ту його виявлення; t_{Σ} — інтервал спостереження; D — імовірність правильного виявлення; P_{fa} — імовірність хибної тривоги; U — обчислювальна складність алгоритму обробки даних; C — функція втрат за рахунок несвоєчасного виявлення розладнання.

Завданням цього дослідження є синтез такої процедури виявлення розладнання, яка забезпечить максимум показника ефективності для випадку заданих вимог до параметрів D , P_{fa} , t_d та U . Інакше кажучи, необхідно забезпечити

$$Ef = \sup(0 \leq Ef \leq 1 \forall \vec{A} : t_d \leq t_d^*, D \geq D^*, P_{fa} \leq P_{fa}^*),$$

де t_d^* , D^* , P_{fa}^* — вимоги до відповідних параметрів.

Синтез процедури виявлення розладнання в тренді нестационарного випадкового процесу

Технічний стан окремого НЗА можна розглядати з точки зору змін визначальних параметрів, що характеризують функціональну придатність НЗА або зміну показників надійності.

Такий розгляд відповідає відомим стратегіям технічного обслуговування (ТО): а) стратегія ТО за станом з контролем визначальних параметрів; б) стратегія ТО за станом з контролем рівня надійності НЗА. Існує також третя стратегія ТО за напрацюванням. В цьому випадку розглядаємо стратегію ТО за станом з контролем рівня надійності НЗА.

До показників надійності відносять середнє напрацювання на відмову, середній час відновлення, коефіцієнт технічного використання, коефіцієнт готовності тощо.

Розглянемо випадок, коли зміна технічного стану НЗА характеризується залежністю інтенсивності відмов в часовому просторі. В науково-технічній літературі розглядають такі моделі нестационарних процесів, що описують надійнісні властивості обладнання [3]: стрибкоподібна, лінійна та квадратична моделі.

Розглянемо стрибкоподібну модель зміни інтенсивності відмов. Вибіркова сукупність, що підлягає обробці, формується у вигляді напрацювань між відмовами t . Вважаємо, що відліки t_i на інтервалі спостереження є незалежними випадковими величинами.

Розглянемо задачу виявлення розладнання. Гіпотезі H_0 — у тренді зміни випадкового процесу відсутнє розладнання, тоді щільність розподілу імовірностей (ЩРІ) має такий вигляд:

$$f_1(t_i) = \lambda^{(0)} e^{-\lambda^{(0)} t_i}, \text{ для } i = \overline{1, n}.$$

де t_i — величина напрацювання на відмову для i -го відліку; $\lambda^{(0)}$ — інтенсивність відмов на інтервалі, де розладнання немає; n — обсяг напрацювань, що підлягають обробленню в процедурі виявлення розладнання.

Альтернативі H_1 — у тренді зміни випадкового процесу має місце розладнання, що виникає на k -му кроці спостереження. Маємо ЩРІ у вигляді:

$$f_2(t_i) = \begin{cases} \lambda^{(0)} e^{-\lambda^{(0)} t_i}, & \text{для } i = \overline{1, k-1}, \\ a^{(0)} \lambda^{(0)} e^{-a^{(0)} \lambda^{(0)} t_i}, & \text{для } i = \overline{k, n}, \end{cases}$$

де $a^{(0)}$ — коефіцієнт зміни інтенсивності відмов, який необхідно виявляти із заданим рівнем ефективності.

У такому варіанті параметри генеральної сукупності $a^{(0)}, \lambda^{(0)}, n$ мають бути відомими для забезпечення гарантованого рівня показників ефективності. Фактичні значення параметрів розподілів імовірностей $f_1(t)$ та $f_2(t)$ будуть пов'язані з поточною ефективністю та враховані при теоретичному аналізі та моделюванні під час формування вибіркової сукупності напрацювань t_i .

Синтез процедури виявлення факту розладнання виконаємо з використанням критерію Неймана–Пірсона для фіксованого обсягу вибірки n . Рішення про наявність або відсутність розладнання приймається після того як проведена обробка даних всієї вибірки обсягом n відліків (випадок з апостеріорним аналізом).

Відношення правдоподібності має вигляд:

$$\Lambda(\vec{t}_n, k, a^{(0)}) = \frac{\Phi(\vec{t}_n / H_1)}{\Phi(\vec{t}_n / H_0)};$$

$$\Phi(\vec{t}_n / H_1) = \prod_{i=1}^n f_2(t_i / H_1);$$

$$\Phi(\vec{t}_n / H_0) = \prod_{i=1}^n f_1(t_i / H_0),$$

де $\Phi(\vec{t}_n / H_1)$ — функція правдоподібності для H_1 ; $\Phi(\vec{t}_n / H_0)$ — функція правдоподібності для H_0 .

Тоді вираз для відношення правдоподібності набуде вигляду:

$$\begin{aligned} \Lambda(\vec{t}_n, k, a^{(0)}) &= \\ &= \frac{\prod_{i=k}^n f_2(t_i / H_1)}{\prod_{i=k}^n f_1(t_i / H_0)} = \frac{\prod_{i=k}^n a^{(0)} \lambda^{(0)} e^{-a^{(0)} \lambda^{(0)} t_i}}{\prod_{i=k}^n \lambda^{(0)} e^{-\lambda^{(0)} t_i}} = \\ &= a^{(0)n-k} e^{\lambda^{(0)}(1-a^{(0)}) \sum_{i=k}^n t_i}. \end{aligned}$$

Логарифм функції відношення правдоподібності:

$$\ln \Lambda(\vec{t}_n, k, a^{(0)}) = (n-k+1) \ln a^{(0)} + \lambda^{(0)}(1-a^{(0)}) \sum_{i=k}^n t_i.$$

Нехай $\theta(a^{(0)}, \vec{t}_n, \lambda^{(0)})$ — це вирішальна статистика, що залежить від обсягу вибірки n і параметрів $a^{(0)}, \lambda^{(0)}, k$. Тоді

$$\theta(a^{(0)}, \vec{t}_n, \lambda^{(0)}) = (n-k+1) \ln a^{(0)} + \lambda^{(0)}(1-a^{(0)}) \sum_{i=k}^n t_i.$$

Процедура виявлення розладнання полягає в такому — після обробки n відліків даних щодо напрацювання t_n згідно з виразом для $\theta(a^{(0)}, \vec{t}_n, \lambda^{(0)})$ формують масив значень вирішальної статистики для всієї сукупності можливих значень параметра k . Далі знаходять у цієї вибіркової сукупності максимальне значення θ_{\max} , яке порівнюють з порогом прийняття рішення V . Якщо $\theta_{\max} > V$, то приймається рішення про наявність розладнання.

Слід зазначити що процедура виявлення в такому вигляді строго кажучи не є оптимальною.

У праці [1] вважають, що алгоритми виявлення подібні тому, що розглядається є так звані алгоритми кумулятивних сум. Згідно з таким підходом максимальному значення вирішальної статистики відповідає значення k , коли об'єктивно відбулась зміна інтенсивності відмов.

Проаналізуємо залежність математичного сподівання від поточного значення k . При цьому вираз для математичного сподівання та дисперсії вирішальної статистики $\theta(a^{(0)}, \vec{t}_n, \lambda^{(0)})$ для випадку коли $k < k_0$ має вигляд:

$$\begin{aligned} m_1(\theta) &= (n-k+1) \ln \frac{a^{(0)} \lambda^{(0)}}{\lambda^{(0)}} - \\ &= (a^{(0)} \lambda^{(0)} - \lambda^{(0)}) \left[(k_0 - k) \frac{1}{\lambda^{(0)}} + (n - k_0 + 1) \frac{1}{a \lambda^{(0)}} \right]; \end{aligned}$$

$$\mu_2(\theta) = \left(a^{(0)}\lambda^{(0)} - \lambda^{(0)}\right)^2 \left[\left(k_0 - k\right) \left(\frac{1}{\lambda^{(0)}}\right)^2 + \right. \\ \left. + (n - k_0 + 1) \left(\frac{1}{a\lambda^{(0)}}\right)^2 \right].$$

Дійсно частина сумарної статистики відліків t_i обсягом $k_0 - k$ величин пов'язана з гіпотезою H_0 . Інша частина сумарної статистики t_i обсягом $n - k_0 + 1$ величин пов'язана з альтернативою H_1 .

Вираз для математичного сподівання та дисперсії вирішальної статистики $\theta(a^{(0)}, \bar{t}_n, \lambda^{(0)})$ для випадку, коли $k = k_0$ має вигляд

$$m_1(\theta) = (n - k_0 + 1) \ln \frac{a^{(0)}\lambda^{(0)}}{\lambda^{(0)}} - \\ - (a^{(0)}\lambda^{(0)} - \lambda^{(0)}) (n - k_0 + 1) \frac{1}{a\lambda^{(0)}}.$$

$$\mu_2(\theta) = \left(a^{(0)}\lambda^{(0)} - \lambda^{(0)}\right)^2 (n - k_0 + 1) \left(\frac{1}{a\lambda^{(0)}}\right)^2.$$

У даному випадку частина сумарної статистики відліків t_i обсягом $n - k_0 + 1$ величин пов'язана з альтернативою H_1 .

Вираз для математичного сподівання та дисперсії вирішальної статистики $\theta(a^{(0)}, \bar{t}_n, \lambda^{(0)})$ для випадку, коли $k > k_0$ має вигляд

$$m_1(\theta) = (n - k + 1) \ln \frac{a^{(0)}\lambda^{(0)}}{\lambda^{(0)}} - \\ - (a^{(0)}\lambda^{(0)} - \lambda^{(0)}) (n - k + 1) \frac{1}{a\lambda^{(0)}}.$$

$$\mu_2(\theta) = \left(a^{(0)}\lambda^{(0)} - \lambda^{(0)}\right)^2 (n - k + 1) \left(\frac{1}{a\lambda^{(0)}}\right)^2.$$

У цьому випадку частина сумарної статистики відліків t_i обсягом $n - k + 1$ величин пов'язана з альтернативою H_1 і обсяг сумарної статистики залежить від конкретного поточного значення параметру k . Результати розрахунків за формулами для математичних сподівань та дисперсій, а також результати моделювання (точкові оцінки математичних сподівань та дисперсій) представлені в таблиці.

На рис. 2 та 3 наведені результати розрахунку та точкові оцінки за результатами статистичного моделювання для залежності математичного сподівання та дисперсії від параметру k .

На рис. 2 та 3 прямокутниками представлені оцінки, отримані за результатами моделювання.

Таблиця

Числові значення математичного сподівання та дисперсії

Набір параметрів	$\lambda = 2 \cdot 10^{-6}, a = 2, n = 50, k_0 = 25$						
k	3	10	17	25	33	40	50
$m_1(\theta)$	-1.73	0.42	2.57	5.02	3.48	2.12	0.19
$m_1^*(\theta)$	-1.798	0.366	2.52	4.999	3.449	2.086	0.187
$\mu_2(\theta)$	28.5	21.5	14.5	6.5	4.5	2.75	0.25
$\mu_2^*(\theta)$	29.618	22.224	14.608	6.501	4.538	2.848	0.261

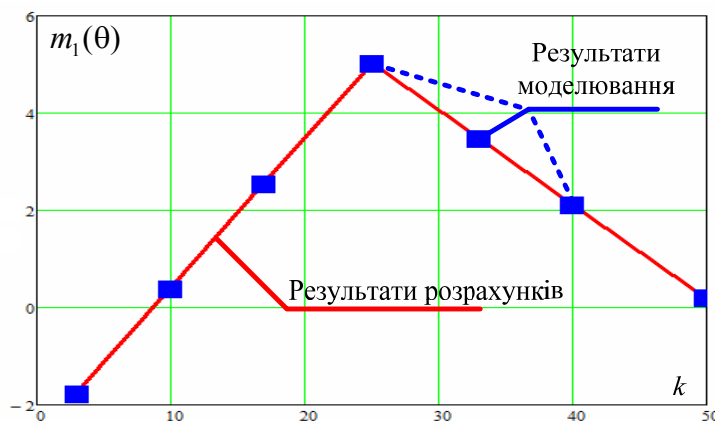


Рис. 2. Графіки залежності математичного сподівання вирішальної статистики θ від параметру k за даними таблиці

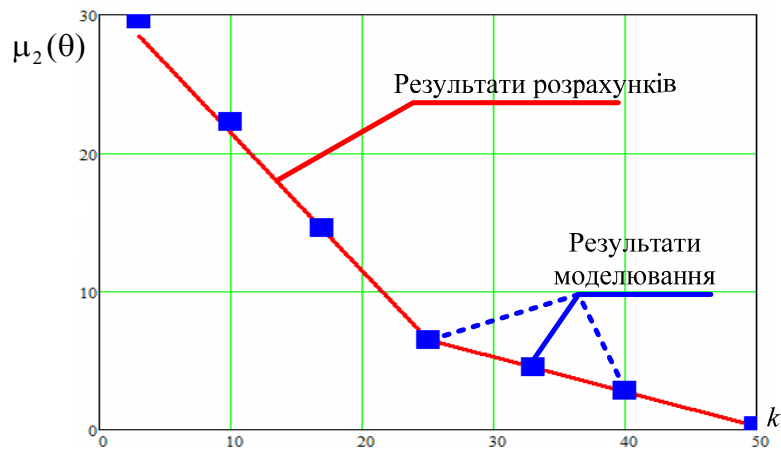


Рис. 3. Графіки залежності дисперсії вирішальної статистики θ від параметру k за даними таблиці

Результати розрахунків свідчать, що максимум на рис. 2 відповідає відліку, коли $k = k_0$. Аналіз рис. 3 показує, що дисперсія монотонно спадає. У цілому, результати статистичного моделювання свідчать про вірність теоретичних розрахунків.

Сформуємо процедуру прийняття рішення про наявність розладнання шляхом порівняння максимального значення статистики з порогом рішення V .

Аналіз ефективності процедури виявлення розладнання в тренді нестационарного випадкового процесу

Аналіз ефективності — це процес розрахунку чисельних значень показників ефективності. У даному випадку, коли розгуляється варіант апостеріорного аналізу вихідної статистики приймаємо, що показниками ефективності процедури виявлення розладнання є: імовірність помилки першого роду α (прийняття альтернативи H_1 , коли справедлива гіпотеза H_0); імовірність помилки другого роду β (прийняття гіпотези H_0 коли справедлива H_1).

У статті розглядається рішення задачі виявлення розладнання для випадку простої гіпотези та альтернативи, тобто заданий рівень імовірності правильного виявлення розладнання $D^{(0)}$ необхідно забезпечити для відомого рівня $\lambda^{(0)}$, обсягу вибірки n , параметрів $a^{(0)}$ та k_0 . З урахуванням цих умов визначають поріг рішення V . Далі пропонується розглянути три варіанти розрахунку характеристик виявлення: 1) для заданого порога V , що розраховано для параметрів генеральної сукупності $\lambda^{(0)}$, k_0 , n визначають залежність $D(a)$ від поточного значення параметра a (тобто з'ясуємо наскільки чутливою є процедура виявлення до змін в рівні λ); 2) для заданого порога V , що розраховано для параметрів генеральної

сукупності $\lambda^{(0)}$, $a^{(0)}$, n визначають залежність $D(k)$ від реального значення номера шага k , коли відбулося розладнання тренду нестационарного процесу (тобто з'ясуємо наскільки чутливою є процедура виявлення від початкового моменту розладнання); 3) для заданого порога V , що розраховано для параметрів генеральної сукупності $\lambda^{(0)}$, k_0 , n , $a^{(0)}$ визначають залежність D від поточного значення параметра a та реального значення номера шага k , коли відбулося розладнання тренду нестационарного процесу (тобто розраховують двовимірну ймовірність виявлення розладнання $D(a, k)$).

Під час аналізу ефективності зробимо два припущення:

1. Поріг рішення V розраховуємо для параметрів генеральної сукупності $a^{(0)}$, $\lambda^{(0)}$, n в точці k_0 , де математичне сподівання вирішальної статистики $\theta(a^{(0)}, \bar{t}_n, \lambda^{(0)})$ є максимальною величиною.

2. Вважаємо, що ЦРІ вирішальної статистики при цьому є нормальною.

Розглянемо випадок побудови характеристики $D(a)$. Імовірність правильного виявлення розраховується за формулою:

$$D = 1 - \int_{-\infty}^V N(\theta/H_1) d\theta,$$

де $N(\theta/H_1)$ — нормальна ЦРІ вирішальної статистики для альтернативи H_1 .

Інтеграл у цьому виразі представимо у вигляді інтеграла ймовірностей Лапласа $\Phi(\cdot)$:

$$\beta = \Phi\left(\frac{V - m_1(\theta/H_1)}{\sigma(\theta/H_1)}\right).$$

Поріг прийняття рішення визначається за формулою:

$$V = m_1(\theta/H_1) + \sigma(\theta/H_1)\Phi^{-1}(\beta),$$

де $\Phi^{-1}(\beta)$ — зворотна функція.

Знаючи значення порогу прийняття рішень V може бути розрахована ймовірність помилки першого роду:

$$\alpha = 1 - \int_{-\infty}^V N(\theta/H_0) d\theta,$$

де $N(\theta/H_0)$ — нормальна ЩРІ вирішальної статистики для гіпотези H_0 .

Для даних із таблиці та значення $\beta^{(0)} = 0.1$ поріг прийняття рішення дорівнює $V^{(0)} = 1.756$ та ймовірність помилки першого роду $\alpha = 0.028$.

На рис. 4 наведені характеристика виявлення розладнання для даних із таблиці, отриманих у результаті аналітичних розрахунків та на основі статистичного моделювання.

Порівняння графіків із рис. 4 свідчать про правильність зроблених розрахунків.

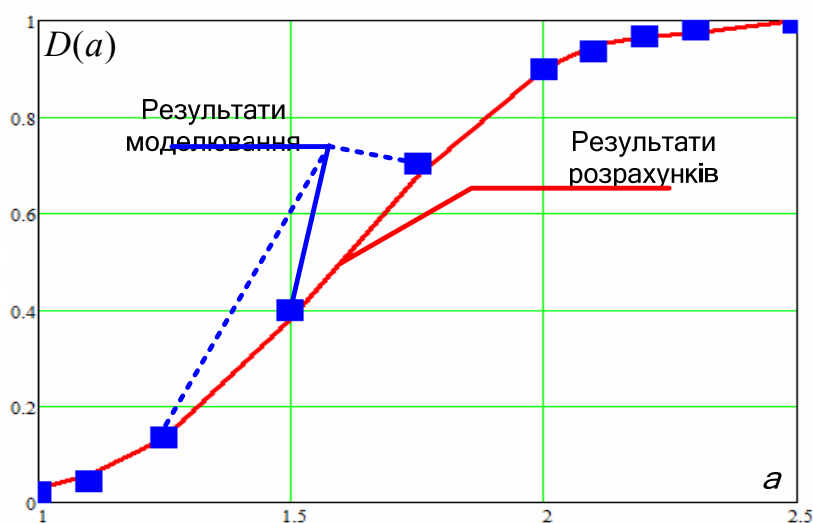


Рис. 4. Характеристики виявлення розладнання

Висновок

Алгоритми виявлення розладнання в реалізаціях нестационарних процесів, що характеризують зміни станів НЗА та інших елементів Системи експлуатації відіграють значну роль під час формування та реалізації своєчасних та правильних дій з точки зору забезпечення ефективності використання НЗА та ефективності функціонування їх СЕ.

Для розглянутої процедури виявлення вирішені задачі синтезу та аналізу ефективності процедури.

Результати статистичного моделювання підтвердили правильність теоретичних результатів.

Результати дослідження можуть бути використані під час проектування та модернізації систем експлуатації наземних засобів аеронавігації цивільної авіації.

ЛІТЕРАТУРА

1. **Жиглявский А. А.** Обнаружение разладки случайных процессов в задачах радиотехники / А. А. Жиглявский, А. Е. Красковский. — Л.: Издательство ЛУ, 1988. — 224 с.

2. **Tartakovsky A., Nikiforov I., Basseville M.** Sequential analysis. Hypothesis testing and change-point detection, Taylor & Francis Group, 2015, 580 p.

3. **Solomentsev O. V.** UAV operation system designing / O. V. Solomentsev, V. H. Melkumyan, M. Yu. Zaliskyi, M. M. Asanov // IEEE 3rd International Conference on Actual Problems of Unmanned Air Vehicles Developments (APUAVD), October 13-15, 2015 (Kyiv, Ukraine), Proceedings. — P. 95–98.

4. **Nakagawa T.** Maintenance theory of reliability, London: Springer-Verlag, 2005. — 270 p.

5. **Goncharenko A. V.** Optimal UAV maintenance periodicity obtained on the multi-optional basis / A. V. Goncharenko // IEEE 4th International Conference on Actual Problems of Unmanned Air Vehicles Developments (APUAVD), October 17-19, 2017, Proceedings. — P. 65–68.

6. **Dhillon B. S.** Maintainability, Maintenance, and Reliability for Engineers. New York: Taylor & Francis Group, 2006. — 214 p.

7. **Rausand M.** System Reliability Theory: Models, Statistical Methods and Applications. New York: John Wiley & Sons, Inc. — 2004. — 458 p.

8. **Smith D. J.** Reliability, Maintainability and Risk. Practical methods for engineers. London: Elsevier, 2005. — 365 p.

Соломенцев О. В., Заліський М. Ю., Герасименко Т. С.

АНАЛІЗ ЕФЕКТИВНОСТІ ПРОЦЕДУРИ ВИЯВЛЕННЯ РОЗЛАДНАННЯ В СИСТЕМАХ ЕКСПЛУАТАЦІЇ НАЗЕМНИХ ЗАСОБІВ АЕРОНАВІГАЦІЇ

Наземні засоби аеронавігації використовуються для забезпечення безпеки та регулярності польотів повітряних суден. До цих засобів відносять обладнання зв'язку, навігації та спостереження. Надійність наземних засобів аеронавігації в значній мірі визначається ефективністю системи їх експлуатації. Стаття присвячена вирішенню задачі синтезу та аналізу алгоритму виявлення розладнання нестационарного випадкового процесу. Первинними даними для обробки є напрацювання на відмову обладнання для експоненціальної моделі, яка на різних ділянках квазістационарності має різні інтенсивності відмов. Синтез процедури виявлення виконаний на основі критерію Неймана–Пірсона з фіксованим обсягом вибірки. Під час аналізу ефективності алгоритму виконані теоретичні розрахунки порогів прийняття рішення, на основі яких були розраховані характеристики виявлення розладнання. Статистичне моделювання на основі методу Монте-Карло підтвердило правильність теоретичних розрахунків.

Ключові слова: системи експлуатації; статистична обробка даних; погіршення технічного стану; розладнання; нестационарні процеси.

Solomentsev O. V., Zaliskyi M. Yu., Herasymenko T. S.

EFFICIENCY ANALYSIS FOR CHANGEPOINT DETECTION PROCEDURE IN OPERATION SYSTEMS OF GROUND NAVIGATION EQUIPMENT

Ground-based navigation equipment is used to ensure the safety and regularity of aircraft flights. This equipment includes communication, navigation and surveillance devices. The reliability of navigation equipment is determined by the efficiency of their operation system. The article is devoted to solving the problem of synthesis and analysis of the algorithm for changepoint detection for non-stationary random process. The input data for processing are equipment's times between failures in case of exponential model, which has different failure rates at different intervals of the quasi-stationarity. The synthesis of the detection procedure is based on Neyman-Pearson criterion with a fixed sample size. During the analysis of the algorithm's efficiency the theoretical calculations of the decision thresholds were made, on the basis of which the characteristics of changepoint detection were calculated. The statistical modeling based on the Monte Carlo method confirmed the correctness of theoretical calculations.

Keywords: operation system; statistical data processing; technical state deterioration; changepoint; non-stationary processes.

Соломенцев А. В., Залиский М. Ю., Герасименко Т. С.

АНАЛИЗ ЭФФЕКТИВНОСТИ ПРОЦЕДУРЫ ОБНАРУЖЕНИЯ РАЗЛАДКИ В СИСТЕМАХ ЭКСПЛУАТАЦИИ НАЗЕМНЫХ СРЕДСТВ АЭРОНАВИГАЦИИ

Наземные средства аэронавигации используются для обеспечения безопасности и регулярности полетов воздушных судов. К этим средствам относят оборудования связи, навигации и наблюдения. Надежность наземных средств аэронавигации в значительной степени определяется эффективностью системы их эксплуатации. Статья посвящена решению задачи синтеза и анализа алгоритма обнаружения разладки нестационарного случайного процесса. Первичными данными для обработки являются наработки на отказ оборудования для экспоненциальной модели, которая на разных участках квазистационарности имеет разные интенсивности отказов. Синтез процедуры выявления выполнен на основе критерия Неймана-Пирсона с фиксированным объемом выборки. При анализе эффективности алгоритма выполнены теоретические расчеты порогов принятия решения, на основе которых были рассчитаны характеристики обнаружения разладки. Статистическое моделирование на основе метода Монте-Карло подтвердило правильность теоретических расчетов.

Ключевые слова: системы эксплуатации; статистическая обработка данных; ухудшение технического состояния; разладка; нестационарные процессы.

Стаття надійшла до редакції 09.09.2018 р.

Прийнято до друку 20.09.2018 р.

Рецензент – д-р техн. наук, проф. Конахович Г. Ф.

Н. С. Ремез, д-р. техн. наук, проф.
НТУУ «КПІ імені Ігоря Сікорського»
orcid.org/0000-0002-8646-6527
e-mail: nataly.remez@gmail.com

А. Г. Бойко, аспірант
НТУУ «КПІ імені Ігоря Сікорського»
orcid.org/0000-0003-3561-6289
e-mail: bag0911@ukr.net

ЕКОЛОГІЧНА САНІТАРІЯ ЯК ЗАСІБ ПОКРАЩЕННЯ ГРУНТОВО-РОСЛИННОГО ПОКРИВУ

Вступ

З давніх часів ґрунт відіграє важливу роль для людства, бо саме він є невід'ємною складовою введення сільського господарства. Дана галузь економіки представлена майже у всіх країнах світу, бо вирішує першочергові потреби людини в їжі. Але на сьогодні існує проблема деградації ґрунтового-рослинного покриву, що зумовлює зниження сільськогосподарського виробництва. Даний процес розпочався ще близько 10 тис. років тому, а саме з появи землеробства. За оцінками спеціалістів, на той час площа придатних для сільськогосподарського використання земель складала близько 4,5 млрд га, а в наш час таких земель залишилося близько 2,5 млрд га [1, с. 93]. Це свідчить про те, що у середньому щороку втрачалось до 200 тис. га придатних для ведення сільського господарства земель.

Однією з основних причин появи ерозії та опустелювання, що знижує сільськогосподарське виробництво, є втрата у ньому поживних речовин. Фермери, вирішуючи цю проблему, застосовують мінеральні добрива — це неорганічні

сполуки, що містять поживні речовини, необхідні для нормального розвитку рослин [2, с. 1]. За рахунок того, що вони є зручними у транспортуванні, зберіганні та розпиленні, їх широко використовують на практиці по всьому світі. Але довгострокове використання цих добрив призводить до утворення несприятливих наслідків, наприклад, підкислення, що з'явилося внаслідок зменшення вмісту органічного вуглецю, тобто вирішення однієї проблеми спричинило появу нових.

Аналіз останніх досліджень і публікацій

Поліпшити сьогоденне становище ґрунтового-рослинного покриву може екологічна санітарія, що являється основною частиною концепції стійкої санітарії, яка захищає та підтримує людське здоров'я, не викликає екологічної деградації або виснаження ресурсної бази, є технічно та інституційно відповідною, економічно життєздатною та соціально прийнятною [3, с. 27]. Вона впроваджує замкнений цикл перетворення відходів життєдіяльності людей на органічні добрива, який представлений на рисунку.



Замкнений цикл застосування продуктів життєдіяльності людей

Технічним засобом такого перетворення є екосанітарні туалети, які зручно використовувати у сільській місцевості як децентралізовані системи. Вони розподіляють потоки відходів життєдіяльності на рідку та тверду фракції (урину та фекальні маси) без додавання води або дуже її малої кількості. Далі ці фракції можна використовувати після обробки, яка одразу відбувається завдяки конструкції екосанітарного туалету, як органічне добриво для сільськогосподарських рослинних культур, що сприяє збагаченню ґрунту поживними речовинами та збільшенню врожайності, тобто поліпшує становище ґрунтово-рослинного покриву.

У свою чергу ця технологія спонукає зменшенню використання водних ресурсів, знижуючи рівень забруднення води, що призводить до позитивного внеску в зберігання прісної води на планеті у цілому. Такий результат був отриманий у дослідженні, яке зазначено у праці [4, с. 160]. Також до переваг даного технологічного рішення належать: відсутність величезної інфраструктури, що зумовлює короткотривалі терміни будівництва, порівняно з централізованим водопостачанням; економія коштів на водопостачання та водовідведення, будівництво нецентралізованих систем утилізації «чорних» вод; зниження рівня захворювання населення на розлад сечовивідної системи, загроз виникнення інфекційних і онкологічних захворювань, спричиненими незадовільним станом санітарії.

Мета статті (постановка завдання)

Висвітлення способу отримання органічного добрива за рахунок застосування екологічної санітарії, підкреслення необхідності враховувати співвідношення макроелементів при внесенні цих добрив як важливого показника підвищення росту рослинної культури, побудова взаємної залежності вмісту мікроелементів у органічному добриві.

Виклад основного матеріалу

Об'єктом дослідження став вміст макроелементів: азоту, фосфору та калію, в органічних добривах, отриманих унаслідок використання екологічної санітарії. Ці три елемента живлення є необхідними для рослин у великих кількостях

(на відміну від мікроелементів), оскільки вони входять у більш складні молекули, які є «будівельним матеріалом» для тканин і органів самої рослини [5, с. 1]. Азот відповідає за ріст рослин, впливаючи на її урожайність. Фосфор здійснює суттєвий вплив на фізіологію рослини, оскільки відіграє вирішальну роль у розподілі енергії. Калій бере участь у ферментативних процесах і в розподілі води рослинної культури, що сприяє стійкості рослин до спеки, холоду чи посухи, тобто відіграє роль у адаптаційних процесах. Отже, макроелементи є важливими для живлення рослин, що і визначає вагому роль їх вмісту в органічних добривах і застосуванні останніх у сільському господарстві.

Уміст макроелементів у твердій фракції відходів життєдіяльності людей нижче, ніж у рідкій, оскільки у фекалії вони в основному перебувають у зв'язаній органічній формі. Тому більшість поживних речовин знаходяться в урині, котра також має оптимальне для багатьох рослин співвідношення мікроелементів — завдяки цій особливості її доцільно використовувати як добриво. Із-за цього саме рідку фракцію відходів життєдіяльності людей розглянуто в дослідженні.

У свою чергу, урина містить велику кількість азоту, близько 81,5 % [6, с. 12], за яким встановлюють об'єми додавання даної фракції до ґрунту для росту рослин. При цьому є важливим входження й інших макроелементів до її складу, таких як фосфору та калію, тому, говорячи про урину як добриво, надають інформацію про вміст цих поживних елементів у ній.

Результати даного аналізу показали, що у деяких джерелах літератури, наприклад [3, с. 31], [7, с. 1], зустрічається вміст азоту та фосфору, не наводячи показники вмісту калію, хоча останній являється не менш вагомим поживним елементом для рослини, а також його кількість є більшою у складі відходів життєдіяльності людей, ніж фосфору. Таким чином, виникає потреба у знаходженні залежності виходу калію від вмісту азоту та фосфору в рідкій фракції відходів життєдіяльності людини.

Дані про вміст макроелементів у рідкій фракції по різних країнах світу [8, с. 625] наведено в таблиці.

Уміст макроелементів у рідкій фракції відходів життєдіяльності людей

Країна	Уміст азоту, кг/рік	Уміст фосфору, кг/рік	Уміст калію, кг/рік
Китай	3,5	0,4	1,3
Гаїті	1,9	0,2	0,9
Індія	2,3	0,3	1,1
Південна Африка	3,0	0,3	1,2
Уганда	2,2	0,3	1,0

Методом найменших квадратів було знайдено рівняння множинної регресії. Для цього за вищенаведеними даними побудовано систему лінійних алгебричних рівнянь:

$$\begin{cases} 5,5 = 5a_0 + 12,9a_1 + 1,5a_2; \\ 14,59 = 12,9a_0 + 34,99a_1 + 4,03a_2; \\ 1,69 = 1,5a_0 + 4,03a_1 + 0,47a_2. \end{cases} \quad (1)$$

Розв'язавши дану систему методом Гаусса, отримано такі значення: $a_0 = 499/1070$; $a_1 = 20/107$; $a_2 = 54/107$. У результаті розрахунку рівняння зв'язку, яке визначає залежність результативної ознаки (вмісту калію) від двох факторів (вмісту азоту та фосфору), було записано у такому вигляді:

$$y_x = 0,4664 + 0,1869x_1 + 0,5047x_2. \quad (2)$$

Щільність зв'язку двох факторів — вмісту азоту та фосфору в урині, та результативної ознаки — виходу калію, підтверджено високим коефіцієнтом кореляції:

$$\begin{aligned} R_{y,x_1,x_2} &= \\ &= \sqrt{\frac{0,97^2 + 0,89^2 - 2 \cdot 0,97 \cdot 0,89 \cdot 0,87}{1 - 0,87^2}} = 0,97. \end{aligned} \quad (3)$$

Висновки

Екологічна санітарія може здійснити вагомий вплив на покращення становища ґрунтово-рослинного покриву, бо дозволяє вирішити проблеми утилізації відходів життєдіяльності людей у сільській місцевості, створюючи з них продукт споживання, а саме: органічне добриво, яке містить значну кількість поживних речовин, зокрема макроелементів, що необхідні для рослин у великих кількостях. Встановлена залежність вмісту калію в органічному добриві рідкої фракції відходів життєдіяльності людей від вмісту азоту та фосфору. За отриманими результатами розрахунків обчислений коефіцієнт множинної кореляції (3) свідчить про залежність на 97 % вмісту калію у рідкій фракції відходів життєдіяльності людей від вмісту азоту та фосфору, тому знайдене рівняння даного зв'язку у вигляді (2) має практичне значення для розрахунку, тобто, маючи дані вмісту азоту та фосфору, можна розрахувати вміст калію.

Перспективи подальших досліджень

Проведене дослідження дозволяє більш детально звернути увагу на зв'язок макроелементів, які складають хімічний вміст органічних добрив, отриманих внаслідок застосування еко-санітарних туалетів, що спонукає на більш глибокі дослідження зв'язків поживних речовин у даному продукті споживання, а також їх взаємодії та впливу, який вони можуть здійснювати, на ґрунтово-рослинний покрив.

ЛІТЕРАТУРА

1. Царик Л. П. Екологія: підруч. для 10 кл. загальноосвіт. навч. закл.: профіл. рівень / Л. П. Царик, П. Л. Царик, І. М. Вітенко. — 2-ге вид. — К. : Генеза, 2011. — 240 с.
2. Мінеральні добрива [Електронний ресурс] // Науково-популярний блог. — 2014. — Режим доступу до ресурсу: <http://www.npblog.com.ua/index.php/himiya/mineralni-dobryva.html>
3. Бодік І. Стійка санітарія в Центральній та Східній Європі — відповідаючи потребам малих та середніх населених пунктів / І. Бодік, Р. Пітер. — Словакія: UVTIP Nitra, 2008. — 90 с.
4. Ремез Н. С. Зменшення споживання води за рахунок альтернативного знешкодження фізіологічних відходів людини / Н. С. Ремез, А. Г. Бойко // Наукоємні технології, 2017 — № 2 (34) — С. 158–161, doi:10.18372/2310-5461.34.11614 (ukr).
5. Елементи живлення рослин: Макроелементи, Мезоелементи та Мікроелементи [Електронний ресурс] // АГРОЛАВКА.— 2015. — Режим доступу: <https://agrolavka.com.ua/a189520-elementi-zhivlennya-roslin.html>.
6. Сухий туалет — це серйозно! — Київ: Всеукраїнська екологічна громадська організація «МАМА-86», 2007. — 15 с.
7. Hill G. B. An Evaluation of Waterless Human Waste Management Systems at North American Public Remote Sites / G. B. Hill. — Vancouver: University of British Columbia, 2013. — 173 p.
8. Jönsson H. / Adapting the nutrient content of urine and faeces in different countries using FAO and Swedish data // H. Jönsson, B. Vinnerås; Proceedings of the 2nd International Symposium on Ecological Sanitation, incorporating the 1st IWA specialist group conference on sustainable sanitation, 7th-11th April 2003. — Lübeck: Ecosan — Closing the loop, 2004. — Pp. 623–626.

Ремез Н. С., Бойко А. Г.

ЕКОЛОГІЧНА САНІТАРІЯ ЯК ЗАСІБ ПОКРАЩЕННЯ ҐРУНТОВО-РОСЛИННОГО ПОКРИВУ

У статті розглянуто проблему деградації ґрунтового-рослинного покриву через виснаження ґрунту недбалим веденням людством сільського господарства. Це зумовлює здійснення кроків вирішення проблем у даній галузі, оскільки обрана сфера діяльності стосується першочергових потреб населення в їжі, що розкриває актуальність обраної теми. У роботі висвітлено один із шляхів поліпшення становища ґрунтового-рослинного покриву завдяки застосуванню екологічної санітарії, яка, насамперед, може поліпшити екологічні показники використання деяких необхідних для нашого життя ресурсів, зокрема замкнений цикл використання відходів життєдіяльності людей, який запроваджує дана технологія, дозволяє зменшити забруднення води. Акцентом роботи є вміст поживних елементів у органічному добриві, отриманому внаслідок застосування екологічної санітарії. Ці знання необхідні для внесення добрив до ґрунту, що зумовлює практичне використання проведеного дослідження.

Ключові слова: ґрунтового-рослинний покрив; екологічна санітарія; екосанітарний туалет; відходи життєдіяльності людей; макроелементи.

Remez N. S., Boiko A. G.

ECOLOGICAL SANITATION AS A WAY OF IMPROVING THE SOIL-VEGETATION COVER

This article is about the problem of degradation of soil-vegetation cover due to the depletion of soil by careless farming of mankind. This determines to implementation of steps to solve problems in this area, because the chosen field of activity relates to the priority needs of the population in food, which reveals the relevance of the chosen topic. The one of the ways to improve soil-vegetation cover through the use of ecological sanitation highlights in the work. The ecological sanitation, first of all, can improve the environmental indicators of some necessary resources for our lives, in particular the closed cycle of waste of human life, which introduces by this technology, helps to reduce water pollution. The emphasis is the content of nutrients in organic fertilizers, which obtained as a result of ecological sanitation use. This knowledge is necessary for applying fertilizers to the soil, this is predetermines the practical use of the research.

Keywords: soil-vegetation cover, ecological sanitation; eco-sanitary toilet; waste of human life; macroelements.

Ремез Н. С., Бойко А. Г.

ЭКОЛОГИЧЕСКАЯ САНИТАРИЯ КАК СРЕДСТВО УЛУЧШЕНИЯ ПОЧВЕННО-РАСТИТЕЛЬНОГО ПОКРОВА

В статье рассмотрена проблема деградации почвенно-растительного покрова из-за истощения почвы небрежным ведением человечеством сельского хозяйства. Это приводит к осуществлению шагов решения проблем в данной области, так как выбранная сфера деятельности касается первоочередных потребностей населения в пище, что раскрывает актуальность выбранной темы. В работе освещен один из путей улучшения состояния почвенно-растительного покрова благодаря применению экологической санитарии, которая, в первую очередь, может улучшить экологические показатели использования некоторых необходимых для нашей жизни ресурсов, в частности замкнутый цикл использования отходов жизнедеятельности людей, который вводит данная технология, позволяет уменьшить загрязнение воды. Акцентом работы является содержание питательных элементов в органическом удобрении, полученном в результате применения экологической санитарии. Эти знания необходимы для внесения удобрений в почву, что приводит к практическому использованию проведенного исследования.

Ключевые слова: почвенно-растительный покров; экологическая санитария; экосанитарный туалет; отходы жизнедеятельности людей; макроэлементы.

Стаття надійшла до редакції 26.06.2018 р.
Прийнято до друку 27.08.2018 р.
Рецензент – д-р техн. наук, проф. Ткачук К. К.

К. І. Капітанчук, канд. техн. наук, доц.
Національний авіаційний університет
orcid.org/0000-0003-3605-0977
e-mail: k.kapitanchuk@ukr.net

М. П. Андрійшин, канд. техн. наук, доц.
Національний авіаційний університет
orcid.org/0000-0002-4439-3526
e-mail: andriishinmp@gmail.com

РОЗРАХУНОК ПОДОВЖЕННЯ ЕНЕРГОПОГЛИНАЛЬНОГО ЕЛЕМЕНТА МОРСЬКОЇ ХВИЛЬОВОЇ ЕЛЕКТРОСТАНЦІЇ ПРИ ТРАНСФОРМАЦІЇ СПРАЛІ У ПЛОЩИНУ

Вступ

Потужність хвиль Світового океану оцінюється приблизно у 10...90 млрд кВт, з яких 2,7 млрд кВт може бути реально використано людством. Енергія морської хвилі, впливаючи на поверхні тіл, може нести не тільки руйнівну дію, але також здатна створювати механічну роботу по пересовуванню цих поверхонь.

Уміння реалізовувати енергію морської хвилі в любий інший вид роботи для відтворення нетрадиційного джерела енергії — найважливіше завдання.

Сучасний рівень розвитку техніки дозволяє використати енергію морських хвиль лише у прибережних зонах, де вона в середньому складає величину у 80 кВт/м. Потужність морських хвиль Чорного та Азовського морів ще менша і складає величину чуть більше 40 кВт/м [1].

Таким чином, з кожного погонного метра фронту хвилі можна відтворити електроенергію для забезпечення 8 будинків, а з фронту у 1000 м можна відтворити електроенергію для 10 енергоємних об'єктів, що знаходяться як на рейді, так і на березі, наприклад, плавзасоби, маяки, локатори та ін.

Питома потужність хвиль, яка відтворюється на великих глибинах при значній віддаленості від берега, на порядок вища за питому потужність хвиль у прибережній зоні. Крім того, процес перетворення енергії морських хвиль в електричну енергію у цьому випадку не пов'язаний з руйнівним екологічним впливом на природу. Тому використання енергії морських хвиль на «глибокій воді» є вкрай необхідними, а наукові розробки для створення хвильових електростанцій — актуальними.

Аналіз останніх досліджень і публікацій

Використання енергії морських хвиль поки що знаходиться на стадії створення дослідних установок різних конструкцій. Вони класифікуються залежно від типу носія, призначення, розташування, способу перетворення енергії, діапазону висот хвиль. У сучасних хвильових установках енергія хвиль може або безпосередньо перетворюватись в енергію обертання валу генератора, або слугувати основою для привода турбіни з генератором на одному валу з нею. Всі відомі хвильові установки складаються з п'яти основних частин: несної конструкції, робочого органу — енергопоглинального елемента, робочого тіла, силового перетворювача та системи кріплення [2; 3].

За ініціативою НВФ «Крок-1» (м. Київ), спільними зусиллями науковців Національного авіаційного університету, Національного університету кораблебудування ім. адмірала Макарова та Інституту гідромеханіки НАН України створена, виготовлена та випробувана конструкція хвильової електростанції (ХЕС) з гнучким енергопоглинальним елементом (рис. 1), яка принципово відрізняється від усіх сучасних аналогів [4].

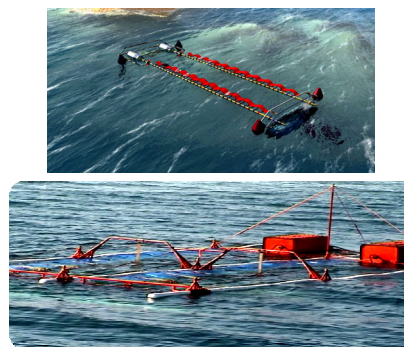


Рис. 1. Загальний вид хвильової електростанції НВФ «Крок-1»

Унікальність установки в тому, що вона здатна ефективно працювати за будь-якого коливання морської поверхні за рахунок саморегулювання форми енергопоглинального елемента під впливом хвиль і занурення станції на необхідну глибину відповідно до погодних умов на поверхні. Собівартість електричної енергії, яка створюється станцією, не перевищує 0,1 цент/кВт.

Мета статті (постановка завдання)

Існує проблема з визначенням довжини енергопоглинального елемента, оскільки при заданих габаритних параметрах хвильової електростанції, його форма трансформується від спіралі на розрахунковому режимі до гофрованої поверхні з переходом у форму стрічки при незбуреному стані поверхні моря. При цьому довжина енергопоглинального елемента повинна збільшуватися. Проблема розв'язана [4] шляхом використання окремих фрагментів (ласти) енергопоглинального елемента з перекриттям їх в навхрест у момент монтажу на величину подовження. На розрахунковому режимі роботи хвильової електростанції це подовження повинно бути використано для трансформації енергопоглинального елемента у вид спіралі.

Постановка завдання на дослідження

Для визначення довжини енергопоглинального елемента хвильової електростанції, при зміні збурення поверхні моря, необхідно розробити методику розрахунку залежно від умов подальшої експлуатації станції.

Результати досліджень

Форма та геометричні розміри залежать від траєкторії руху кожної окремо взятої елементарної точки поверхні енергопоглинального елемента станції в процесі переміщення її під впливом енергії морської хвилі. Кожна окремо взята елементарна точка поверхні бере участь у складному русі вздовж поверхні циліндра з радіусом R_i і поверхні хвилі з амплітудою a та довжиною хвилі λ [2; 3]. Необхідно визначити основні рівняння траєкторії руху та зміни площі контакту енергопоглинального елемента при коливанні поверхні моря для визначення габаритних та енергетичних параметрів станції.

За умови $R_i \leq a$ траєкторія руху являє собою складну гвинтову лінію, рівняння якої представимо у вигляді:

$$y_i = R_i \sin \varphi, \quad z_i = R_i \cos \varphi, \quad x = \lambda \varphi / 2\pi. \quad (1)$$

Виключимо з системи рівнянь (1) параметр φ шляхом уведення в квадрат перших двох рівнянь з подальшим їх додаванням. Дістанемо

$$y_i^2 + z_i^2 = R_i^2. \quad (2)$$

Рівняння (2) являє собою рівняння циліндра, на якому розташована гвинтова лінія траєкторії руху елементарної точки.

Поділивши послідовно друге рівняння в системі (1) на перше і підставивши результат в значення φ із третього рівняння, знайдемо рівняння поверхні, на якій розташована гвинтова лінія:

$$\frac{y_i}{z_i} = \operatorname{tg} \frac{2\pi x}{\lambda}. \quad (3)$$

Рівняння (3) описує синусоїдальну гвинтову поверхню — синусоїдальний гелікоїд. Таким чином, пошукова гвинтова лінія є лінією перетину поверхонь (2) та (3).

Відстань, яку проходить елементарна точка вздовж гвинтової лінії за повний період від 0 до 2π , визначається довжиною дуги за формулою:

$$l_i = \int_0^{2\pi} \sqrt{(dx/d\varphi)^2 + (dy/d\varphi)^2 + (dz/d\varphi)^2} d\varphi = \sqrt{(2\pi R_i)^2 + \lambda^2} \quad (4)$$

Кривизна кривої в довільній точці лінії є змінною за радіусом кривизни:

$$R^* = R_i [1 + (\lambda/2\pi R_i)^2]. \quad (5)$$

Оскільки енергопоглинальний елемент розглядається у вигляді стрічки кінцевої ширини b [2, 3], то можна констатувати, що зовнішні (найбільш віддалені від центра обертання) точки за повний період проходять відстань

$$l_R = \int_0^{2\pi} \sqrt{(dx/d\varphi)^2 + (dy/d\varphi)^2 + (dz/d\varphi)^2} d\varphi = \sqrt{(2\pi R)^2 + \lambda^2}, \quad (6)$$

а внутрішні (найбільш наближені до центра обертання) точки за повний період проходять відстань

$$l_{R-b} = \int_0^{2\pi} \sqrt{(dx/d\varphi)^2 + (dy/d\varphi)^2 + (dz/d\varphi)^2} d\varphi = \sqrt{[2\pi(R-b)]^2 + \lambda^2}. \quad (7)$$

Отже, енергопоглинальний елемент повинен мати довжину поверхні контакту з хвилею в $l_R/\lambda = \sqrt{[2\pi(R-b)/\lambda]^2 + 1}$ раз більшу за довжину хвилі λ та забезпечити подовження зовнішньої сторони стрічки відносно внутрішньої без зміни її ширини на величину

$$\Delta l = l_R \left(1 - \sqrt{1 - 8\pi^2 RbA/l_R^2} \right), \quad (8)$$

де $A = 1 - b/2R$.

За умови $R_i = a$ без перевероту ця величина зменшиться вдвічі, а за умови $Ri \geq a$ відбувається режим «гойдалки» за якого подовження зовніш-

ньої сторони стрічки відносно внутрішньої визначається за формулою

$$\Delta l = 2\phi l_R \left(1 - \sqrt{1 - 8\pi^2 R b A / l_R^2} \right) / \pi. \quad (9)$$

Величина Δl визначає мінімальну кількість напрямних n_n на довжині хвилі λ енергопоглинального елемента з умови

$$l_{гр} = \Delta l / n_n, \quad (10)$$

де $l_{гр}$ — граничнодопустиме подовження матеріалу (з умови міцності), що з'єднує окремі частини енергопоглинального елемента.

Відмітимо, що робоча частина енергопоглинального елемента визначається з умови його зачеплення з валом через напрямні, тому довжина робочої частини менша за довжину хвилі за умови перпендикулярного розташування до фронту хвилі.

За умови $Ri \geq a$ довжина робочої частини становить половину довжина хвилі. При заданій величині довжини енергетичної станції L кількість робочих частин складає величину L/λ .

У прямокутній системі координат $Oxyz$ поверхня (3) синусоїдального гелікоїда обмежена циліндричними поверхнями з радіусами $R-b$ та R . Під дією знакозмінного за часом t тиску морської хвилі в кожній точці даної поверхні визначений вектор сили

$$\vec{F} = p_y(x, y, z, t)\vec{i} + p_z(x, y, z, t)\vec{j} + p_x(x, y, z, t)\vec{k}, \quad (11)$$

де p_y — неперервна функція надлишкового тиску стовпа води.

Величина сили визначається за допомогою обчислення поверхового інтеграла векторного поля \vec{F} через поверхню синусоїдального гелікоїда при $t = 0$ з подальшим пересовуванням величини \vec{F} в часі

$$\iint \vec{F} ndS = \iint p_y dydz + p_z dzdx + p_x dxdy. \quad (12)$$

Таким чином, для визначення величини сили, що діє у довільній точці поверхні енергопоглинального елемента, необхідно знати закони змінення площ проекцій її поверхонь уздовж всіх осей.

Відмітимо, що енергопоглинальний елемент займає площу поверхонь (3) синусоїдального гелікоїда в межах від $R-b$ до R . Різниця площ від проекцій зовнішнього та внутрішнього радіусів гелікоїда на всі поверхні системи координат є проекції площі енергопоглинального елемента на ці поверхні.

Результати розрахунку величини Δl при умові $R_i = a$ без перевероту, при $\lambda/a = 7$ та різних величинах R/b показані на рис. 2, а.

Відзначимо, що подовження збільшується пропорційно радіусу. Зі збільшенням величини R/b нахил залежності збільшується за степеневу залежністю.

Розглянемо змінення площі проекцій енергопоглинального елемента на всі поверхні прямокутної системи координат у межах однієї довжини хвилі при фіксованому часі.

Проекція поверхні енергопоглинального елемента на поверхню Ozx обмежена поверхнями:

$$y = R \cos(2\pi/\lambda)(x - ct),$$

$$y = (R - b) \cos(2\pi/\lambda)(x - ct). \quad (13)$$

Площа проекції енергопоглинального елемента на поверхню Ozx визначається у вигляді

$$S_y = \int_{x_1}^{x_2} R \cos(2\pi/\lambda)(x - ct) dx -$$

$$- \int_{x_1}^{x_2} (R - b) \cos(2\pi/\lambda)(x - ct) dx =$$

$$= \int_{x_1}^{x_2} b \cos(2\pi/\lambda)(x - ct) dx.$$

де x_1, x_2 — границі діапазону змінення параметра x в межах λ .

Оскільки енергопоглинальний елемент виконує обертальний рух, то підінтегральна функція залежить від параметра ϕ і для розв'язання представленої інтеграла необхідно використовувати формулу Лейбніца.

Для енергопоглинального елемента діапазон змінення параметра x в межах λ (від x_1 до x_2) визначається з умови контакту напрямних з валом через храповик. При цьому величина ϕ змінюється за законом:

$$\phi = \arcsin(y/R) = \arcsin \frac{a}{R} \sin(2\pi/\lambda)x. \quad (14)$$

За умови $R_i = a$ діапазон змінення параметрів хвилі і руху енергопоглинального елемента визначають як: $x_1 = \lambda/4$, $x_2 = 3\lambda/4$ та $\phi_1 = \pi/2$, $\phi_2 = 3\pi/2$.

У цьому випадку

$$S_y = \int_{\lambda/4}^{3\lambda/4} b \cos \phi dx = b(2 + \cos \phi_1 + \cos \phi_2) \frac{\lambda}{2\pi} = \frac{b\lambda}{\pi}. \quad (15)$$

Таким чином, закон змінення площі S_y вздовж x представляється у вигляді

$$dS_y/dx = b \cos \phi. \quad (16)$$

Результати розрахунку змінення площі проекції енергопоглинального елемента на поверхню Ozx вздовж радіусу за різних величин R/b представлені на рис. 2, б.

Відзначимо, що площа проекції енергопоглинального елемента на поверхню Ozx збільшується пропорційно ширині та квадрату радіусу.

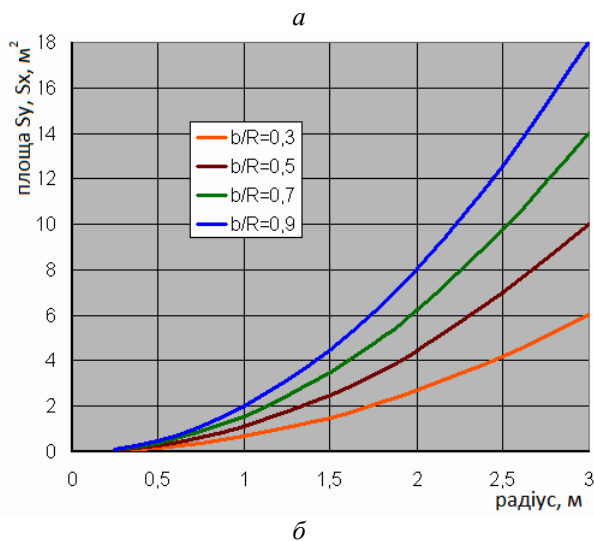
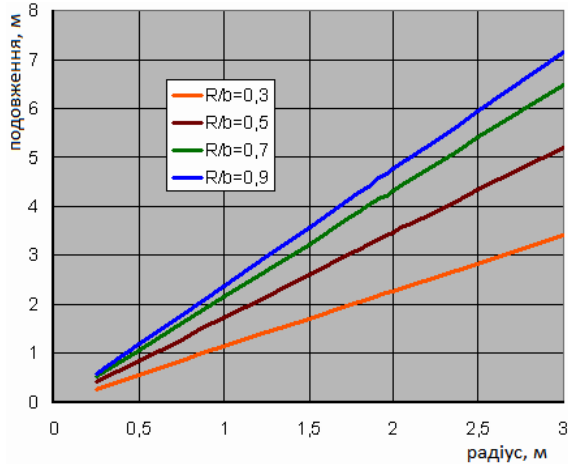


Рис. 2. Залежність подовження зовнішньої сторони стрічки без перевероту (а) відносно внутрішньої сторони без зміни її ширини та площі проекцій енергопоглинального елемента на площину Ozx та Oyx (б) від радіуса за умови $R = a$, $\lambda/a = 7$ та різних величин R/b

Проекція поверхні енергопоглинального елемента на поверхню Oyx обмежена поверхнями:

$$y = R \sin(2\pi/\lambda)(x - ct),$$

$$y = (R - b) \sin(2\pi/\lambda)(x - ct). \quad (17)$$

Площа проекції енергопоглинального елемента на поверхню Oyx визначається як

$$S_z = \int_{x_1}^{x_2} R \sin(2\pi/\lambda)(x - ct) dx -$$

$$- \int_{x_1}^{x_2} (R - b) \sin(2\pi/\lambda)(x - ct) dx =$$

$$= \int_{x_1}^{x_2} b \sin(2\pi/\lambda)(x - ct) dx.$$

За умови $R_i = a$

$$S_z = \int_{\lambda/4}^{3\lambda/4} b \sin \varphi dx = -b(\sin \varphi_1 + |\sin \varphi_2|) \frac{\lambda}{2\pi} = \frac{b\lambda}{\pi}. \quad (18)$$

Відзначимо, що величина площі проекції енергопоглинального елемента на поверхню Oyx за умови $R_i = a$ дорівнює за величиною площі проекції енергопоглинального елемента на поверхню Ozx .

Тому для визначення величини площі проекції енергопоглинального елемента на поверхню Oyx можна використовувати дані рис. 2, б.

Таким чином, закон змінення площі S_z вздовж осі x представляється у вигляді

$$dS_z / dx = b \sin \varphi. \quad (19)$$

Проекція поверхні енергопоглинального елемента на поверхню Oyx являє собою поверхню, яка створюється шляхом перетину цієї поверхні двома циліндричними поверхнями з радіусами R та $R - b$. При умові $R_i \leq a$ вона являє собою кільце, а при $R_i > a$ тільки його частину.

Площа проекції енергопоглинального елемента на поверхню Oyx визначається у вигляді

$$S_x = \int_{\varphi_1}^{\varphi_2} \frac{Rb}{4} A d\varphi. \quad (20)$$

При $R_i \leq a$ $S_x = \frac{\pi Rb}{4} A. \quad (21)$

Під час роботи енергопоглинального елемента в режимі «гойдалки»

$$S_x = \frac{\varphi Rb}{2} A. \quad (22)$$

Таким чином, закон змінення площі S_x за φ представляється у вигляді

$$dS_x / d\varphi = \frac{Rb}{2} A. \quad (23)$$

Висновки

Аналіз змінення подовження зовнішньої сторони стрічки без перевероту та площі проекцій енергопоглинального елемента на поверхні прямокутної системи координат показує, що:

1. Подовження збільшується пропорційно радіусу. Зі збільшенням величини R/b нахил залежності збільшується за степеневою залежністю

2. За умови $R_i = a$ площі проекцій енергопоглинального елемента на поверхню Oyx та поверхню Ozx рівні. Величини їх прямо пропорційні ширині енергопоглинального елемента та довжині хвилі.

3. Площа Sz змінюється вздовж осі x від максимального значення, що дорівнює величині $Szi/dx = b$ при $x_1 = \lambda/4$, до нуля при $x = \lambda/2$, а потім знов збільшується до максимального значення при $x_2 = 3\lambda/4$.

4. Площа Sy змінюється вздовж осі x асиметрично площі Sz при аналогічних зміненнях.

5. При $R_i \leq a$ площа Sx не залежить від x .

Перспективи подальших досліджень. Для визначення конструкційних матеріалів основних елементів хвильової електростанції, що здатні довготривало витримувати руйнівну силу морських хвиль, проведення розрахунків з визначення габаритних та енергетичних параметрів станції необхідно вивчити закони змінення складових сил та моментів, що діють на поверхню енергопоглинального елемента.

ЛІТЕРАТУРА

1. Енергетичні ресурси та потоки. — К. : Українські енциклопедичні знання, 2003. — 472 С.

2. **Ищенко Ю. А.** Захват энергии взаимодействия глубин и волн Мирового океана // Энергия, 2003, №3. — С. 28–36.

3. **Капітанчук К. І., Овсянкін В. В.** Досвід розробки та впровадження хвильової електричної станції // Матеріали XIV Міжнар. наук.-тех. конф. АС Промислова гідраліка і пневматика. — Одеса: «ГЛОБУС-ПРЕС». — 2013. — С. 126–127.

4. Патент України № 56481. Пристрій для перетворення енергії хвиль водної поверхні. МКИ7 F03B13/12.

5. **Греков П. І., Капітанчук К. І., Овсянкін В. В.** Методика розрахунку глибини занурення морської енергетичної станції при збільшенні висоти хвиль // Вісник НАУ, 2006. — №4(30). — С. 166–168. doi.org/10.18372/2306-1472.30.1399.

6. **Капітанчук К. І., Сотников А. В., Овсянкін В. В.** Один из путей независимого энергетического обеспечения подразделений Вооруженных Сил Украины приморского базирования // Арсенал—ХІ. — 2007. — № 1. — С. 37–41.

7. **Капітанчук К. І., Овсянкін В. В., Ластивка І. А., Греков П. І.** Децентрализованное энергетическое обеспечение жизнедеятельности населения прибрежных областей Украины // Васильків — південні ворота столиці : тези доповідей І Всеукр. наук.-практ. конф. — Ч. І. — Васильків: вид-во Сяйво, 2008. — С. 87–88.

Капітанчук К. І., Андрійшин М. П.

РОЗРАХУНОК ПОДОВЖЕННЯ ЕНЕРГОПОГЛИНАЛЬНОГО ЕЛЕМЕНТА МОРСЬКОЇ ХВИЛЬОВОЇ ЕЛЕКТРОСТАНЦІЇ ТРАНСФОРМАЦІЇ СПІРАЛІ У ПЛОЩИНУ

Використання енергії морських хвиль на «глибокій воді» є вкрай необхідним, а наукові розробки для створення хвильових електростанцій — актуальним. Унікальність створеної установки в тому, що вона здатна ефективно працювати при будь-якому коливанні морської поверхні за рахунок саморегулювання форми енергопоглинального елемента під впливом хвиль і занурення станції на необхідну глибину відповідно до погодних умов на поверхні.

Проблема руйнівного впливу хвиль в період різкого змінення сили вітру і, відповідно, амплітуди коливань поверхні моря, вирішено шляхом підтоплення станції на глибину, де коливання хвиль відповідають розрахунковим значенням, без зміни режиму роботи самої станції. При цьому споживачі стабільно отримують заявлену кількість електроенергії за любых погодних умов.

Існує проблема з визначенням довжини енергопоглинального елемента, оскільки при заданих габаритних параметрах хвильової електростанції, його форма трансформується від спіралі на розрахунковому режимі до гофрованої поверхні з переходом у форму стрічки при незбуреному стані поверхні моря. При цьому довжина енергопоглинального елемента збільшується.

Уперше визначено довжину енергопоглинального елемента хвильової електростанції при зміні збурення поверхні та розроблено методику розрахунку залежно від умов експлуатації станції. Виявлено змінення подовження зовнішньої сторони стрічки без перевероту та площ проєкцій енергопоглинального елемента на поверхні прямокутної системи координат.

Ключові слова: морські хвилі, електростанція, енергопоглинальний елемент, подовження, площа.

Капитанчук К. И., Андрийшин М. П.

CALCULATIONS OF POWER TAKE-OFF ELEMENT LENGTH VALUES DURING SHAPE CHANGES CAUSED BY WEATHER

Use of sea wave's energy is the extremely necessary. Scientific development for creation of wave energy stations, are extraordinarily actual. Wave energy station is able effectively to work at any size of waves, because form of energetically absorbing element is self-regulated under the action of waves.

Problem of destructive influence of waves during sharp change of force of a wind and as consequence of amplitude of fluctuations of a surface of the sea, it is solved by flooding is a energetically absorbing element and a platform of

station on depth, where fluctuations of waves correspond to calculation values, without change of an operating mode of the station. Thus consumers stably receive the declared quantity of the electric power.

In article for the first time calculations of power take-off element length dependencies of wave length during WEC submersion and algorithms of such calculations are presented. Changes of length in power take-off element on working surface are in belt form are accounted for.

Keywords: waves energy, wave energy converter, power take-off element modifications

Капитанчук К. И., Андришин М. П.

РАСЧЕТ УДЛИНЕНИЯ ЭНЕРГОПОГЛОЩАЮЩЕГО ЭЛЕМЕНТА МОРСКОЙ ВОЛНОВОЙ ЭЛЕКТРОСТАНЦИИ ПРИ ТРАНСФОРМАЦИИ СПИРАЛИ В ПЛОСКОСТЬ

Использование энергии морских волн на «глубокой воде» является крайне необходимым, а научные разработки по созданию волновых электростанций — актуальными. Уникальность созданной установки состоит в том, что она способна эффективно работать при любом колебании морской поверхности за счет саморегулирования формы энергопоглощающего элемента под воздействием волн и погружения станции на необходимую глубину в соответствии с погодными условиями на поверхности.

Проблема разрушительного воздействия волн в период резкого изменения силы ветра и, соответственно, амплитуды колебаний поверхности моря, решена путем подтопления энергопоглощающего элемента и платформы станции на глубину, где колебания волн соответствуют расчетным значениям, без изменения режима работы самой станции. При этом потребители стабильно получают заявленное количество электроэнергии при любых погодных условиях.

Существует проблема с определением длины энергопоглощающего элемента, так как при заданных габаритных параметрах волновой электростанции, его форма трансформируется от спирали на расчетном режиме до гофрированной поверхности с переходом у форму ленты при невозбужденном состоянии поверхности моря. При этом длина энергопоглощающего элемента увеличивается.

Впервые определено длину энергопоглощающего элемента волновой электростанции при изменении возбужденности поверхности моря и создана методика расчета в зависимости от условий эксплуатации станции. Выявлено изменение удлинения внешней стороны ленты без переворота та площади проекций энергопоглощающего элемента на поверхности прямоугольной системы координат.

Ключевые слова: морские волны, электростанция, энергопоглощающий элемент, удлинение площадь

Стаття надійшла до редакції 26.06. 2018 р.
Прийнято до друку 27.08.2018 р.
Рецензент — канд. техн. наук, доц. Єнчев С. В.