UDC 004.7.056 **doi: 10.32620/reks.2021.4.12**

O. MOROZOVA[1], A. NICHEPORUK[2], A. TETSKYI[1], V. TKACHOV[3]

[1] ***National Aerospace University "Kharkiv aviation institute", Ukraine***
[2] ***Khmelnytskyi National University, Ukraine***
[3] ***Kharkiv National University of Radio Electronics, Ukraine***

METHODS AND TECHNOLOGIES FOR ENSURING CYBERSECURITY OF INDUSTRIAL AND WEB-ORIENTED SYSTEMS AND NETWORKS

The subject matter *of the article is methods and technologies of ensuring the cybersecurity of industrial and web-oriented systems and networks, training of cybersecurity specialists during the acquisition of professional knowledge.* ***The purpose*** *of the article is to ensure the cybersecurity of industrial and web-oriented systems and networks by developing and implementing appropriate methodologies (concepts, principles, set of models, methods) and technologies in the industry, as well as in training the cybersecurity specialists during the acquisition of professional knowledge.* ***The problem*** *of developing models, methods, and technologies for ensuring the cybersecurity of mobile systems, web-oriented systems based on content management systems, virtual networks that provide their interaction, and a methodology for training cybersecurity specialists are formulated.* ***Based on the analysis the particular tasks*** *of developing convolutional neural network model, information technology methods and models for ensuring the cybersecurity of web-oriented systems and networks, a methodological framework of creating information technology, and a model of digital knowledge platform for use in the field of cybersecurity specialists training and security of industrial systems were formulated.* ***The basic theoretical decisions,*** *which underlie the construction of real industrial and web-oriented systems and networks, were described in the article.* ***The results of work*** *are increased reliability value of detecting the malware in the Android operating system, reduced rates of false positives, provided an allowable value of the success rate of attacks at a minimum cost, reduced time spent on building and rebuilding the structure of the virtual network, increased efficiency of cybersecurity specialists training and security of industrial systems. From the above, it is possible to* ***conclude*** *that the obtained results can be used in a line of existing and prospective approaches at designing difficult, complex, hybrid, technical, cyber-physical systems with a web-oriented interface for users and administrators.*

Keywords: *cybersecurity; Industry 4.0; web-based systems; computer networks; information technologies; professional education.*

Introduction

One of the promising areas in the sustainable development of modern information and communication technologies in ensuring the cybersecurity of industrial and web-oriented systems and networks [1-3]. This is since the Fourth Industrial Revolution is gradually transforming all spheres of social life, production, and economy, integrating their processes into cyberspace.

Along with the obvious benefits and conveniences of implementing industrial systems, many potential bottlenecks in the cybersecurity of such systems remain for attackers. All data that is created, transmitted, and processed has value for cybercriminals. Third-party access to data can lead to a variety of losses.

Any device connected to the network can be potentially vulnerable. An attacker can attack any part of the industrial system, including physical devices controlled by stationary or mobile operating systems, network services, web-based systems, cloud services.

Analysis of known works, projects, and systems operation experience, showed that the use of known similar solutions allows obtaining individual technical solutions in which there is no way to unification. In particular, the well-known approach [2] allows the creation of cybersecurity web-oriented systems models and methods built on the platform of such technology giants as Google, Amazon. But the main disadvantage of this approach, as well as similar approaches, is the impossibility of integrating the obtained solutions into existing information systems of previous generations.

Most technological processes in the industry are directly related to the use of virtualization technology [4, 5]. Indeed, the availability of a large number of different equipment creates additional difficulties for system administrators who maintain this infrastructure. To improve cybersecurity in the industry, thin clients are increasingly used as workplaces, for which communications take place according to a certain protocol (the protocol itself depends on the choice of a specific terminal

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

solution). An important issue is to ensure the cybersecurity of virtual networks, which are the medium for data transmission.

However, the creation and operation of any cybersecurity system are impossible without a highly qualified specialist in the field of cybersecurity. Today, professional education in Ukraine is in a constant state of reorganization and modernization, continuously adapting to the requirements of employers [6].

In particular, this applies to the mechanisms of training the specialists who must have the latest knowledge and competencies.

In the view of cybersecurity professionals' training, the main strategies for the development of professional education in the coming years include creating a viable system of lifelong training to achieve relevant knowledge and competencies. In addition, competencies are formed through the training of many different disciplines, the use of the mathematical apparatus in the educational process, and various methods of presenting knowledge, which is not always close to those needed for solving the problems of employers. As a result, one of the ways to train cybersecurity professionals is to introduce a dual system of vocational education.

Thus, the current area of research is the development and implementation of models, methods, and technologies for providing the cybersecurity of industrial and web-based systems and networks.

Concept of cybersecurity in industrial and web-oriented systems and networks

The objectives of the paper are ensuring the cybersecurity of industrial and web-oriented systems and networks by

- developing methods and technologies in the industry;
- creating set of models;
- construction of principles;
- formation of concept;
- developing and implementing appropriate methodologies and mechanisms training the cybersecurity specialists during the acquisition of professional knowledge.

The concept of the work is to ensure the cybersecurity of industrial and web-oriented systems and networks, taking into account the dynamics of modern cyberthreats to the hierarchical infrastructure of an enterprise.

To achieve this purpose, it is necessary to solve a set of the following tasks:

1. Develop a model of convolutional neural network based on the use of mixed data and a method for detecting malware in the Android operating system based on the processing of calls to the Application Programming Interface (API) and a set of permissions.

2. Develop information technology methods for ensuring the cybersecurity of web-oriented systems based on content management systems, which in turn are based on assessing the susceptibility to common attack scenarios and choosing the most effective means of protection.

3. Develop models and methods for ensuring the cybersecurity of virtual networks based on using the concept of virtual tunneling on the Internet.

4. Develop a methodological framework for creating information technology and a model of digital knowledge platform for use in the field of cybersecurity specialists training and security of industrial systems.

The main conditions of the proposed concept are the formulation and implementation of the following principles:

1. The principle of integrated consideration of threats to mobile and web-based systems due to the impact of malicious software based on the model of a convolutional neural network with the use of mixed data.

2. The principle of cybersecurity of web-based systems, based on the model in the form of an attack tree, which includes common scenarios of attacks on similar systems.

3. The principle of selection and implementation of measures to ensure the cybersecurity of industrial virtual networks, based on the model of a virtual network with a temporal criterion for scheduling service requests on the nodes.

4. The principle of creating an educational resource to support the processes of acquiring the professional knowledge in the field of training the specialists in cybersecurity and security of industrial systems, based on the model of a digital platform to support the processes of acquiring the professional knowledge.

To achieve these principles, it is necessary to get a set of the following methods considering research domains:

1. Method of technology for ensuring the cybersecurity of mobile systems.

2. Method for providing cybersecurity of web systems based on content management systems.

3. Method for ensuring the cybersecurity of virtual networks.

The above provisions allow us to develop the following list of the technologies which have been developed:

1. Information technology for ensuring the cybersecurity of mobile systems.

2. Information technology for formalizing educational processes in the field of cyber-security specialists training and security of industrial systems.

Thus, this concept includes the stages of developing the models, methods, and technologies for cybersecurity of industrial and web-based systems and networks.

Stage 1. Model and method of technology for ensuring cybersecurity of mobile systems

To ensure cybersecurity and increase the reliability of malware detection in systems run by the Android operating system, a method based on the involvement of the Convolution Neural Network (CNN) is proposed. Application Programming Interface (API) method calls and a set of permissions were used as data for CNN in our study.

No high-level action takes place without the involvement of API calls. Thus, performing their analysis, the behavior of the application can be represented through the sequence of API calls. Then the detection process may be focused on finding similarities (proximity) in the behavior of the studied program with knowledge of the typical behavior of existing malware.

The process of obtaining the program behavior or a sequence of API calls can be carried out in two ways: conversion and disassembling of the dex file.

Involving API calls allows representing all (or part) of the application's behavior. However, an equally important attribute that can complement the application's behavior and make it more complex is a set of permissions. The permissions mechanism restricts access to certain components or functionality of the application. All permissions used by the application are specified in the AndroidManifest.xml file. According to the previous research, the distribution of permissions in malware and useful applications is different. Thus, knowledge of obtaining permission may indicate a set of potential actions (sequences of API calls), the implementation of which will require granting permissions.

The proposed method [7] of detecting Android malware based on the use of mixed data for CNN consists of two main steps: creating or training a CNN model and applying the model to detect Android malware.

The training phase involves the creation of a CNN model on a set of training data and involves the implementation of three successive stages: data preprocessing, data vectorization, and CNN training.

The deployment phase involves pre-processing for a suspicious Android application, vectorizing its API calls and set of permissions, and classifying using the created neural network model.

The generalized structure of the malware detecting method in the Android operating system based on the processing of the application software interface calls and a set of permissions is given in [7] and used in this paper as a basis.

Let us analyze the main mechanisms for implementing the technology for ensuring the cybersecurity of mobile systems:

1) pre-processing: obtaining and presenting signs. First, we get a list of API calls and a set of permissions. This is necessary to reflect them in the behavior of the application. Therefore, in the process of receiving API calls, it is important to follow them, which will allow presenting the internal relationships between API calls. To get the behavior of the program, it is necessary to track all the ways the application runs. To do this, all service and activity objects contained in AndroidManifest.xml are added to the list of application behavior tracking start points. Next, all calls belonging to the Android, java, and javax libraries are added to the resulting list of all API calls. The algorithm for obtaining API calls is described in [8];

2) vectorization of API calls – representation of API calls in the form of real numbers. Achievement is possible by encoding each API call as a one-hot vector. All bits are encoded by the number 0, and the bit corresponding to the API call is encoded by the number 1. As the dimension of the vector increases, the number of bits with zero value increases rapidly. The word2vec method was used to obtain a compact vector representation of API calls [8];

3) vectorization of permissions. It is based on statistical information about the implementation of permission in malware and useful applications. The peculiarity is that the grouping of the bit sequence into tetrads is used. After that, the bit sequence of the input data will be converted into a coded bit sequence, where each value represents an integer in the range from 0 to 15, which is a vector representation of the resolutions set. To process the obtained feature vector by the neural network, its values are normalized to real numbers in the range from 0 to 1, by using min-max normalization [7, 8];

4) model of convolutional neural network. It is used to form a conclusion involving information about API method calls and a set of permissions from the Android application. This neural network can be represented as a container that has two separate convolutional neural networks, each of which processes its type of data (API calls or permissions). To ensure the nonlinearity of the decision, there is a hidden layer between the different layers. Obtaining the result is provided by the last layer consisting of two neurons. At the stage of neural network deployment, pre-processing of data for a suspicious Android application, vectorization of API calls, and a set of permissions and classification using the created neural network model are performed [8].

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

The choice of hyperparameters for the convolutional neural network and evaluation of the effectiveness of the method for detecting malware in Android is based on experimental studies, taking into account the proposed theoretical apparatus and practical results [7].

The results of experiments carried out to determine the effectiveness of the proposed method for detecting malware Android showed that the average value of "accuracy" was 0.94 (which almost coincides with the values of the metric F1 [7, 8]), while the level of false positives was 3.25 %.

Thus, the use of the proposed model of convolutional neural network has increased the reliability of detecting both new and known samples of malware in the Android operating system compared to known antivirus tools and has been further developed to refine its parameter.

Stage 2. Method for providing cybersecurity of web systems based on content management systems

The exploitation of system kernel vulnerabilities or functionality extension components is a common cause of successful attacks. Vulnerabilities can also be found in other software running on the server. Using insecure network protocols may compromise the integrity or confidentiality of information. Malicious software on a device that accesses content management system control functions can be used to compromise administrator credentials. The knowledge level of the administrator in the field of information security also plays an important role. This applies to the complexity of the password and its storage, and a high knowledge level reduces the risk of successful use of social engineering methods by attackers.

The purpose of this stage is to develop methods for assessing and ensuring the cybersecurity of web systems based on content management systems, which allows creating information technology to ensure the cybersecurity of content management systems. To achieve this purpose, it is necessary to solve the following tasks:

1) creating a model of attack scenarios in the form of an attack tree. The model is based on the principle of constructing a tree from top to bottom [9]. This construction uses the following scenarios: attacks with the disclosure of the existing administrator password; attacks with the creation of a new administrator; attacks bypassing authorization. The main event of this tree is to gain access to the functions of the content management system administrator. Estimation of the probability of the main event is possible using different types of scales [10];

2) parameterization of the model. There are two options: a scale of fuzzy logic variables and a five-point rating scale for selected indicators. When using a numerical scale, it is possible to obtain the evaluation result in the range [0; 1]. To do this, each base event is characterized by three (according to the number of evaluation indicators) scores on a scale from 1 to 5 [9, 10];

3) setting up a method to ensure the cybersecurity of content management systems. Assume the following as basic countermeasures: the use of two-factor authentication; training for staff; use of HTTPS; use of VPN; protection against the search of logins and passwords; setting complex passwords and non-standard logins; installation and configuration of the firewall. Combinations of these countermeasures are also possible. In contrast to the existing method of providing the cybersecurity of web systems based on content management systems [10], it can be minimizing the value of the attack success rate or minimize the cost of services;

4) development of information technology to ensure the cybersecurity of content management systems, which is presented in the form of IDEF0-diagram (Fig. 1).

IDEF0-diagrams contain the following elements:

– rectangles showing the functions (processes of information flow processing) performed when using an IT application;

– horizontal arrows displaying information flows, in particular input and output data;

– vertical arrows, directed from top to bottom, reflect the control inputs;

– vertical arrows, directed from the bottom up, reflect the tools to support decision-making used for the implementation of IT.

One of the scenarios for the application of elements of the developed IT is given in [9, 10].

Thus, this stage allowed to ensure the reliability of cybersecurity assessment of web systems based on content management systems through the use of audit results and penetration testing in parameterization. Using the method on the example of one installation of a content management system allowed to reduce the value of the attack success rate by 44.2 %.

Stage 3. Method for ensuring cybersecurity of virtual networks

The purpose of this stage is to create a method for ensuring the cybersecurity of virtual networks for secure interaction of subsystems of industrial and web-oriented systems and networks.

Assume that software agents (SAs) which analyze a virtual network must pass through all nodes of the virtual network, but the number of nodes is either unknown or dynamically variable. Typically, such networks are represented by a class of anonymous virtual

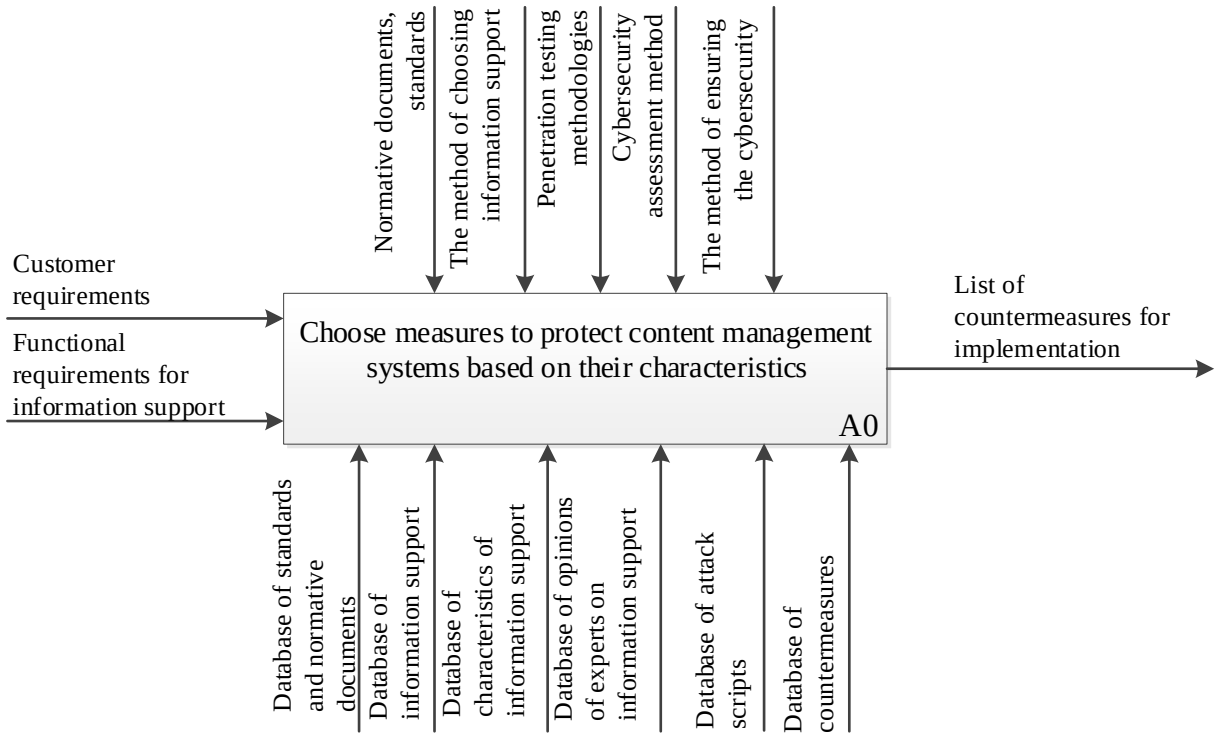

Fig. 1. General view of the IDEF0-diagram illustrating the information technology for ensuring the cybersecurity of content management systems

networks. Therefore, each of SAs analyzes the data on each of the nodes specified by the node time. It is necessary to establish in what order each of SAs will pass all nodes so that the time of passing nodes for each of SAs would be minimum. Additional conditions of the problem are: known distances between nodes within the existing cluster in the virtual network; the starting nodes of the SA input into the system are different, according to an arbitrarily taken distribution function; the time of SA analysis in the node and the availability of information about the occupancy of nodes by other SAs at the current time (queue). A mathematical description of a similar virtual network is given in [11].

Nodes that do the same type of work can be united in clusters by the features of performed actions, and the SA must be serviced by all nodes in any sequence of passing the nodes. The clarifying requirements are: the terms of the review do not require access unless specified by other terms; the amount of SA maintenance times in a node does not require an increase in the relevant time of the task performance as a whole; the sum of the time of passing all nodes must refer to the minimum. Within the SA, there is a set of coefficients that determine the priority of the node for the SA at any given time. The node with the highest priority will be processed for the transition of the SA for further maintenance.

A prototype of the algorithm that implements this method was introduced in [12]. But unlike it, this modification provides that the cycle is repeated among all participants until all SAs will have passed of all nodes.

In [11], a numerical experiment of implementing the proposed method is given, taking into account that the filling of the matrix with values occurs after obtaining the SA value of the finish of the starting node.

The minimum value among the columns of time nodes in the row of the second step is the optimal node, which is determined for the SA for further processing. In the last step, when there are no more nodes available for passing, the network determines the next node – the finish node.

Based on these assumptions, a method for filtering requests on a cloud firewall platform is proposed.

Imagine a cloud firewall in the form of a tuple:

$$\Theta=\left\langle K_n, D_{K_n}, \Psi_m \right\rangle, \quad (1)$$

where K_n – border router;

D_{K_n} – load balancer;

Ψ_m – cloud firewall.

The cloud firewall works as follows (Fig. 2). The input of routers with some intensity receives a stream of requests. Each router has a unique IP address, but all IP addresses are tied to a single domain name (for example, a web-based system that needs to be protected by a cloud firewall) using peripheral technologies [11, 12].

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

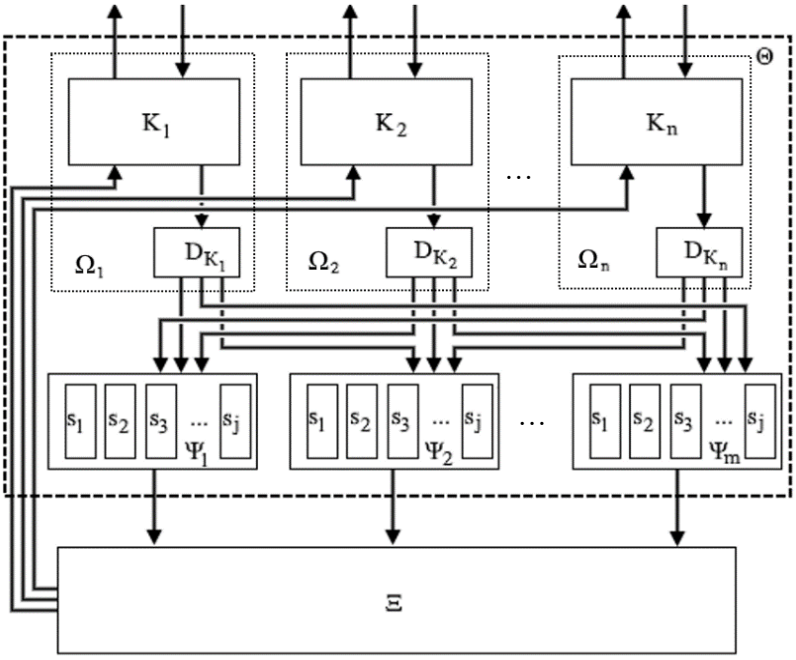

Fig. 2. Block diagram of the cloud firewall

The load balancer determines as the destination the firewall that will serve a particular request. A firewall can be represented by a virtual machine, or a set of virtual applications, or a hybrid solution. It performs a request filtering procedure and, in the case of a normal request, forwards it to the desired web resource server. The resource server, responding to a request from an external network, responds to it through the border router from which the request has come to the cloud firewall.

The calculated performance indicator allows estimating the costs associated with waiting for requests in queues for virtual machines. If costs increase sharply, this is an indication that the embedded virtual machine requires reactivation and its requests need to be forwarded to another machine.

Next, the scenario of multilayer VPN tunneling is used in the organization of remote control of technological equipment [12].

To assess the state of bandwidth, all border routers (including virtual) clients must transmit special data packets to the enterprise's VPN server. For example, consider the delivery of a packet from a computer in the enterprise network to all remotely connected clients of the VPN network and determine the value of bandwidth, which is not effectively used during data exchange.

The total capacity of the tunnel of a single connection to the computer network of the enterprise through the VPN tunnel can be calculated analytically for the "point-to-point" connection by the formula:

$$\Psi = D\ell(2S + (2i-1)\sum_{i=1}^{log_2 S} 2^{i-1}), \quad (2)$$

where D – the number of intermediate routers between VPN networks (including virtual routers);

S – number of border routers;

ℓ – number of connected clients.

If the control unit of the technological equipment transmits data over the "point-broadcast" connection (for example, for broadcasting monitoring information) for each of the tunnels to all VPN network clients, the total bandwidth can be represented as:

$$\Psi' = D(1 + log_2 S + \sum_{i=1}^{log_2 S} 2^i + \ell S). \quad (3)$$

As a result, for the proposed example of a network, the value of bandwidth, which is not effectively used during transmission from each of the subscribers of the VPN network, can be defined as:

$$\theta = D(\ell S - YW), \quad (4)$$

where Y – the average number of vertices of the virtual network, depending on the number of routers in the subnets of the enterprise transport traffic through real IP-addresses;

W – the number of branches of the routing tree in the cascade connection schemes.

Probable problems of practical implementation of the proposed method are the dependence of most services on the unstable Internet channel.

Thus, using known scenarios and a modified method of ensuring the cybersecurity of virtual networks, according to the results [11], it was found that the use of multilayer VPN tunneling can reduce the time to create a highly secure virtual data channel by 30 %, and the cloud firewall speed of detecting malicious network requests is by 34 % higher.

Stage 4. Information technology for formalizing educational processes in the field of cybersecurity specialists training and security of industrial systems

At the final stage, it is important to formalize the acquired knowledge to train professionals in this field, but given that the study of the educational system of cybersecurity specialists training is a difficult task, the difficulties of which are caused not only by weak structures in them but also by the diversity of their structures, forms, methods, techniques, specific content, etc., hence, the diversity of processes is an obstacle in creating appropriate models and their implementation.

The purpose of creating an information technology for the formalization of educational processes in the field of cybersecurity specialists training and security of industrial systems is to develop tools for formal presentation, providing a unified approach in building special mathematical support for information technology solutions in training the cybersecurity.

From the analysis of existing formalization technologies [13], it follows that its "power" is not enough to solve more complex problems of process integration. The term "power" here refers to some shortcomings that lead to the weakening of the formal representation, as well as the impossibility of formalizing the processes of integration between educational systems. In addition, when using formalization technology, there are insurmountable difficulties informally presenting processes in the field of training cybersecurity professionals. One of the disadvantages of existing formalization technologies is the use of methods for systems analysis, which does not provide a formal representation of space-time training processes in the relevant systems.

It is a comprehensive detailed analysis of geospatial characteristics of the educational system of training, as well as recent advances in ontological modeling that have led to the realization that the developed technology of formalization should be based not only on methods of systems analysis but also on linguistic and functional analysis.

The essence of a comprehensive analysis of the studied systems is to identify the features of formalized processes, as well as the selection of objects to be formalized and the construction of their models.

At this stage, the methodological basis of the formal representation of knowledge is heuristic and logical methods of modeling, and the basis for the separation of the cores of subject areas are methods and formalisms of the set theory. Let us consider the structural scheme of the methodological basis for the technology of formalizing information technology solutions (Fig. 3), which is based on expanding the list of methods of analysis, application of knowledge modeling methods by ontologies, the use of modeling methods based on topological diversity.

Thus, the general characteristic of the formal representation of the processes taking place in the field of training the cybersecurity specialists and security of industrial systems is given, and also, the representation of the processes of integration of the studied systems and processes is formalized. The application of the proposed approach in its various variants [14] showed that the absolute success of training specialists increased by an average of 4.5 %, and qualitative success – by 14.2 %.

Conclusions and prospects for further research

The results of research were implemented at the enterprises, which is confirmed by acts of use and implementation:

- at the company "LineUp", which specializes in information technologies (Kharkiv);
- at the enterprise "GMhost" when providing hosting services for virtualization of web-oriented systems (Khmelnytsky);
- at LLC "Blackthorn Vision" in the development of mobile systems (Khmelnitsky);
- at LLC "ITT" when testing software in industrial data transmission systems (Khmelnitsky);
- at LLC "HAKEN" when providing solutions for cybersecurity of web-oriented systems (Kyiv);
- at LLC "Company "Electronic World" in conducting e-commerce (Kharkiv);
- at the state enterprise "State Project and Scientific Aviation Industry Research Institute" in the aviation enterprises complex project (Kharkiv);
- at the machine-building enterprise of JSC "FED" (Kharkiv);
- at the educational process of higher education institutions of Ukraine (National Aerospace University "Kharkiv Aviation Institute", Khmelnytskyi National University, Kharkiv National University of Radio Electronics);

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

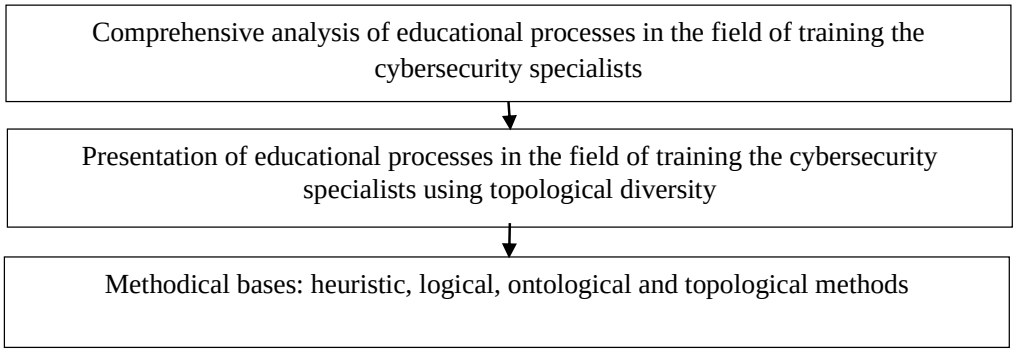

Fig. 3. The main components of the formal presentation of knowledge in the field of training the cybersecurity specialists

- in the implementation of international projects under the European programs TEMPUS, ERASMUS+, Horizon2020;

- in the implementation of national projects at the request by the Ministry of Education and Science of Ukraine in 2011-2020.

The proposed models, methods and technologies for the cybersecurity of industrial and web-based systems and networks, which were implemented in the above enterprises, have allowed to:

– achieve the value of the reliability of malware detection in the Android operating system at 0.94 % and reduce the error rate to 3.25 %, compared with known methods of detecting malware in the Android operating system;

– ensure the allowable value of attack success rate at minimum cost and choose protection measures, taking into account their impact on attack success rate and cost, namely the use of methods on the example of one installation of content management system allowed to reduce the value of attack success rate by 44.2 %;

– reduce the time spent on building and rebuilding the structure of the virtual network in case of reaching the limit values of network delay or compromise of nodes by cybercriminals by an average of 30 %;

– increase the efficiency of training the cybersecurity specialists and security of industrial systems; in particular, experimental verification shows that the absolute success due to the introduction of the proposed information technology in the educational process increased by 4.5 % and qualitative success – by 14.2 % respectively.

The obtained results can be used in a line of existing and promising approaches in the design of difficult, complex, hybrid, technical, cyberphysical systems [15-17] with a web-based interface for users and administrators, in particular, dependability systems [18], including those belonging to the class of critical infrastructure solutions [19-21], intelligent systems [22, 23].

References (GOST 7.1:2006)

1. Cybersecurity for industrial control systems: A survey [Text] / D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, N. Meskin // Computers & security. – 2020. –Vol. 89. – Article No. 101677. DOI: 10.1016/j.cose.2019.101677.

2. Thames, L. Cybersecurity for industry 4.0. Analysis for Design and Manufacturing [Text] / L. Thames, D. Schaefer. – Heidelberg : Springer, 2017. – 265 p.

3. Gansac, V. E-learning platform for cybersecurity of scada systems [Text] / V. Gansac, A. M. Udroiu, S. Pistol // International Scientific Conference "Strategies XXI", "Carol I" National Defence University, 2020. – P. 346-350.

4. Huang, A. Teaching, learning, and assessment with virtualization technology [Text] / A. Huang // Journal of Educational Technology Systems. – 2019. – Vol. 47, No. 4. – P. 523-538.

5. Application of Server Virtualization Technology in Power Information Construction [Text] / H. Yu, J. Guo, L. Wu, S. Wu, B. Peng // Journal of Physics: Conference Series. – 2021. – Vol. 1744, No. 2. – Article No. 022008.

6. Davydova, I. The formation of a practical and theoretical-practical component of the educational process in the context of legal education reform in Ukraine [Text] / I. Davydova // Dilemas Contemporáneos: Educación, Política y Valores. – 2020. – Vol. 7, Iss. 2. – P. 1-25.

7. Niczeporuk, A. Technologia informacyjna do wykrywania wirusów metamorficznych w lokalnych sieciach komputerowych / Wyniki badań interdyscyplinarnych w aspekcie edukacji techniczno-informatycznej i bezpieczeństwa [Text] / A. Niczeporuk, E. Kalinowska-Ozgowicz. – Politechnika Lubelska, Wydawnictwo Politechniki Lubelskiej, 2020. – P. 34-68.

8. Kim, S. G. A Study on Open API Security Protocol based on Multi-Channel [Text] / S. G. Kim // Journal of Convergence for Information Technology. – 2020. – Vol. 10, No. 11. – P. 40-46.

9. Modeling and Availability Assessment of Mobile Healthcare IoT Using Tree Analysis and Queueing Theory [Text] / A. Strielkina, D. Uzun, V. Kharchenko, A. Tetskyi // Dependable IoT for Human and Industry: Modeling, Architecting, Implementation. – River Publishers, 2018. – P. 105-126.

10. A Multi-Objective 2- Approach for Test Suite Reduction During Testing of Web Applications: A Search-Based Approach. International [Text] / M. Khanna, N. Chauhan, D. K. Sharma, L. K. Singh // International Journal of Applied Metaheuristic Computing. – 2021. – Vol. 12, No. 3. – P. 81-122.

11. Method of Building Dynamic Multi-Hop VPN Chains for Ensuring Security of Terminal Access Systems [Text] / V. Tkachov, A. Budko, K. Hvozdetska, D. Hrebeniuk // IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), 2020. – P. 613-618.

12. Tensor Multiflow Routing Model to Ensure the Guaranteed Quality of Service Based on Load Balancing in Network. [Text] / O. Lemeshko, O. Yeremenko, M, Yevdokymenko, A. M. Hailan // International Conference on Computer Science, Engineering and Education Applications. – Springer, Cham, 2020. – P. 120-131.

13. Метешкин, К. А. Кибернетическая педагогика: теоретические основы управления образованием на базе интегрированного интеллекта. [Текст]: монография / К. А. Метешкин. – Х. : Международный Славянский университет, 2004. – 400 с.

14. Тецький, А. Г. Аспекти кібербезпеки платформ дистанційного навчання [Текст] / А. Г. Тецький, О. І. Морозова // Радіоелектронні і комп'ютерні системи. – 2020. – № 4 (96). – С. 93-97. DOI: 10.32620/reks.2020.4.08.

15. Slipachuk, L. The Process of the Critical Infrastructure Cyber Security Management using the Integrated System of the National Cyber Security Sector Management in Ukraine [Text] / L. Slipachuk, S. Toliupa, V. Nakonechnyi // 3rd International Conference on Advanced Information and Communications Technologies (AICT), 2019. – P. 451-454.

16. Sharbaf, M. Reengineering Cyber Security Process: A New Perspective on Cyber Security Quality Management [Text] / M. Sharbaf // IEEE International Conference on Dependable, Autonomic and Secure Computing, International Conference on Pervasive Intelligence and Computing, International Conference on Cloud and Big Data Computing, International Conference on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), 2019. – P. 332-337.

17. Hacimahmud, A. V. Structure and Metrics of Emerging Computing [Text] / A. V. Hacimahmud // IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), 2020. – P. 920-925,

18. Kolisnyk, M. Vulnerability analysis and method of selection of communication protocols for information transfer in internet of things systems [Текст] / M. Kolisnyk // Радіоелектронні і комп'ютерні системи. – 2021. – № 1 (97). – С. 133-149. DOI: 10.32620/reks.2021.1.12.

19. Improving big data centers energy efficiency: Traffic based model and method [Text] / G. Kuchuk, A. Kovalenko, I. E. Komari, A. Svyrydov, V. Kharchenko // Green IT Engineering: Social, Business and Industrial Applications. – Springer, Cham, 2019. – P. 161-183.

20. Approaches to selection of combinatorial algorithm for optimization in network traffic control of safety-critical systems [Text] / G. Kuchuk, V. Kharchenko, A. Kovalenko, E. Ruchkov // IEEE East-West Design & Test Symposium (EWDTS), 2019. – P. 1-6.

21. Criticality Assessment of Critical Information Infrastructure Objects: A Category Based Methodology and Ukrainian Experience. [Text] / O. Potii, Y. Tsyplinskyi, O. Illiashenko, V. Kharchenko, // International Conference on Multimedia Communications, Services and Security. – Springer, Cham, 2020. – P. 78-97.

22. Доценко, С. І. Інтелектуальні системи: принципи евристичної самоорганізації [Текст] / С. І. Доценко // Радіоелектронні і комп'ютерні системи. – 2020. – № 1(93). С. 4-16. DOI: 10.32620/reks.2020.1.01.

23. Доценко, С. І. Інтелектуальні системи: принципи евристичної самоорганізації процесів смислового мислення та смислової діяльності [Текст] / С. І. Доценко // Радіоелектронні і комп'ютерні системи. – 2020. – № 2(94). С. 4-22. DOI: 10.32620/reks.2020.2.01.

References (BSI)

1. Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., & Meskin, N. Cybersecurity for industrial control systems: A survey. *Computers & security*, 2020, vol. 89, article no. 101677. DOI: 10.1016/j.cose.2019.101677.

2. Thames, L., Schaefer, D. *Cybersecurity for industry 4.0. Analysis for Design and Manufacturing*. Heidelberg, Springer Publ., 2017. 265 p.

3. Gansac, V., Udroiu, A. M., Pistol, S. E-learning platform for cybersecurity of scada systems. *International Scientific Conference "Strategies XXI". "Carol I" National Defence University*, 2020, pp. 346-350.

4. Huang, A. Teaching, learning, and assessment with virtualization technology. *Journal of Educational Technology Systems*, 2019, vol. 47, no. 4, pp. 523-538.

5. Yu, H., Guo, J., Wu, L., Wu, S., Peng, B. Application of Server Virtualization Technology in Power Information Construction. *Journal of Physics: Conference Series*, 2021, vol. 1744, no. 2, article no. 022008.

6. Davydova, I. The formation of a practical and theoretical-practical component of the educational

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

process in the context of legal education reform in Ukraine. *Dilemas Contemporáneos: Educación, Política y Valores*, 2020, vol. 7, iss. 2, pp. 1-25.

7. Niczeporuk, A., Kalinowska-Ozgowicz, E. *Technologia informacyjna do wykrywania wirusów metamorficznych w lokalnych sieciach komputerowych*. *Wyniki badań interdyscyplinarnych w aspekcie edukacji techniczno-informatycznej i bezpieczeństwa*. Politechnika Lubelska, Wydawnictwo Politechniki Lubelskiej, 2020, pp. 34-68.

8. Kim, S. G. A Study on Open API Security Protocol based on Multi-Channel. *Journal of Convergence for Information Technology*, 2020, vol. 10, no. 11, pp. 40-46.

9. Strielkina, A., Uzun, D., Kharchenko, V., Tetskyi, A. Modeling and Availability Assessment of Mobile Healthcare IoT Using Tree Analysis and Queueing Theory. *Dependable IoT for Human and Industry: Modeling, Architecting, Implementation*. River Publishers, 2018, pp. 105-126.

10. Khanna, M., Chauhan, N., Sharma, D. K., & Singh, L. K. A Multi-Objective 2- Approach for Test Suite Reduction During Testing of Web Applications: A Search-Based Approach. *International Journal of Applied Metaheuristic Computing (IJAMC)*, 2021, vol. 12, no. 3. pp. 81-122.

11. Tkachov, V., Budko, A., Hvozdetska, K. and Hrebeniuk, D. Method of Building Dynamic Multi-Hop VPN Chains for Ensuring Security of Terminal Access Systems. *IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T)*, 2020, pp. 613-618.

12. Lemeshko, O., Yeremenko, O., Yevdokymenko, M., Hailan, A. M. Tensor Multiflow Routing Model to Ensure the Guaranteed Quality of Service Based on Load Balancing in Network. *International Conference on Computer Science, Engineering and Education Applications*. Springer, Cham, 2020, pp. 120-131.

13. Meteshkin, K. A. *Kiberneticheskaya pedagogika: teoreticheskiye osnovy upravleniya obrazovaniyem na baze integrirovannogo intellekta.* [Cybernetic pedagogy: theoretical foundations of educational management based on integrated intelligence]. Kharkiv, International Slavic University Publ., 2004. 400 p.

14. Tetskyi, A. G., Morozova O. I. *Aspekty kiberbezpeky platform dystantsiynoho navchannya.* [Cybersecurity aspects of e-learning platforms]. *Radioelektronni i komp'uterni sistemi – Radioelectronic and computer systems*, 2020, vol. 4(96), pp. 93-97. DOI: 10.32620/reks.2020.4.08.

15. Slipachuk, L., Toliupa, S., Nakonechnyi, V. The Process of the Critical Infrastructure Cyber Security Management using the Integrated System of the National Cyber Security Sector Management in Ukraine. *3rd International Conference on Advanced Information and Communications Technologies (AICT)*, 2019, pp. 451-454.

16. Sharbaf, M. Reengineering Cyber Security Process: A New Perspective on Cyber Security Quality Management. *IEEE International Conference on Dependable, Autonomic and Secure Computing, International Conference on Pervasive Intelligence and Computing, International Conference on Cloud and Big Data Computing, International Conference on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, 2019, pp. 332-337.

17. Hacimahmud, A. V. Structure and Metrics of Emerging Computing. *IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, 2020, pp. 920-925.

18. Kolisnyk, M. Vulnerability analysis and method of selection of communication protocols for information transfer in internet of things systems. *Radioelektronni i komp'uterni sistemi – Radioelectronic and computer systems*, 2021, vol. 1(97), pp. 133-149. DOI: 10.32620/reks.2021.1.12.

19. Kuchuk, G., Kovalenko, A., Komari, I. E., Svyrydov, A., Kharchenko, V. Improving big data centers energy efficiency: Traffic based model and method. *Green IT Engineering: Social, Business and Industrial Applications*. Springer, Cham, 2019, pp. 161-183.

20. Kuchuk, G., Kharchenko, V., Kovalenko, A., Ruchkov, E. Approaches to selection of combinatorial algorithm for optimization in network traffic control of safety-critical systems. *2016 IEEE East-West Design & Test Symposium (EWDTS)*, 2016, pp. 1-6.

21. Potii, O., Tsyplinskyi, Y., Illiashenko, O., Kharchenko, V. Criticality Assessment of Critical Information Infrastructure Objects: A Category Based Methodology and Ukrainian Experience. *International Conference on Multimedia Communications, Services and Security*. Springer, Cham, 2020, pp. 78-97.

22. Dotsenko, S. Intelektual′ni systemy: pryntsypy evrystychnoyi samoorhanizatsiyi [Intellectual systems: a principle of heuristic self-organization]. *Radioelektronni i komp'uterni sistemi – Radioelectronic and computer systems*, 2020, vol. 1(93), pp. 4-16. DOI: 10.32620/reks.2020.1.01.

23. Dotsenko, S. Intelektual′ni systemy: pryntsypy evrystychnoyi samoorhanizatsiyi protsesiv smyslovoho myslennya ta smyslovoyi diyal′nosti [Intellectual systems: principles of heuristic self-organization of the processes of sense thinking and sense activity]. *Radioelektronni i komp'uterni sistemi – Radioelectronic and computer systems*, 2020, vol. 2(94), pp. 4-22. DOI: 10.32620/reks.2020.2.01.

Надійшла до редакції 28.08.2021, розглянута на редколегії 26.11.2021

МЕТОДИ ТА ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ІНДУСТРІАЛЬНИХ І ВЕБ-ОРІЄНТОВАНИХ СИСТЕМ І МЕРЕЖ

О. І. Морозова, А. О. Нічепорук, А. Г. Тецький, В. М. Ткачов

Предметом статті є методи та технології забезпечення кібербезпеки індустріальних і веб-орієнтованих систем і мереж, підготовка фахівців з кібербезпеки під час здобуття професійних знань. Метою статті є забезпечення кібербезпеки індустріальних і веб-орієнтованих систем і мереж шляхом розроблення та впровадження відповідної методології (концепції, принципів, комплексу моделей, методів) і технологій в індустрії, а також при підготовці фахівців з кібербезпеки під час здобуття професійних знань. Сформульовано проблему розроблення моделей, методів і технологій забезпечення кібербезпеки мобільних систем, веб-орієнтованих систем на ос-нові систем керування вмістом, віртуальних мереж, що забезпечують їх взаємодію, та методології підготовки фахівців з кібербезпеки. На основі аналізу були сформульовані окремі завдання розроблення моделі згорткової нейронної мережі, методів, моделей та інформаційної технології забезпечення кібербезпеки веб-орієнтованих систем та віртуальних мереж, методологічних основ створення інформаційної технології й моделі цифрової платформи знань для використання в галузі підготовки фахівців з кібербезпеки та безпеки індустріальних систем. Базові теоретичні рішення, які лежать в основі побудови реальних індустріальних і веб-орієнтованих систем і мереж, що наведено у статті. Результатами роботи є: підвищено значення достовірності виявлення шкідливого програмного забезпечення в операційній системі Android, зменшено показники хиб-них спрацювань, забезпечено допустиме значення показника успішності атак при мінімальній вар-тості, зменшено часові затрати на побудову та перебудову структури віртуальної мережі, підвищено ефективність підготовки фахівців з кібербезпеки та безпеки індустріальних систем. Зі сказаного вище можна зробити висновок, що одержані результати можна використовувати в лінійці існуючих та перспективних підходів при проектуванні складних, комплексних, гібридних, технічних, кіберфізичних систем з веб-орієнтованим інтерфейсом для користувачів та адміністраторів.

Ключові слова: кібербезпека; Індустрія 4.0; веб-орієнтовані системи; комп'ютерні мережі; інформаційні технології; фахова освіта.

МЕТОДЫ И ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ ИНДУСТРИАЛЬНЫХ И ВЕБ-ОРИЕНТИРОВАННЫХ СИСТЕМ И СЕТЕЙ

О. И. Морозова, А. А. Ничепорук, А. Г. Тецкий, В. Н. Ткачев

Предметом статьи являются методы и технологии обеспечения кибербезопасности индустриальных и веб-ориентированных систем и сетей, подготовка специалистов по кибербезопасности при получении профессиональных знаний. Целью статьи является обеспечение кибербезопасности индустриальных и веб-ориентированных систем и сетей путем разработки и внедрения соответствующей методологии (концепции, принципов, комплекса моделей, методов) и технологий в индустрии, а также при подготовке специалистов по кибербезопасности при получении профессиональных знаний. Сформулирована проблема разработки моделей, методов и технологий обеспечения кибербезопасности мобильных систем, веб-ориентированных систем на основе систем управления содержанием, виртуальных сетей, обеспечивающих их взаимодействие, и методологии подготовки специалистов по кибербезопасности. На основе анализа были сформулированы отдельные задачи разработки модели сверточной нейронной сети, методов, моделей и информационной технологии обеспечения кибербезопасности веб-ориентированных систем и виртуальных сетей, методологических основ создания информационной технологии и модели цифровой платформы знаний для использования в области подготовки специалистов по кибербезопасности и безопасности индустриальных систем. Базовые теоретические решения, которые лежат в основе построения реальных индустриальных и веб-ориентированных систем и сетей, приведены в статье. Результатами работы являются: увеличено значения достоверности обнаружения вредоносного программного обеспечения в операционной системе Android, уменьшено показатели ложных срабатываний, обеспечено допустимое значение показателя успешности атак при минимальной стоимости, уменьшено временные затраты на построение и перестройку структуры виртуальной сети, повышена эффективность подготовки специалистов по кибербезопасности и безопасности индустриальных систем. Из вышесказанного можно сделать вывод, что полученные результаты можно использовать в линейке существующих и перспективных подходов при проектировании сложных, комплексных, гибридных, технических, киберфизических систем с веб-ориентированным интерфейсом для пользователей и администраторов.

Ключевые слова: кибербезопасность; Индустрия 4.0; веб-ориентированные системы; компьютерные сети; информационные технологии; профессиональное образование.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Морозова Ольга Ігорівна – д-р техн. наук, доц., проф. каф. комп'ютерних систем, мереж і кібербезпеки, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Нічепорук Андрій Олександрович – канд. техн. наук, доц., доц. каф. комп'ютерної інженерії та системного програмування, Хмельницький національний університет, Хмельницький, Україна.

Тецький Артем Григорович – канд. техн. наук, ст. викл. каф. комп'ютерних систем, мереж і кібербезпеки, Національний аерокосмічний університет ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Ткачов Віталій Миколайович – канд. техн. наук, доц., доц. каф. електронних обчислювальних машин, помічник ректора з питань ІТ, Харківський національний університет радіоелектроніки, Харків, Україна.

Olga Morozova – Doctor of Technical Science, Associate Professor, Professor of the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine,
e-mail: o.morozova@csn.khai.edu, ORCID: 0000-0001-7706-3155.

Andrii Nicheporuk – Candidate of Technical Science, Associate Professor, Associated Professor of the Department of Computer Engineering and Systems Programming, Khmelnytskyi National University, Khmelnytskyi, Ukraine,
e-mail: andrey.nicheporuk@khnu.km.ua, ORCID: 0000-0002-7230-9475.

Artem Tetskyi – Candidate of Technical Science, Senior Lecturer of the Department of Computer Systems, Networks and Cybersecurity, National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine,
e-mail: a.tetskiy@csn.khai.edu, ORCID: 0000-0003-1745-2452.

Vitalii Tkachov – Candidate of Technical Science, Associate Professor, Associated Professor of the Department of Electronic Computers, Assistant Rector of Information Technology, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine,
e-mail: tkachov@ieee.org, ORCID: 0000-0002-6524-9937.