UDC 004.81
DOI: 10.15587/1729-4061.2026.355570

DEVELOPMENT OF METHODS OF INTELLIGENT MANAGEMENT OF SECURITY PARAMETERS OF INFORMATION SYSTEMS

Hennadii Shapovalov
Doctor of Philosophy (PhD), Senior Researcher
Research Department of Information Confrontation Research Center
Military Institute of Taras Shevchenko National University of Kyiv
Yuliyi Zdanovskoi str., 81, Kyiv, 03680
ORCID: https://orcid.org/0000-0002-8979-0648

Olha Salnikova
Doctor of Sciences in Public Administration, Senior Researcher, Honored Worker of Science and Technology of Ukraine, Professor
Department of Theory and Practice of Management
National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute»
Peremohy ave., 37, Kyiv, Ukraine, 03056
ORCID: https://orcid.org/0000-0002-7190-6091

Oleksii Kuvshynov
Doctor of Technical Sciences, Professor, Deputy Head of Institute
Institute of Professional Military Education «Leadership Training»**
ORCID: https://orcid.org/0000-0003-2183-7224

Yevhenii Kapran
Adjunct
Scientific and Organizational Department
Kruty Heroes Military Institute of Telecommunications and Information Technology
Kniaziv Ostrozkykh str., 45/1, Kyiv, Ukraine, 01011
ORCID: https://orcid.org/0009-0009-9131-5756

Oleksii Nalapko
Doctor of Philosophy (PhD), Doctoral Student
Scientific and Organizational Department
Central Scientifically-Research Institute of Armaments and Military Equipment of the Armed Forces of Ukraine
Air Force ave., 28, Kyiv, Ukraine, 03049
ORCID: https://orcid.org/0000-0002-3515-2026

Oksana Dmytriieva
Doctor of Economic Sciences, Professor, Head of Department
Department of Economics and Entrepreneurship*
ORCID: https://orcid.org/0000-0001-9314-350X

Ihor Borysov
PhD, Associate Professor, Deputy Head of the Institute for Scientific Work
Research Institute of Military Intelligence
Yuriy Illenka str., 81, Kyiv, Ukraine, 04050
ORCID: https://orcid.org/0000-0003-2276-9913

Viktor Yerko
PhD, Senior Researcher, Head of Department
Scientific Research Department
State Research Institute of Aviation
Kazarmenna str., 6, Kyiv, Ukraine, 01135
ORCID: https://orcid.org/0000-0002-5150-5303

Hryhorii Stepanov
PhD, Associate Professor, Deputy Head of Department
Department of Air Force**
ORCID: https://orcid.org/0000-0002-9190-2821
*Kharkiv National Automobile and Highway University
Yaroslava Mudroho str., 25, Kharkiv, Ukraine, 61002
**National Defence University of Ukraine
Povitrianykh Syl ave., 28, Kyiv, Ukraine, 03049

Andrii Shyshatskyi
Corresponding author
Doctor of Technical Sciences, Senior Researcher, Professor
Department of Computer Science and Information Systems*
E-mail: ierikon13@gmail.com
ORCID: https://orcid.org/0000-0001-6731-6390

The object of the study is information systems (IS). The problem that is being solved in the study is an increase in the level of IS protection. The study developed a methodology for intelligent management of IS security parameters. The originality of the study consists of:

– conducting a multi-level and systematic assessment of the state of IS security using the proposed set of analytical expressions;

– determining the influence of IS security parameters on each other when the IS security state changes due to the use of fuzzy analytical expressions;

– construction of multidimensional dependencies of the security state of the special-purpose IS, which evaluates the security of the IS based on an arbitrary number of parameters;

– assessment of IS security in conditions of incompleteness of information about evaluation parameters, which solves the dimensionality problem;

– construction of time dependences of changes in parameters that characterize the state of IS protection, which allows determining the moments of deviation of their values from the nominal;

– reducing the error of assessing the state of IS security due to the human factor through the verification of IS parameters;

– attracting additional computing resources (if necessary), which achieves the prevention of looping of the methodology;

– determination of the influence of control decisions on a separately defined parameter for assessing the state of IS security, which achieves an increase in the accuracy of control influences.

Modeling of the work of the proposed methodology was carried out, during which it was established that increasing the security of the IS is achieved by increasing the efficiency of decision-making at the level of 12–16% due to the use of additional procedures and ensuring the reliability (correctness) of the decisions made at the level of 0.94. This allows to avoid distortions and distortions of the information provided for decision-makers (systems)

Keywords: multidimensionality of assessment, complex systems, efficiency of decision-making, efficiency of assessment, bio-inspired algorithms

Received 18.12.2025
Received in revised form 09.03.2026
Accepted 18.03.2026
Published 30.04.2026

How to Cite: *Shapovalov, H., Salnikova, O., Kuvshynov, O., Kapran,Y., Nalapko, O., Dmytriieva, O., Borysov, I., Yerko, V., Stepanov, H., Shyshatskyi, A. (2026). Development of methods of intelligent management of security parameters of information systems. Eastern-European Journal of Enterprise Technologies, 2 (4 (140)), 16–25. https://doi.org/10.15587/1729-4061.2026.355570*

1. Introduction

Armed conflicts of the last decade have become a catalyst for the rapid development of information technologies, including information systems (IS). IS is currently used to address both purely specific tasks in the interests of defense and national security and purely urgent issues in society.

Below are some of the tasks that are solved by IS [1–3]:

– collecting, processing, and summarizing information coming from end users;

– storage of various types of data, their archiving, and output;

– solving individual and/or complex calculation tasks for a wide range of users;

– modeling the nature of military conflicts;

– transfer of information between IS elements, etc.

The main features of the functioning of IS for various functional purposes are [2, 4, 5]:

– constant growth in the volume of information circulating in the middle of the IS and between the IS;

– expansion of the nomenclature of means that destructively affect the process of data exchange in the middle of the IS and between the IS themselves;

– improvement of forms and methods of influencing the process of IS functioning, which negatively affects such indicators as efficiency and reliability of data exchange;

– simultaneous growth of requirements for a set of indicators characterizing the process of IS functioning;

– imperfection of the mechanisms for ensuring the security of IS in the process of their functioning, etc.

Taking into account the above, one of the urgent directions for increasing the efficiency of the functioning of complex technical systems is the development of a methodology for intelligent management of the state of security of information systems.

2. Literature review and problem statement

In work [6], it is proposed to use Bayesian hierarchical networks to determine the quantitative assessment of the level of cybersecurity risks in special-purpose IS. However, this approach is limited by the statistical distribution that can be used and by the extensibility of the model structure. This imposes restrictions on the architecture of the information system and does not take into account the qualitative factors that affect the cybersecurity of the IS.

Work [7] proposed a security certification methodology developed for ISs to enable various stakeholders to evaluate security solutions for large-scale IS deployments automatically. The methodology supports transparency regarding the level of IS safety for consumers, as the methodology provides labeling as one of the main results of the certification process. The disadvantages of the proposed approach include the inability to train knowledge bases for new threats, the problematic nature of generalization, and the analysis of various types of data circulating in the network.

Work [8] proposes a model that integrates fault tree analysis, decision theory, and fuzzy theory to establish the current causes of refusals to prevent cyberattacks. The model has been applied to assess cybersecurity risks associated with a website attack, e-commerce, and corporate resource planning, and to assess the possible consequences of such attacks. The specified model has a flexible architecture; at the same time, the disadvantages of the proposed model include the accumulation of evaluation error during the fuzzification and defuzzification procedure.

Work [9] proposes a model for the distribution of special-purpose IS resources in conditions of insufficient information about the development of the operational situation. In the specified model, mechanisms for the distribution of IS resources are proposed, taking into account the impact of cyber-attacks. This allows the representation of the solution of the vector optimization problem in binary relations of conflict, facilitation, and indifference. It also takes into account the operational situation and allows to predict the state of the IS, taking into account external influences, build utility and guaranteed gain functions, as well as a numerical optimization scheme on this set. At the same time, the specified model does not allow working with various indicators of the assessment of the functioning of the IS state.

Work [10] proposes a hierarchical concept for the introduction of a governance model based on e-government. The article examines the main threats to critical cyber-physical systems as the basis of mechanisms for performing e-government functions. This hierarchical system is based on the use of symmetric and asymmetric cryptosystems, which do not allow them to be used for the task of identifying cyber influences on IS.

Work [11] proposes a model for choosing the optimal set of cybersecurity insurance policies by a firm, given the limited number of policies offered by one or more insurance companies. The proposed model provides a risk-sharing approach that helps the root-mean-square choices of cybersecurity insurance policies in a way that contributes to an efficient cybersecurity insurance market. At the same time, the disadvantages of this approach include the impossibility of introducing new risks to the knowledge base during work and a limited number of assumptions. This makes it impossible for it to work in real time.

Work [12] discusses the importance of incorporating vulnerability analysis into cybersecurity, not only as part of process hazard analysis, but also in terms of protecting the process management network and implementing adequate safeguards in general against cyber threats. Protection level analysis is tailored to assess potential weaknesses and ensure critical applications are protected from cyber-attacks. The integration of cybersecurity into hazard and risk analysis, as well as other elements of technological process security management, is demonstrated by examples, making the plant more resistant to traditional and cyber threats. However, the proposed approach is adapted only for a clear architecture and is not intended for adjustment during operation.

The work [13] proposes a risk management process for identifying, analyzing, evaluating, responding to cyber threats, and monitoring risks at each stage of the cyber protection chain. This approach can be used in organizations that are going to implement security mechanisms to align them to current requirements or reduce cyber risks to acceptable levels. Risk assessment method based on a continuous Markov chain. At the same time, the disadvantages of the proposed method include the impossibility of simultaneous consideration of both quantitative and qualitative indicators, and the impossibility of adaptation to new threats in the system.

In the work [14], a theoretical-analytical approach to the analysis of the impact of information transmission delay in traffic regulation caused by cyber influence is proposed. The evaluation takes place using the method of consecutive averages. However, this approach is limited to use only in motion control systems and is not adapted for use in other systems.

Work [15] proposed to consider cyber security of an object in the form of a graph of transient processes. The said approach allows for describing the threats that affect the object, to determine their degree of impact on cybersecurity. Disadvantages of the proposed approach include the possibility of working only with single-dimensional values and the

impossibility of adding new threats during the operation of the proposed approach.

Work [16] presents a method for creating and solving a game theory model to address cybersecurity issues specifically for advanced manufacturing systems with high-level integrated computer integration. This method introduces a unique approach to determining the content of the game's payoff matrix, including support for defense strategies, production losses, and recovery from attacks as part of the cost function. Disadvantages of the proposed method include great computational complexity and the possibility of working only with one-dimensional values.

So, summarizing the above, the general disadvantage of all these approaches is the impossibility of working with multidimensional data in real time. Several different solutions have been proposed to eliminate this shortcoming.

Work [17] presents an approach to evaluating input data for IS. The essence of the proposed approach is the clustering of the basic set of input data, their analysis, and after which the system is trained based on the analysis. The disadvantages of the mentioned approach are the gradual accumulation of evaluation and learning errors due to the lack of the possibility to evaluate the adequacy of the decisions made.

Work [18] presents an approach to data processing from various sources of information. This approach allows processing data from various sources. The disadvantages of the specified approach include the low accuracy of the received assessment and the impossibility of checking the reliability of the received assessment.

In the work [19], a comparative analysis of existing decision support technologies was carried out, namely: the method of analyzing hierarchies, neural networks, the theory of fuzzy sets, genetic algorithms, and neuro-fuzzy modeling. The advantages and disadvantages of these approaches are indicated. The areas of their application are defined. For the tasks of assessing the state of functioning of the IS state in conditions of risk and uncertainty, the use of a neuro-fuzzy approach is justified.

Work [20] states that the use of a combination of different strategies for applying metaheuristic algorithms. The disadvantages of this approach are the insufficient convergence of the obtained results when several metaheuristic algorithms are used together to assess the security of IS functioning.

The analysis of works [9–20] showed that the common shortcomings of the above-mentioned studies are:

– assessment of the state of IS security is carried out only at a separate level of their functioning, or only at a separate element of IS;

– with a comprehensive approach to assessing the state of IS security, as a rule, one or two components affecting the security of IS functioning are considered. This does not allow to fully assess the impact of management decisions on the further functioning of the IS;

– the approaches listed above (methods, techniques), provide weak integration into each other (or make it impossible at all), which does not allow them to be combined for a joint assessment of the functioning of the IS security state;

– the above approaches for assessing the state of security of IS functioning use a different mathematical apparatus, which requires appropriate mathematical transformations, which in turn increase computational complexity and reduce the accuracy of assessing the state of functional reliability of IS, etc.

All this necessitates research on the development of methods of intelligent management of information system security parameters.

3. The aim and objectives of the study

The aim of the study is to increase the security level of information systems due to the development of a methodology for intelligent management of their security parameters. This will allow comprehensive, objective, and full decision-making regarding the management of IS security parameters at different levels of their functioning (individual elements of IS).

Also, it will make it possible to develop (improve) the software of modern and promising IS by integrating the proposed methodology into the corresponding software.

To achieve this aim, the following objectives were accomplished:

– to propose the main procedures of the methodology of intelligent management of information system security parameters;

– to evaluate the effectiveness of the proposed methodology according to certain criteria.

4. Materials and methods

The object of the study is IS. The problem that is being solved in the study is an increase in the level of IS protection. The subject of the study is the process of assessing and managing the state of IS security. The hypothesis of the study is the possibility of increasing the level of IS security due to the development of a methodology for intelligent management of IS security parameters.

To carry out modeling and calculations, it is accepted that the information system performs typical calculations and computing operations under the conditions of constant influence of destructive factors. The simplifications adopted in this study are the modeling of the effectiveness of the specified methodology only on the specified composition of the information system, without taking into account other possible components of the information system.

In the course of the study, the following methods were used:

– general scientific method of analysis – for decomposing problematic issues of assessing the security level of IS when they perform tasks as intended. Also, the general scientific method of analysis is used to determine the advantages and disadvantages of known approaches to assessing the security level and managing the security level of IS when they perform tasks as intended.

– general scientific method of synthesis – to substantiate the most appropriate approaches for assessing the level of IS and managing the security level when they perform tasks as intended;

– methodical approach based on the use of fuzzy cognitive models – to determine control solutions, to manage the level of IS security. The specified improved algorithm provides the possibility of combining into a single system indicator of the security of information systems of different units of measurement and origin.

As an IS for simulation, the communication and information system of the operational grouping of troops (forces) was adopted in this study. The operational group of troops (forces) was formed according to the state of martial law (typical state). Mode of operation of the communication and information systems system – defense operation.

The organizational and personnel structure of the operational grouping of troops (forces), for modeling, includes 197 elements of the information system located on various platforms (carriers). Also, the information system of the operational grouping of troops (forces) selected for modeling includes stationary elements of the information system.

Distribution of elements of the information system, for modeling according to the main aggregate tactical and technical characteristics:

– unmanned aerial vehicles of multicopter type and type "wing" – 62;

– broadband radio access facilities – 33;

– tactical level radio communication facilities – 47;

– operational layer radio communication facilities – 13;

– satellite communications facilities – 10;

– secure field servers – 4;

– secure field personal computing machines – 28.

Generalized tactical and technical characteristics of means of destructive influence on the information system of the operational grouping of troops (forces) chosen for the computational experiment:

1. Means of radio-electronic countermeasures that simultaneously exert a destructive effect with the following tactical and technical characteristics – 4 units:

– lower/upper limit of the frequency range of radio electronic intelligence, MHz – 20...6000;

– lower/upper limit of the suppression frequency range, MHz – 20...6000;

– interference output power, W – 600;

– max. number of channels suppressed simultaneously – 12;

– the possibility of determining the coordinates of radio emitting means;

– ability to suppress channels of global satellite positioning systems NAVSTAR L1/L2/L5, GLONASS L1/L2.

– channel suppression capability, MHz GSM 900/1800, CDMA 400...530/850...895/2100...2170, UMTS 850...900/1800...2025/2110...2200, LTE 790...850/1800...1880/2600...2700; Wi-Fi 2300...2600/3400...3800/5170...6000; WiMAX 1500/2300...2500; WiMAX 2700/3400...3800;

– capability to suppress VHF and trunking systems, MHz 20...1000;

– capability to suppress satellite communications systems, MHz 1525...1559; 1616...1625; 3400...3625;

– ability to suppress control channels of unmanned aerial vehicles, MHz 440...3000/3000...6000 MHz.

2. Means of cyber influence that simultaneously exert a destructive influence on the radio channel – 12 units. Type of cyber infusion – denial of service.

A computational experiment of the proposed methodology was conducted in the Microsoft Visual Studio 2022 software environment (USA). The hardware of the research process is AMD Ryzen 5.

The general computational experiment is laid out on 151 sheets and contains information sensitive to disclosure.

5. Research results on intelligent management of security parameters of information systems

5. 1. Development of the main procedures of the methodology of intelligent management of security parameters of information systems

The method of intelligent management of IS security parameters consists of the following sequence of actions:

Action 1. Entering output data about IS.

In the specified procedure, initial data on the IS and the conditions of its functioning are entered. The following output data are entered:

– the number of electronic warfare (EW) that affect IS (both own and enemy);

– the number of means of cyber influence, the intensity of cyber influence on IS;

– type of cyber-attacks that act on IS;

– spectral-energy parameters of obstacles of EW means affecting IS;

– the number of means of fire damage that act in the line of operation of the IS;

– intensity of fire impact on IS, etc.

Action 2. Construction of a fuzzy IS security graph

$$FSCN = \langle P, S, R, U, D \rangle, \quad (1)$$

where $P = \{p_i | i = 1, ..., I\}$ – set of fuzzy situational signs (assessment parameters), which describe the state of IS security;

$S = \{s_j | j = 1, ..., J\}$ – set of fuzzy IS situations (IS risks and security threats);

$R = \left\{ r_{k_i}^{(p_i)} \mid k_i = 1,\ldots,K_i, i = 1,\ldots,I \right\}$ – set of fuzzy control decisions for managing the IS security state;

$U = \left\{ u_{j_k, j_l} \mid s_{j_k}, s_{j_l} \in S \right\}$ – set of control transitions between fuzzy situations in IS;

$D = \left\{ D_{s_{cur}, s_{tar}} \right\}$ – set of all IS routes that includes subsets $D_{s_{cur}, s_{tar}} = \left\{ d_b^{(s_{cur}, s_{tar})} \mid b = 1,\ldots,B_{s_{cur}, s_{tar}} \right\}$, $s_{cur}, s_{tar} \in S$ routes between different current (identified) s_{cur} and target s_{tar} unclear situations in IS.

Action 2. 1. Verification of a fuzzy graph.

At this stage, with the help of an improved bio-inspired algorithm [19], the fuzzy IS security graph is verified. In case of detection of deviations, the initial data is adjusted using the results of the bio-inspired algorithm.

Action 2. 2. Description of the parameters for assessing the security status of the IS state p_i, $i = 1, ..., I$ to describe the state of IS security.

The parameters for assessing the security status of IS are described by variables $\langle p_i, T_{p_i}, X_{p_i} \rangle$, where

$$T_{p_i} = \left\{ T_m^{(p_i)} \mid m = 1,\ldots,M \right\}$$

– term-set of variables; X_{p_i} – basic set p_i.

For submission $T_m^{(p_i)}$, $m = 1,\ldots,M$ fuzzy sets are used

$$T_m^{(p_i)} = \left\{ \left(\mu_{T_m^{(p_i)}}(x) / x \right) \right\}, x \in X_{p_i}.$$

Action 2. 3. Description of fuzzy situations of the IS security state in the form of a fuzzy set of the 2nd level:

$$\forall s_j \in S : \tilde{s}_j = \left\{ \left(\mu_{\tilde{s}_j}(\tilde{p}_j) / P \right) \right\}, p_i \in P,$$

$$\tilde{p}_i = \left\{ \left(\mu_{\tilde{p}_i}\left(T_m'^{(p_i)} \right) / T_m^{(p_i)} \right) \mid m = 1,\ldots,M \right\}, i \in \{1,\ldots,I\}. \quad (2)$$

Action 2. 4. Formation of management decisions regarding the management of IS security parameters:

$$r_{k_i}^{(p_i)} = \left\langle Tr^{\left(r_{k_i}^{(p_i)}\right)}, Er^{\left(r_{k_i}^{(p_i)}\right)}, Xr^{\left(r_{k_i}^{(p_i)}\right)} \right\rangle, \quad (3)$$

$$r_{k_i}^{(p_i)} \in R, k_i = 1,\ldots,K_i, i = 1,\ldots,I.$$

where $Tr^{\left(r_{k_i}^{(p_i)}\right)}$ – term set "of direction" influence $r_{k_i}^{(p_i)}$ on a sign p_i (IS security parameter), for example ($\{Tr_1^{\left(r_{k_i}^{(p_i)}\right)}$ – increase, $Tr_2^{\left(r_{k_i}^{(p_i)}\right)}$ – reduce, $Tr_3^{\left(r_{k_i}^{(p_i)}\right)}$ – do not change $\}$);

$Er^{\left(r_{k_i}^{(p_i)}\right)}$ – term set of degree of influence $r_{k_i}^{(p_i)}$ on a sign p_i, for example ($\{Er_1^{\left(r_{k_i}^{(p_i)}\right)}$ – very weak, $Er_2^{\left(r_{k_i}^{(p_i)}\right)}$ – weakly, $Er_3^{\left(r_{k_i}^{(p_i)}\right)}$ – strongly, $Er_4^{\left(r_{k_i}^{(p_i)}\right)}$ – very strong $\}$);

$Xr^{\left(r_{k_i}^{(p_i)}\right)}$ – scale of degree of influence $r_{k_i}^{(p_i)}$ [–1, 1].

It is the influence of the management decision $r_{k_i}^{(p_i)}$ on the sign (IS security parameter) p_i implemented by the fuzzy operation max-min- compositions between fuzzy set $\tilde{p}_i$, and a vague relationship $\tilde{r}_{k_i}^{(p_i)}$. As a result of this influence, the fuzzy value of the sign changes p_i

$$\tilde{p}_i' = \tilde{p}_i \cdot \tilde{r}_{k_i}^{(p_i)}. \quad (4)$$

The locality property of control solutions determines the number of features (IS security parameters) that change as a result of applying one control solution (the control solution is k-local if it leads to a change in the values of k features).

For fuzzy situational management of the security parameters of the IC under consideration, it is advisable to decompose k-local control solutions and present them in the form of a sequence of l-local control solutions, ordered by the degree of influence on the corresponding features. It allows:

– form and rank ordered sets of l-local control solutions corresponding to the k-local control solution, taking into account the setting of threshold values of the influence of control solutions on the dependent parameters of the IS security state;

– increase the flexibility of fuzzy graph adaptation when structurally and parametrically configuring the composite hybrid model for managing IS security parameters.

Action 3. Assessment of the indirect influence of control decisions on changing IS security parameters.

Action 3. 1. For each pair of features (for all pairwise c0ations of the influence of signs on each other, the property of transitivity is violated, then a transitive closure is performed for them, for example

$$Ef_{p_i,p_z} = Ef_{p_i,p_z} \vee Ef_{p_i,p_z}^2 \vee \ldots \vee Ef_{p_i,p_z}^1 \vee \ldots, \quad (7)$$

where $Ef_{p_i,p_z}^k = Ef_{p_i,p_z}^{k-1} \cdot Ef_{p_i,p_z}$.

If it is not possible to provide a transitive closure for any fuzzy relations, then it may be necessary to clarify them by an expert.

Action 3. 4. As a result, a generalized matrix of agreed fuzzy relations of the influence of all parameters of the IS security assessment on each other is formed:

$$Ef = \begin{vmatrix} Ef_{p_1,p_1} & Ef_{p_1,p_2} & \ldots & Ef_{p_1,p_I} \\ Ef_{p_2,p_1} & Ef_{p_2,p_2} & \ldots & Ef_{p_2,p_I} \\ \ldots & \ldots & \ldots & \ldots \\ Ef_{p_I,p_1} & Ef_{p_I,p_2} & \ldots & Ef_{p_I,p_I} \end{vmatrix}. \quad (8)$$

Action 3. 5. As a result of the application of the management decision $r_{k_i}^{(p_i)}$ the value of the IS security parameter p_i, represented by a fuzzy set $\tilde{p}_i = \left\{\left(\mu_{\tilde{p}_i}\left(T_m^{(p_i)}\right)/T_m^{(p_i)}\right) | m = 1,\ldots,M\right\}$, changes as follows

$$\tilde{p}_i' = \left\{\left(\mu_{\tilde{p}_i}\left(T_m'^{(p_i)}\right)/T_m^{(p_i)}\right) | m = 1,\ldots,M\right\}.$$

Action 3. 6. The resulting change in the IS security parameter p_i it is presented in the form of two fuzzy sets for separate consideration of positive and negative influences:

– $\delta p_i^+ = \left\{\left(\mu_{\delta p_i^+}\left(T_m^{(p_i)}\right)/T_m^{(p_i)}\right) | m = 1,\ldots,M\right\}, i \in \{1,\ldots,I\}$ – to take into account positive changes in the values of the IS security assessment parameter p_i;

– $\delta p_i^- = \left\{\left(\mu_{\delta p_i^-}\left(T_m^{(p_i)}\right)/T_m^{(p_i)}\right) | m = 1,\ldots,M\right\}, i \in \{1,\ldots,I\}$ – to take into account negative changes in the values of the IS security assessment parameter p_i.

Action 3. 7. Fuzzy sets are defined δp_i^+ and δp_i^-, what are the positive and negative changes in the IS security assessment parameter p_z taking into account its interdependence with the sign p_i:

$$\delta p_i^+ = \delta p_i^+ \cdot Ef_{p_i,p_z} = \left\{\left(\mu_{\delta p_z^+}\left(T_m^{(p_z)}\right)/T_m^{(p_z)}\right) | m = 1,\ldots,M\right\}, i \in \{1,\ldots,I\}, \quad (9)$$

$$\delta p_i^- = \delta p_i^- \cdot Ef_{p_i,p_z} = \left\{\left(\mu_{\delta p_z^-}\left(T_m^{(p_z)}\right)/T_m^{(p_z)}\right) | m = 1,\ldots,M\right\}, i \in \{1,\ldots,I\}. \quad (10)$$

Action 3. 8. The indirect effect on the IS security assessment parameter is determined p_z management decision $r_{k_i}^{(p_i)}$, which directly affects the sign p_i:

$$\forall p_z \in P: \quad \tilde{p}_z' = \left\{\left(\min\left(1, \max\left(0, \begin{pmatrix} \mu_{\tilde{p}_z}\left(T_m^{(p_z)}\right) + \\ +\mu_{\delta p_z^+}\left(T_m^{(p_z)}\right) - \\ -\mu_{\delta p_z^-}\left(T_m^{(p_z)}\right) \end{pmatrix}\right)\right)/T_m^{(p_z)}\right) | m = 1,\ldots,M\right\}. \quad (11)$$

Similarly, the indirect influence of the management decision is taken into account $r_{k_i}^{(p_i)}$ but for all other vague situational signs with P.

Action 3. 9. As a result of the application of the above proposed procedure for each management decision with R a set of local control decisions is formed, ordered by the degree of their influence on dependent fuzzy situational features. Moreover, the number of these local control decisions may be limited depending on the threshold values established and the effects of the control decisions on dependent features.

The results of assessing the degree of influence of control decisions on fuzzy situational features are the basis for setting control transitions when implementing a direct approach to constructing a fuzzy graph for managing IS security parameters.

Action 4. Identification of the current unclear situation regarding the state of IS security, which is:

– firstly, in matching the feature values of the current IS security situation with the feature values of all reference fuzzy situations of the constructed fuzzy graph;

– secondly, in determining the reference fuzzy situation of the fuzzy graph, closest in a certain sense to the current situation of the IC security scenario according to the chosen method of their comparison;

– thirdly, in identifying the current fuzzy situation with the nearest fuzzy graph reference situation found.

One of the main requirements for the chosen method of comparing fuzzy situations is the possibility of establishing the degree of their closeness (similarity). This requirement is satisfied, for example, by the indicator of fuzzy equality of situations, which is well established for matching fuzzy sets of level 2 [10]

$$\theta\left(s_{cur}, s_j\right) = \underset{p_i \in P}{\wedge} \theta\left(\mu_{\tilde{s}_{cur}}\left(\tilde{p}_i\right), \mu_{\tilde{s}_j}\left(\tilde{p}_i\right)\right),$$

where:

$$\theta\left(\mu_{\tilde{s}_{cur}}\left(\tilde{p}_i\right), \mu_{\tilde{s}_j}\left(\tilde{p}_i\right)\right) = \underset{T_m^{(p_i)}}{\wedge} \theta\left(\left(\mu_{\tilde{s}_{cur}}\left(p_i\right)/T_m^{(p_i)}\right), \left(\mu_{\tilde{s}_j}\left(p_i\right)/T_m^{(p_i)}\right)\right),$$

$$\theta\left(\left(\mu_{\tilde{s}_{cur}}\left(p_i\right)/T_m^{(p_i)}\right), \left(\mu_{\tilde{s}_j}\left(p_i\right)/T_m^{(p_i)}\right)\right) = \begin{cases} \min\begin{pmatrix} \max\left(1-\left(\mu_{\tilde{s}_{cur}}\left(p_i\right)/T_m^{(p_i)}\right), \left(\mu_{\tilde{s}_j}\left(p_i\right)/T_m^{(p_i)}\right)\right) \\ \max\left(1-\left(\mu_{\tilde{s}_j}\left(p_i\right)/T_m^{(p_i)}\right), \left(\mu_{\tilde{s}_{cur}}\left(p_i\right)/T_m^{(p_i)}\right)\right) \end{pmatrix}, \\ \text{IF}\begin{pmatrix} \left(\mu_{\tilde{s}_{cur}}\left(\tilde{p}_i\right)/T_m^{(p_i)}\right) \notin (1-\sigma, \sigma) \\ \text{?}\left(\mu_{\tilde{s}_j}\left(p_i\right)/T_m^{(p_i)}\right) \notin (1-\sigma, \sigma) \end{pmatrix}; \\ 1, \text{IF}\left(\mu_{\tilde{s}_{cur}}\left(p_i\right)/T_m^{(p_i)}\right) \in (1-\sigma, \sigma) \\ \text{OR}\left(\mu_{\tilde{s}_j}\left(p_i\right)/T_m^{(p_i)}\right) \in (1-\sigma, \sigma), \end{cases} \quad (12)$$

σ – the threshold of fuzzy equality of situations is 0.95.

The juxtaposition of fuzzy situations may be carried out based on one of the following approaches [19]:

– reduction of the multi-criteria evaluation problem to a single-criteria one based on the aggregation of the results of the comparison of individual features using different convolutions (additive, multiplicative, maximin, minimax, etc.);

– on individual or several priority features, while other features are considered additional, the matching results of which satisfy the set limit.

It is important to set fuzzy situations and determine the degree of fuzzy equality of situations in such a way that each time they are compared, there is one situation exceeding the fuzzy equality threshold.

Action 5. Determination of the target situation, strategy, and search for routes in a fuzzy graph.

Determining the target situation significantly affects the search for the best route in a fuzzy graph. At the same time, it is not always possible to predict its reach from an arbitrary current situation. This collision is resolved by adapting the fuzzy graph depending on the detected typical case of its adaptation and careful processing of routes.

Strategies for situational management of IS security parameters are formed sequences of control decisions that affect fuzzy situational features for the transition of a fuzzy graph from the current to the target situation.

As strategies of fuzzy situational management under different conditions of functioning of the fuzzy graph, the following can be chosen to achieve the target situation star, for example:

– maximizing the efficiency of IS message transmission (management strategy "Efficiency");

– minimization of the consumption of IS computing resources (management strategy "Savings");

– maximizing the reliability of messages transmitted to the IS (management strategy "Security");

– maximum average route weight – ratio of the sum of the weights of the control transitions included in the arc route to the number of these arcs according to one selected strategy (control strategy "Balanced");

– mixed strategies.

The restrictions imposed on the choice of route are requirements for intermediate situations, namely, for the composition and values of signs of unclear situations.

In order to ensure a greater possibility of choosing an appropriate fuzzy management strategy, a preliminary assessment (weighting) of each management decision is performed regarding the criteria of the relevant strategies.

Table 1 presents examples of management decisions and their weighting factors with respect to the criteria of the management strategy in question.

To achieve the target situation s_{tar} from the current one s_{cur} different routes may be involved (as a result of the execution of the corresponding sequences of control decisions), the choice of which depends on the given strategy of fuzzy situational control of the fuzzy graph.

Table 1

Management solutions and their weight solutions for various strategies for managing IS security parameters

Output situation	Final situation	Management decision	Managed parameter	The direction of influence of the management decision	The degree of influence of the management decision	Weight management solution for strategy «Security»	Weight management solution for strategy «Savings»	The weight of the control solution for the strategy «Efficiency»
...	...	...	...	...	...	...	...	...
S_k	S_5	R_{13}	p_2	Do not change	Weakly	0.9	0.1	0.2
S_k	S_j	R_{14}	p_2	Do not change	Average	0.8	0.2	0.3
...	...	...	...	...	...	...	...	...
S_4	S_3	R_{21}	p_1	Reduce	Weakly	0.8	0.7	0.5
S_4	S_6	R_{18}	p_1	Reduce	Average	0.5	0.5	0.7
S_4	S_K	R_{19}	p_1	Reduce	Strongly	0.2	0.3	0.4
...	...	...	...	...	...	...	...	...
S_2	S_3	R_c	p_m	Enlarge	Weakly	0.4	0.5	0.8
...	...	...	...	...	...	...	...	...
S_2	S_K	R_c	p_m	Enlarge	Strongly	0.1	0.9	0.6

Between the current (identified) s_{cur} but targeted s_{tar} different routes are possible by fuzzy situations of a fuzzy graph

$$\forall s_{cur}, s_{tar} \in S, s_{cur} \xrightarrow{D_{s_{cur},s_{tar}} \subset D} s_{tar} : D_{s_{cur},s_{tar}} = \\ = \left\{ d_b^{(s_{cur},s_{tar})} \mid b = 1,\ldots, B_{s_{cur},s_{tar}} \right\}, \quad (13)$$

where $B_{s_{cur},s_{tar}}$ – number of possible routes between situations s_{cur} and s_{tar}.

The choice of one or another route is carried out depending on the given strategy and is implemented in the form of the execution of a corresponding sequence of control decisions that translate a fuzzy graph through possible control transitions and intermediate situations from s_{cur} in s_{tar}.

So, after identifying the current situation s_{cur} the influence of a given management decision $r_{k_i}^{(p_i)} \in R$ on s_{cur} it is reduced to a fuzzy composition of a fuzzy set $\tilde{s}_{cur}$ and a vague relationship $\tilde{r}_{k_i}^{(p_i)}$. Then a fuzzy set is obtained $\tilde{s}_{mid}$ (defines some intermediate situation s_{mid}) mapped to fuzzy set $\tilde{s}_{fin}$ (defines a vague situation s_{fin}). If the given degree of similarity is exceeded, a conclusion is made about the transition of the fuzzy graph from the situation s_{cur} in the situation s_{fin}

$$\tilde{s}_{mid} = \tilde{s}_{cur} \cdot r_{k_i}^{(p_i)}, \tilde{s}_{fin} \approx \tilde{s}_{mid}. \quad (14)$$

After that, the assignment of the parameter of the current situation to the fuzzy graph of the reference values of the indicators can be performed s_{fin}.

Direct search and selection of routes in a fuzzy graph, taking into account the chosen strategy, can be carried out both by the iterative method and on the basis of known search algorithms in oriented weighted graphs, for example, Ford, Moore, Bellman, and Floyd.

Action 6. Adaptation of a fuzzy graph to changes in the hybrid composition model of IS.

Adaptation of a fuzzy graph is necessary if there are changes in the composite hybrid model based on the results of monitoring the state of IS components and the system in general.

Table 2 shows typical cases of fuzzy graph adaptation.

Table 2

Typical cases of fuzzy graph adaptation

A case of adaptation of a fuzzy graph	Characteristics
Case 1. Change in the set of fuzzy situational signs	Fuzzy situations, control solutions, control transitions, structure of the fuzzy graph, routes are set again
Case 2. Direct change in the composition of unclear situations	Additional control transitions are installed, the structure of the fuzzy graph is supplemented, and routes are changed
Case 3. Change in the composition of management decisions	Additional control transitions are installed, the structure of the fuzzy graph is supplemented, and routes are changed

Action 7. Determination of the amount of necessary computing resources of the IS.

In order to prevent looping of calculations on actions 1–6 of the specified technique and to increase the efficiency of calculations, the load of the IS is additionally determined. If the specified computational complexity threshold is exceeded, the number of software and hardware resources that must be additionally attracted is determined using the method proposed in work [19].

End.

5. 2. Effectiveness evaluation of the method of intelligent management of information system security parameters

In order to determine the effectiveness of the methodology of intelligent management of security parameters of information systems, its modeling was carried out when solving the task of intelligent management of security parameters of the special-purpose IS of the group of troops (forces) under the initial conditions specified in section 4.

Separate parts of the computational experiment, using the proposed method of intelligent management of IS security parameters, are given in the Tables 3, 4.

Table 3

Effectiveness evaluation of the proposed method of intelligent management of information system security parameters according to the criterion of prompt decision-making

Function name	Metrics	Canonical particle swarm algorithm [19]	Ant colony algorithm [19]	Black widow algorithm [19]	Grey wolf pack algorithm [19]	Cheetah pack algorithm [19]	Proposed methodology
1	2	3	4	5	6	7	8
U22-1	Average value	300.000	300.000	300.000	300.000	300.000	300.000
	Standard value	2.17547E-07	1.94448E-07	1.73866E-07	1.73121E-07	1.51021E-07	1.68168E-07
B22-2	Average value	400	400.265772	400.7973158	400.265772	400.3986579	399.5315429
	Standard value	4.9898E-08	1.011427534	1.621892282	1.011427535	1.216419212	1.368342398
B22-3	Average value	600.0071815	600.0644622	600.0240021	600.012832	600.031303	599.0449987
	Standard value	0.021632777	0.184980091	0.115606243	0.053463097	0.147011513	0.101164243
B22-4	Average value	826.5653461	827.3281442	823.8789639	826.3000191	826.2668486	828.7693662
	Standard value	9.13817552	8.364210734	11.30806963	8.186625055	9.136107323	9.07921317
B22-5	Average value	900.743876	900.9504411	900.9726169	900.8007883	900.5452042	899.2016312
	Standard value	0.781626306	1.424558753	1.275779755	0.903385622	0.635781924	1.578982565
B22-6	Average value	1888.524629	1874.869967	1876.294359	1847.184924	1888.926953	1855.878175
	Standard value	127.2561383	91.22185049	69.00003268	32.76980351	140.693674	29.57108747
H22-7	Average value	2027.479588	2030.758499	2029.556604	2032.238674	2028.177978	2052.128603
	Standard value	6.106897592	8.027195324	5.81348717	7.446489204	8.003968446	7.397733191

Continuation of Table 3

1	2	3	4	5	6	7	8
H22-8	Average value	2223.108804	2223.537417	2222.070633	2223.140251	2220.888475	2219.690533
	Standard value	4.749655105	2.963408213	4.895282849	3.995669404	5.451654006	5.347353983
H22-9	Average value	2510.930321	2510.930321	2536.358938	2498.216012	2523.644629	2499.216012
	Standard value	65.93880108	65.93880108	85.778947	48.38585173	77.58997694	47.38585173
C22-10	Average value	2594.615905	2596.833927	2585.256107	2591.210109	2605.304194	2618.308989
	Standard value	48.2013289	49.71807546	57.1034079	56.36586785	42.57395199	34.10382553
C22-11	Average value	2695.981932	2685.587394	2733.855734	2710.621315	2700.168413	2713.333781
	Standard value	116.3652035	110.1475838	146.333679	118.5098748	113.7913849	109.3008673
C22-12	Average value	2857.067086	2858.742176	2854.959949	2861.414681	2859.407788	2895.718769
	Standard value	9.364347909	14.88960231	5.539104327	17.96133754	15.00545163	15.34731781

Table 4

Effectiveness evaluation of the proposed methodology according to the criterion of reliability of decision-making

Function name	Metrics	Canonical particle swarm algorithm [19]	Ant colony algorithm [19]	Black widow algorithm [19]	Grey wolf pack algorithm [19]	Cheetah pack algorithm [19]	Proposed methodology
U22-1	Average value	0.66	0.73	0.67	0.68	0.8	0.94
	Standard value	0.7	0.73	0.68	0.69	0.83	0.95
B22-2	Average value	0.7	0.73	0.7	0.71	0.77	0.94
	Standard value	0.71	0.73	0.72	0.72	0.76	0.94
B22-3	Average value	0.68	0.73	0.7	0.71	0.76	0.92
	Standard value	0.69	0.73	0.69	0.73	0.77	0.93
B22-4	Average value	0.67	0.74	0.7	0.72	0.78	0.93
	Standard value	0.67	0.72	0.67	0.72	0.79	0.92
B22-5	Average value	0.6	0.71	0.64	0.73	0.8	0.93
	Standard value	0.61	0.72	0.64	0.74	0.88	0.93
B22-6	Average value	0.64	0.73	0.66	0.77	0.85	0.93
	Standard value	0.66	0.75	0.66	0.78	0.83	0.93
H22-7	Average value	0.67	0.72	0.68	0.75	0.81	0.91
	Standard value	0.68	0.71	0.69	0.74	0.83	0.94
H22-8	Average value	0.68	0.74	0.69	0.75	0.84	0.93
	Standard value	0.65	0.74	0.67	0.77	0.81	0.94
H22-9	Average value	0.64	0.75	0.66	0.69	0.83	0.94
	Standard value	0.7	0.72	0.71	0.71	0.84	0.93
C22-10	Average value	0.69	0.71	0.7	0.72	0.8	0.94
	Standard value	0.68	0.71	0.7	0.73	0.8	0.95
C22-11	Average value	0.67	0.71	0.69	0.71	0.82	0.94
	Standard value	0.67	0.72	0.68	0.74	0.91	0.94
C22-12	Average value	0.63	0.73	0.65	0.75	0.82	0.94
	Standard value	0.62	0.74	0.66	0.76	0.83	0.94

Table 4 shows the results of the assessment of the reliability of the decisions made for each of the decision optimization methods for making a decision on the management of IS security parameters.

From the analysis of Tables 3, 4, it can be concluded that the proposed technique ensures stable operation of the algorithm for the main test functions of the unimodal and multimodal form.

As can be seen from Tables 3, 4, increasing the security of IS is achieved by increasing the efficiency of decision-making at the level of 12–16% due to the use of additional procedures and ensuring the reliability of decisions made at the level of 0.94.

6. Discussion of the results of the development of the methodology of intelligent management of security parameters of information systems

The advantages of the proposed method of intelligent management of IS security parameters are the following:

– conduct a multi-level and systematic assessment of the state of IS security using the proposed set of analytical expressions. This will allow a comprehensive and objective assessment of the state of security of the IS, both its individual elements and the IS as a whole (expressions (1)–(14)), compared to works [4, 5];

– determine the influence of IS security parameters on each other when the IS security state changes due to the use of fuzzy analytical expressions (expressions (5)–(11)), compared to works [3, 7];

– construct multidimensional dependencies of the security state of the special-purpose IS (expressions (1)–(14)), which will allow to estimate the security of the IS by an arbitrary number of parameters, compared to works [9, 13];

–assess the security of the IS in conditions of incompleteness of information about the evaluation parameters (expressions (1)–(12)), which will allow solving the problem of dimensionality, compared to works [9, 12];

– build a time dependence of the change in parameters that characterize the state of security of the IS (expressions (1)–(14)), which allows to determine the moments of deviation of their values from the nominal, compared to works [11, 14];

– reduce errors in assessing the state of IS security due to the human factor during the verification of IS parameters (action 2), compared to works [4, 7];

– attract additional computing resources (if necessary) (action 7), which achieves the prevention of looping of the methodology's work, compared to research [13, 16];

– determine the influence of control decisions on a separately defined parameter for assessing the state of IS security (action 3.5–3.8), which achieves an increase in the accuracy of control influences compared to research [11, 15].

Among the disadvantages of the proposed method of IS intellectual security parameters, a slight loss of accuracy when converting security parameters to a fuzzy form should be attributed.

The proposed technique allows:

– simulate the state of IS security under the conditions of complex influence of destabilizing factors;

– identify effective measures to increase the level of IS protection;

– comprehensively assess the change in the level of IS protection during control effects on IS.

The limitations of the study are the need to take into account the delay time for collecting and proving information from IS sensors.

The proposed methodology should be used as software for automated troop control systems such as "Dzvin-AS", "Oreanda-PS", as well as integrated information systems such as "Delta".

7. Conclusions

1. The study proposes the main procedures of the method of intelligent management of information system security parameters. The features of the proposed methodology procedures are:

– conducting a multi-level and systematic assessment of the state of IS security using the proposed set of analytical expressions;

– determining the influence of IS security parameters on each other when the IS security state changes due to the use of fuzzy analytical expressions;

– constructing the multidimensional dependencies of the security state of the special-purpose IS, which evaluates the security of the IS based on an arbitrary number of parameters;

– assessing IS security in conditions of incompleteness of information about evaluation parameters, which solves the dimensionality problem;

– constructing the time dependences of changes in parameters that characterize the state of IS protection, which allows determining the moments of deviation of their values from the nominal;

– reducing the error of assessing the state of IS security due to the human factor through the verification of IS parameters;

– attracting additional computing resources (if necessary), which achieves the prevention of looping of the methodology;

– determining the influence of control decisions on a separately defined parameter for assessing the state of IS security, which achieves an increase in the accuracy of control influences.

2. The proposed technique provides an increase in IS security by increasing the efficiency of decision-making at the level of 12–16% due to the use of additional procedures and ensuring the reliability of decisions made at the level of 0.94, which is confirmed by the results of a computational experiment.

Conflict of interest

The authors declare that they have no conflict of interest in this study, including financial, personal, authorship or other nature that could affect the study and its results presented in this article.

Financing

The study was conducted without financial support.

Data availability

The manuscript has related data in the data warehouse.

Use of artificial intelligence tools

The authors confirm that they did not use artificial intelligence technologies when creating the presented work.

Authors' contributions

Hennadii Shapovalov: Conceptualization; Methodology; Project administration; Writing – original draft; Writing – review & editing; **Olha Salnikova:** Methodology; Writing; Writing – review & editing; **Yevhenii Kapran:** Writing – original draft; **Oleksii Kuvshynov:** Writing – review & editing; **Oleksii Nalapko:** Resources; Data Curation; **Viktor Yerko:** Validation; Data Curation; **Hryhorii Stepanov:** Software; Validation; Data Curation; **Ihor Borysov:** Methodology; Formal analysis; Visualization; **Oksana Dmytriieva:** Software: Programming, software development; designing computer programs; implementation of the computer code and supporting algorithms; testing of existing code components; Validation; Data Curation; **Andrii Shyshatskyi:** Software; Validation; Data Curation.

References

1. Sova, O., Radzivilov, H., Shyshatskyi, A., Shvets, P., Tkachenko, V., Nevhad, S. et al. (2022). Development of a method to improve the reliability of assessing the condition of the monitoring object in special-purpose information systems. Eastern-European Journal of Enterprise Technologies, 2 (3 (116)), 6–14. https://doi.org/10.15587/1729-4061.2022.254122
2. Dudnyk, V., Sinenko, Y., Matsyk, M., Demchenko, Y., Zhyvotovskyi, R., Repilo, I. et al. (2020). Development of a method for training artificial neural networks for intelligent decision support systems. Eastern-European Journal of Enterprise Technologies, 3 (2 (105)), 37–47. https://doi.org/10.15587/1729-4061.2020.203301
3. Sova, O., Shyshatskyi, A., Salnikova, O., Zhuk, O., Trotsko, O., Hrokholskyi, Y. (2021). Development of a method for assessment and forecasting of the radio electronic environment. EUREKA: Physics and Engineering, 4, 30–40. https://doi.org/10.21303/2461-4262.2021.001940
4. Pievtsov, H., Turinskyi, O., Zhyvotovskyi, R., Sova, O., Zvieriev, O., Lanetskii, B., Shyshatskyi, A. (2020). Development of an advanced method of finding solutions for neuro-fuzzy expert systems of analysis of the radioelectronic situation. EUREKA: Physics and Engineering, 4, 78–89. https://doi.org/10.21303/2461-4262.2020.001353
5. Zuiev, P., Zhyvotovskyi, R., Zvieriev, O., Hatsenko, S., Kuprii, V., Nakonechnyi, O. et al. (2020). Development of complex methodology of processing heterogeneous data in intelligent decision support systems. Eastern-European Journal of Enterprise Technologies, 4 (9 (106)), 14–23. https://doi.org/10.15587/1729-4061.2020.208554
6. Wang, J., Neil, M., Fenton, N. (2020). A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model. Computers & Security, 89, 101659. https://doi.org/10.1016/j.cose.2019.101659
7. Matheu-García, S. N., Hernández-Ramos, J. L., Skarmeta, A. F., Baldini, G. (2019). Risk-based automated assessment and testing for the cybersecurity certification and labelling of IoT devices. Computer Standards & Interfaces, 62, 64–83. https://doi.org/10.1016/j.csi.2018.08.003
8. Henriques de Gusmão, A. P., Mendonça Silva, M., Poleto, T., Camara e Silva, L., Cabral Seixas Costa, A. P. (2018). Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory. International Journal of Information Management, 43, 248–260. https://doi.org/10.1016/j.ijinfomgt.2018.08.008
9. Folorunso, O., Mustapha, O. A. (2015). A fuzzy expert system to Trust-Based Access Control in crowdsourcing environments. Applied Computing and Informatics, 11 (2), 116–129. https://doi.org/10.1016/j.aci.2014.07.001
10. Mohammad, A. (2020). Development of the concept of electronic government construction in the conditions of synergetic threats. Technology Audit and Production Reserves, 3 (2 (53)), 42–46. https://doi.org/10.15587/2706-5448.2020.207066
11. Bodin, L. D., Gordon, L. A., Loeb, M. P., Wang, A. (2018). Cybersecurity insurance and risk-sharing. Journal of Accounting and Public Policy, 37 (6), 527–544. https://doi.org/10.1016/j.jaccpubpol.2018.10.004
12. Cormier, A., Ng, C. (2020). Integrating cybersecurity in hazard and risk analyses. Journal of Loss Prevention in the Process Industries, 64, 104044. https://doi.org/10.1016/j.jlp.2020.104044
13. Hoffmann, R., Napiórkowski, J., Protasowicki, T., Stanik, J. (2020). Risk based approach in scope of cybersecurity threats and requirements. Procedia Manufacturing, 44, 655–662. https://doi.org/10.1016/j.promfg.2020.02.243
14. Perrine, K. A., Levin, M. W., Yahia, C. N., Duell, M., Boyles, S. D. (2019). Implications of traffic signal cybersecurity on potential deliberate traffic disruptions. Transportation Research Part A: Policy and Practice, 120, 58–70. https://doi.org/10.1016/j.tra.2018.12.009
15. Isong, A., Stephen, B. U.-A., Asuquo, P., Ihemereze, C., Enang, I. (2026). Machine learning based cloud computing intrusion detection. Advanced Information Systems, 10 (1), 115–125. https://doi.org/10.20998/2522-9052.2026.1.13
16. Zarreh, A., Saygin, C., Wan, H., Lee, Y., Bracho, A. (2018). A game theory based cybersecurity assessment model for advanced manufacturing systems. Procedia Manufacturing, 26, 1255–1264. https://doi.org/10.1016/j.promfg.2018.07.162
17. Zhuravskyi, Y. (Ed.) (2026). Intelligent decision support systems: methods for optimizing and supporting management decisions. Kharkiv: TECHNOLOGY CENTER PC. https://doi.org/10.15587/978-617-8360-23-8
18. Koval, M., Sova, O., Shyshatskyi, A., Artabaiev, Y., Garashchuk, N., Yivzhenko, Y. et al. (2022). Improving the method for increasing the efficiency of decision-making based on bio-inspired algorithms. Eastern-European Journal of Enterprise Technologies, 6 (4 (120)), 6–13. https://doi.org/10.15587/1729-4061.2022.268621
19. Shyshatskyi, A. (Ed.) (2024). Information and control systems: modelling and optimizations. Kharkiv: TECHNOLOGY CENTER PC. https://doi.org/10.15587/978-617-8360-04-7
20. Voznytsia, A., Sharonova, N., Babenko, V., Ostapchuk, V., Neronov, S., Feoktystov, S. et al. (2025). Development of methods for intelligent assessment of parameters in decision support systems. Eastern-European Journal of Enterprise Technologies, 4 (4 (136)), 73–82. https://doi.org/10.15587/1729-4061.2025.337528