UDC 004.81
DOI: 10.15587/1729-4061.2026.362504

DEVELOPING A SET OF MODELS TO SUPPORT INTELLIGENT DECISION SUPPORT 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
Yulii Zdanovskoi str., 81, Kyiv, Ukraine, 03680
ORCID: https://orcid.org/0000-0002-8979-0648

Vladyslav Shostak
Candidate of Technical Sciences, Chief of the Research Institute
State Research Institute of Aviation
Kazarmenna str., 6, Kyiv, Ukraine, 01135
ORCID: https://orcid.org/0000-0002-2956-1069

Oleg Sova
Corresponding author
Doctor of Technical Sciences, Professor, Head
Simulation Modeling Center*
E-mail: soy2311@gmail.com
ORCID: https://orcid.org/0000-0002-7200-8955

Viktor Pokaliuk
Doctor of Pedagogical Sciences, Associate Professor
Department of Fire and Rescue and Physical Training
National University of Civil Defence of Ukraine
Onopriyenko str., 8, Cherkasy, Ukraine, 18034
ORCID: https://orcid.org/0000-0001-8706-7096

Oleksandr Yefymenko
Candidate of Technical Sciences, Professor
Department of Construction and Road Machinery
Kharkiv National Automobile and Highway University
Yaroslava Mudroho str., 25, Kharkiv, Ukraine, 61000
ORCID: https://orcid.org/0000-0003-0628-7893

Elena Odarushchenko
Candidate of Technical Sciences, Associate Professor
Department of Information Systems and Technologies
Poltava State Agrarian University
Skovorody str., 1/3, Poltava, Ukraine, 36003
ORCID: https://orcid.org/0000-0002-2293-2576

Olesia Zhuk
Candidate of Technical Sciences, Associate Professor, Leading Researcher
Strategic Communications Institute*
ORCID: https://orcid.org/0000-0002-8974-0309

Bohdan Molodetskyi
Candidate of Technical Sciences, Chief Specialist
Research Institute of Military Intelligence
Yuriy Illenka str., 81, Kyiv, Ukraine, 04050
ORCID: https://orcid.org/0000-0002-2704-7963

Yevhen Sudnikov
Senior Researcher
Scientific Center of Distance Learning*
ORCID: https://orcid.org/0000-0003-2484-4972

Roman Lazuta
Junior Researcher
Research Center
Institute of Special Communications and Information Protection
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
Beresteiskyi ave., 37, Kyiv, Ukraine, 03056
ORCID: https://orcid.org/0000-0003-3254-9690
*National Defence University of Ukraine
Povitroflotskyi ave., 28, Kyiv, Ukraine, 03049

Intelligent decision support systems are the object of the study. The problem addressed in the study is the improvement of the validity of the functioning of intelligent decision support systems. The hypothesis of the study is the possibility of increasing the efficiency of the functioning of intelligent decision support systems due to the development of a set of mathematical models of their functioning.

The originality of the study consists of:

– comprehensive assessment of the state of functioning of intelligent decision support systems due to multi-level assessment;

– modeling of possible states of functioning of intelligent decision support systems;

– reconfiguring the number of input parameters to model the functioning process of intelligent decision support systems due to the use of evolving artificial neural networks, which achieves an increase in the efficiency and reliability of the received decisions and evaluations;

– setting the number of input channels of destructive influence for their accurate assessment due to the use of queuing theory;

– setting the input parameters of the models by adjusting the parameters of the membership function of evolving artificial neural networks, which achieves an increase in the accuracy of modeling the state of functioning of intelligent decision support systems.

Modeling of the proposed set of mathematical models of the functioning of intelligent decision support systems was carried out. In the course of modeling, it was established that an average of up to 20% gain is ensured in the efficiency and reliability of calculations, while ensuring an average level of use of hardware resources

Keywords: destabilizing factors, complex systems, efficiency of decision-making, modeling of complex systems

Received 04.03.2026
Received in revised form 18.05.2026
Accepted 25.05.2026
Published 26.06.2026

How to Cite: *Shapovalov, H., Shostak, V., Sova, O., Pokaliuk, V., Yefymenko, O., Odarushchenko, E., Zhuk, O., Molodetskyi, B., Sudnikov, Y., Lazuta, R. (2026). Developing a set of models to support intelligent decision support systems. Eastern-European Journal of Enterprise Technologies, 3 (4 (141)), 44–53. https://doi.org/10.15587/1729-4061.2026.362504*

1. Introduction

Intelligent decision support systems (IDSS) are the mathematical, software-hardware, and functional core of modern information, automation, and telecommunication systems for various purposes [1, 2]. IDSSs are currently used to solve a wide range of information and settlement tasks in the interests of a wide range of consumers [3, 4]:

– 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 changes in processes, events, including military conflicts, etc.

IDSS, which is used in the interests of special users, is subject to stricter requirements for the efficiency and reliability of heterogeneous data processing, complex reliability, etc. [5].

This is due to the peculiarities of the IDSS's functioning in the interests of special users and the conditions under which the systems in whose interests the specified IDSS are used operate.

The main features of the functioning of the IDSS for various functional purposes are:

– constant growth in the amount of information circulating in the middle of them and between the systems themselves;

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

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

– imperfection of the modeling mechanisms of the nature of the functioning of the IDSS in terms of taking into account the fullness of destabilizing factors of influence, etc.

Taking into account the above, one of the options for increasing the efficiency of the functioning of the IDSS is the development of a set of models for the functioning of intelligent decision support systems.

Therefore, studies devoted to the search for new ways to increase the efficiency of the functioning of IDSS under the influence of destabilizing factors are relevant.

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 IDSS for special-purpose information systems. 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 IDSS and does not take into account the qualitative factors that affect the cybersecurity of the information system.

Work [7] proposed a security certification methodology developed for information systems to enable various stakeholders to evaluate security solutions for large-scale information system deployments automatically. The methodology supports transparency regarding the level of security of information systems 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.

In work [9], a model of resource allocation of an automated special-purpose management system is proposed in conditions of insufficient information about the development of the operational situation. In the specified model, mechanisms for distributing resources of the automated control system 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 system, 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, this model does not allow working with various indicators.

The 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. The specified 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 the system.

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 model allows for the systematic evaluation of various insurance policies as a function of the likelihood that a cybersecurity breach will occur during the term of policy-related policies and premiums. 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 cybernetic 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.

In work [15], a method of synthesis of an information-analytical system for assessing the state of security of the level of protection of data transmission channels is proposed. 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.

The work [16] presents a method of creating and solving a game theory model for solving cybersecurity issues, specifically for advanced production 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. Below are considered well-known works that allow solving the specified shortcoming. Several different solutions have been proposed to eliminate this shortcoming.

Work [17] presents an approach to evaluating input data for support and decision-making systems. 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. It is shown that the method of analyzing hierarchies works well with complete initial information, but due to the need for experts to compare alternatives and choose evaluation criteria, it has a high proportion of subjectivism. For forecasting tasks in conditions of risk and uncertainty, the use of the theory of fuzzy sets and artificial neural networks is justified.

The analysis of works [6–20] showed that the common shortcomings of the above-mentioned studies are:

– modeling of each approach is carried out only at a separate level of IDSS functioning;

– with a complex approach, as a rule, two components of the functioning of the IDSS are considered. This does not allow to fully assess the impact of management decisions on their further functioning;

– the models listed above, constituting the constituent parts of the above approaches, provide weak integration into each other, which prevents them from being combined together to function together;

– the above models use a different mathematical apparatus, which does not require appropriate mathematical transformations, which in turn increases computational complexity and reduces the accuracy of modeling, etc.

All this allows to assert the expediency of researching the development of a set of models for the functioning of intelligent decision support systems.

3. The aim and objectives of the study

The aim of the study is to increase the reliability of the functioning of intelligent decision support systems under the influence of destabilizing factors by developing a set of models. This will allow complex and multidimensional modeling of the functioning of intelligent decision support systems (their individual elements) under the influence of destabilizing factors for the development of subsequent management decisions. Also, it will make it possible to develop (improve) the software of modern and promising intelligent decision support systems by integrating the proposed set of mathematical models into the corresponding software.

To achieve the aim, the following objectives were set:

– to develop a model for predicting the state of intelligent decision support systems;

– to develop a model of the dynamics of detection and elimination of software vulnerabilities;

– to develop a mathematical model of the functioning of intelligent decision support systems in conditions of antagonistic conflict;

– to evaluate the effectiveness of the proposed set of mathematical models.

4. Materials and methods

Intelligent decision support systems are the object of the study. The problem addressed in the study is the improvement of the validity of the functioning of intelligent decision support systems. The subject of the study is the process of modeling the functioning of intelligent decision support systems. The hypothesis of the study is the possibility of increasing the efficiency of the functioning of intelligent decision support systems due to the development of a set of mathematical models of their functioning.

The assumptions of this study should be considered, as due to the increase in the number of conditions and factors that are taken into account when modeling intelligent decision support systems, an increase in the reliability of their functioning will be achieved.

To simplify the modeling of intelligent decision support systems, it is accepted that the intensity and number of destabilizing influences are unchanged during the modeling.

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

– is a general scientific method of analysis for decomposing problematic issues of modeling the functioning of intelligent decision support systems 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 modeling the state of intelligent decision support systems when they perform tasks as intended;

– general scientific method of synthesis – to substantiate the most expedient approaches to modeling the process of

functioning of intelligent decision support systems when they perform tasks as intended;

– artificial neural networks evolving – to predict the state of functioning of intelligent decision support systems. The specified mathematical apparatus allows to perform information and calculation tasks regardless of their complexity, due to the possibility of changing the architecture and parameters of the membership function.

– queuing systems – to process applications for intelligent decision support software vulnerabilities. The advantage of said approach is the ability to perform parallel processing of software vulnerability detection in real time.

For modeling, this study adopted an intelligent decision support system that functions in the interests of the communication and informatization system of the operational grouping of troops (forces). 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.

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

The effectiveness of the set of proposed mathematical models of the functioning of intelligent decision support systems was evaluated during the functioning of the communication and informatization system of the operational grouping of troops (forces) during the defense operation. Multifunctional means of radio-electronic countermeasures capable of suppressing the operating frequency range from 30 MHz to 9 GHz, in the amount of 12 units, were considered as means of destabilizing influence. Means of cyber influence (12 units) operated on the radio channel together with noise blocking obstacles of means of radio-electronic countermeasures. Type of cyber impact: denial of service.

5. The results of the study on the development of a set of models for the functioning of intelligent decision support systems

5. 1. Model for forecasting the state of intelligent decision support systems

One of the main factors affecting the IDSS reliability is the presence of vulnerabilities in the software used by IDSS to solve information and calculation tasks.

To analyze the IDSS state, a forecast is needed regarding the dynamics of detecting vulnerabilities of the IDSS software, which can be used to destabilize its state. To destabilize the IDSS functioning, only those vulnerabilities are used that can be used to violate the integrity and availability of information in IDSS. At the moment, there are a number of analytical models for detecting vulnerabilities of IDSS software, which allow predicting their detection dynamics. The main and most common models used to solve the above problem are:

– Anderson thermodynamic model;

– Rescorley linear model;

– Rescorley exponential model;

– logarithmic Poisson model;

Alhazmi-Malaya logistics model et al.

At the same time, the models listed above are able to predict only the averaged trends in the change in the intensity of detection of IDSS software vulnerabilities, when in fact there are many more of them. To take into account the above-mentioned factors, it is proposed to use an approach for predicting the detection of vulnerabilities based on evolving artificial neural networks [17].

This approach involves the execution of two complex procedures using separate algorithms at each step.

At the first stage, data on previously detected IDSS vulnerabilities, obtained, as a rule, at moments of time, was pre-processed $t^{(1)}, \ldots, t^{(P)}$ with different intervals between adjacent moments. An appropriate processing algorithm should ensure their smoothing and interpolation for presentation as a continuous functional time dependence.

During pre-processing, it is proposed to restore dependence in the form of a weighted sum of radial-basic functions:

$$F(t)=\sum_{i=1}^{K} w_i\varphi_i(t)=w^T\varphi(t),$$

$$\varphi_i(t)=\varphi\left(\|t-u_i\|\right)=\exp\left[-\frac{\left(\|t-u_i\|\right)^2}{2\sigma_i^2}\right], \quad (1)$$

where $\varphi_i(t)$ – i-th radial-basic function; u_i – center i-th radial-basic function; σ_i – impact parameter i-th radial-basic function; w_i – corresponding weighting factor of the radial-base function; K – number of functions used.

Impact parameter i-th radial-basic function σ_i $(i=\overline{1,K})$ selected based on the rule

$$\sigma_i=C_1 du,\ C_1>0, \quad (2)$$

where du – the minimum distance between the centers of the radial-basic functions, and C_1 – some constant.

The number of radial-base functions is chosen to be equal to

$$K=\left[C_2\left(P-1\right)\right],\ 0<C_2\le 1, \quad (3)$$

where P – the number of moments of time for which the values of radial-basic functions are calculated, and C_2 – some constant.

When calculating the coefficients of the series, the solution of the overridden system of linear equations was carried out:

$$Gw=d, \quad (4)$$

$$G=\left\|g_{p,i}\right\|,\ g_{p,i}=\left\|\varphi_i\left(t^{(p)}\right)\right\|,$$

$$p=\overline{1,P},\ i=\overline{1,K},\ K<P,$$

where G – rectangular Green's matrix; $d=(d^{(1)},\ldots,d^{(P)})^T$ – a target vector defined from the original set of approximated data.

The solution of this system of linear equations is described by several methods, including the Gaussian least squares method, the Moore-Penrose pseudo-reverse matrix method, and the regularization method. The last method allows to take into account and a priori solution, which makes it possible to combine the advantages of a neural network forecasting algorithm and a vulnerability detection algorithm.

Solving the system of equations (2) by the regularization method

$$w=w^{(a)}+\left(G^TG+\alpha I\right)^{-1}G^T\left(d-Gw^{(a)}\right), \quad (5)$$

where $w^{(\alpha)}$ – a priori solution; α – a regularization parameter which may be selected by one of the standard methods; I – unit size matrix $K\times K$.

In this case, the parameter α it is proposed to determine based on the following condition (selection method): all values of the recovered dependency $F(t) = Gw$ should fall within the interval from $(Gw^{(a)} - \sigma^{(a)} : Gw^{(a)} - \sigma^{(a)})$, where $\sigma^{(\alpha)}$ – root mean square deviation of the recovered dependence $F(t) = Gw$ at $w = w^{(a)}$ from real data d, at the same time, inviscid $||Gw - d||$ – d should be minimal.

Selection of this parameter determination rule α due to the fact that, on the one hand, it is proposed to trust the a priori decision. On the other hand, it is proposed to limit the degree of trust in such a way that, with a slight deviation from it ($<\sigma^{(\alpha)}$) restored dependence $F(t) = Gw$ minimally different from real data d.

In the second processing step, prediction of smoothed and interpolated data using artificial neural networks, with an evolving architecture [19], is carried out.

5. 2. Model of dynamics of detection and elimination of software vulnerabilities

Sources of destabilizing influence (in this case, means of radio-electronic countermeasures (REC), cyber influence) negatively affect IDSS and their constituent parts. One of the approaches for modeling conflict interactions between sources of destabilizing influence and IDSS is to assess the dynamics of changes in the number of vulnerabilities in IDSS software.

It is necessary not only to predict the dynamics of identifying vulnerabilities that can be used to destabilize the functioning of the IDSS, but also to assess the intensity of countermeasures against identified vulnerabilities in the IDSS.

The average vulnerability elimination rate in IDSS is presented as follows

$$\mu = k\mu_v, \tag{6}$$

where μ_v – the average rate of changes to IDSS software, which eliminates a vulnerability in IDSS software, and k – the coefficient characterizing the efficiency of the functioning of the cyber protection subsystem of the IDSS.

Evaluation μ_v conducted as follows

$$\mu_v = \frac{1}{T_v}, \tag{7}$$

where T_v – the average time to make changes to the IDSS software, which closes the vulnerability after it is detected. For each IDSS software, the score μ_v it is carried out separately, because the speed of making changes to the IDSS software, depending on its complexity, is different.

The process of the appearance of new vulnerabilities of the IDSS software and their elimination as a process of the functioning of the mass service system (MSS) is presented. But it is assumed that the MSS entrance receives a non-stationary Poisson flow of applications (vulnerabilities) with intensity $\lambda(t)$, which depends on time t.

The vulnerability flow is non-stationary Poisson because it actually represents the sum of about 100 ÷ 1000 independent non-stationary flows with about the same intensity.

Next, the MSS services these applications (eliminates vulnerabilities) with intensity μ, which is calculated according to formula (6). It is assumed that work on eliminating each vulnerability begins immediately after its detection, accordingly, this MSS has an infinite number of service channels.

Under these assumptions, the average number of vulnerabilities in IDSS software at this point in time t calculated using the formula

$$N_{av}(t) = \frac{e^{-t}}{\mu}\left(\lambda(t) + \int_0^t \lambda(\tau)e^{\tau}\mathrm{d}\tau\right). \tag{8}$$

Subject to (6), (7), formula (8) is presented

$$N_{av}(t) = \frac{T_v e^{-t}}{k}\left(\lambda(t) + \int_0^t \lambda(\tau)e^{\tau}\mathrm{d}\tau\right), \tag{9}$$

where $\lambda(t)$ – intensity of vulnerability detection, T_v – the average time to make changes to the IDSS software that closes the vulnerability after it is detected, and k – coefficient characterizing the efficiency of the functioning of the cyber protection subsystem of the IDSS.

So, in this case, the average number of vulnerabilities in IDSS is equal to the average number of vulnerabilities detected in IDSS software during the entire observation time

$$N_{av}(t) = \int_0^t \lambda(\tau)\mathrm{d}\tau. \tag{10}$$

With these assumptions, the probability that IDSS is found in a specific software is found n vulnerabilities, equal to

$$P_n(t) = \frac{\left[N_{av}(t)\right]^n}{n!}e^{-N_{av}(t)}. \tag{11}$$

Thus, the probability of the absence of vulnerabilities in the IDSS software is equal to

$$P_0(t) = e^{-N_{av}(t)}. \tag{12}$$

The developed model takes into account the presence in practice of periods of increase and decrease in the number of vulnerabilities in IDSS software (increase and decrease in the probability of the absence of software vulnerabilities), and, therefore, is more acceptable for further use in modeling.

5. 3. Mathematical model of the functioning of intelligent decision support systems in conditions of antagonistic conflict

Several types of software are installed in IDSS. The simplest mathematical model of the functioning of IDSS in conditions of internal vulnerabilities and conflict interactions can be presented as a set of mass service systems. Each of these systems models the dynamics of vulnerabilities in each individual software.

In this case, the average number of vulnerabilities in IDSS will be the sum of the average number of vulnerabilities in each software used by IDSS:

$$N_{av}(t) = \sum_{m=1}^{M} N_{av}^{(m)},$$

$$N_{av}^{(m)}(t) = \frac{T_v^{(m)} e^{-t}}{k^{(m)}}\left(\lambda^{(m)}(t) + \int_0^t \lambda^{(m)}(\tau)e^{\tau}\mathrm{d}\tau\right). \tag{13}$$

The probability of the absence of vulnerabilities in the IDSS can be calculated according to formula (12), if instead of the average number of vulnerabilities in a specific software (9), it is substituted with the average number of vulnerabilities in the IDSS (13).

In the simplest case, when destabilizing factors affect all kinds of software installed in IDSS, and the vulnerabilities of

each software can be used directly to negatively affect IDSS. The potential probability that the reliability of the IDSS at the moment of time t not disturbed by the source of destabilizing influence, coincides with the probability of the absence of vulnerabilities in the IDSS

$$P_{rel}(t) = P_0(t). \tag{14}$$

This probability is of a potential nature, since its calculation does not take into account the characteristics of destabilizing factors that can negatively affect the IDSS, but only considers the potential possibility of such an impact.

Thus, the probability of reliability of a given IDSS for a given moment in time with respect to external destabilizing influence is calculated according to the following formula

$$P_{rel}(t) = P_0^{(CS)}(t) + P_0^{(PS)}(t)\left(1 - P_0^{(CS)}(t)\right), \tag{15}$$

where $P_0^{(CS)}$ – the probability of the absence of vulnerabilities in the cyber protection subsystem of the IDSS, and $P_0^{(PS)}$ – the possibility of no vulnerabilities in other IDSS software.

The mathematical model of the conflict is based on the representation of the process of changing the IDSS states – of the source of destabilizing influence in the form of a Markov chain with a finite number of states, the transitions between which are carried out according to the exponential (Poisson) law of distribution. Markov chain nodes correspond to the following states:

S_0 – the source of destabilizing influence lacks any information about IDSS;

S_1 – the source of destabilizing influence includes information about IDSS software;

S_{2m} – the source of the destabilizing impact has information about IDSS software and one vulnerability in this software;

S_{3m} $(m \in 1 \ldots M)$ – the source of the destabilizing impact has information about the IDSS software, about one vulnerability in this software, as well as about the procedure for using this vulnerability.

Let's denote the probabilities of being in the specified states accordingly P_0, P_1, P_{21}, ..., P_{2m}, ..., P_{2M}, P_{3m}, ..., P_{3M}.

State transition S_0 to S_1 carried out with intensity

$$\lambda_1 = \frac{1}{T_{ps}}, \tag{16}$$

where T_{ps} – the average time required by a source of destabilizing influence to find information about IDSS software. State transitions S_1 state S_{2m} $(m \in 1 \ldots M)$ carried out with intensity $P_{PS}^{(m)}\lambda_2$, where $P_{PS}^{(m)}$ – the probability of finding information about the vulnerability in the IDSS m-software, which is equal to

$$P_{PS}^{(m)} = \frac{N_{av\_conf}^{(m)}}{N_{av\_conf}}, \tag{17}$$

where $N_{av\_conf}^{(m)}$ – arithmetic average of the average number of vulnerabilities located in m-th software $N_{av}^{(m)}(t)$ IDSS during the consideration of the conflict; N_{av_conf} – arithmetic average of the average total number of vulnerabilities in IDSS software $N_{av}(t)$ during the consideration of the conflict.

The intensity of vulnerability detection in IDSS software is presented as follows

$$\lambda_2 = \frac{N_{av\_conf}}{T_{vul}}, \tag{18}$$

where T_{av} – the average time it takes for a source of destabilizing influence to find information about all vulnerabilities in IDSS.

Taking into account (17), (18) the intensity of transitions from the state S_1 in states S_{2m} $(m \in 1 \ldots M)$ equals

$$P_{PS}^{(m)}\lambda_2 = \frac{N_{av\_conf}^{(m)}}{T_{vul}}, \tag{19}$$

State transition S_{2m} $(m \in 1 \ldots M)$ in state S_{3m} $(m \in 1 \ldots M)$ has intensity

$$\lambda_3 = \frac{1}{T_{nv}}, \tag{20}$$

where T_{nv} – the average time it takes for a source of destabilizing influences to find information about how to use a vulnerability in IDSS software to influence IDSS.

To calculate the average time, from the moment the source of the destabilizing effects of the vulnerability to its elimination IDSS, it is proposed that the time of detection (appearance) of the vulnerability in m-th software $T_{search\_vul}^{(m)}$ is a random variable.

This is taken with equal probability of the value from the interval of the difference of the current time T_{now} and average life time vulnerability in m-th software $T_{life\_vul}^{(m)}$ until the current time T_{now}.

So, its mathematical expectation is equal to $T_{now} - \frac{T_{life\_vul}^{(m)}}{2}$, and the time from the moment of finding the source of destabilizing influence of information about vulnerability in m-th IDSS software until closing $T_{close}^{(m)}$ this vulnerability is accordingly equal to

$$T_{close}^{(m)} = \frac{T_{life\_vul}^{(m)}}{2}. \tag{21}$$

The average lifetime of the vulnerability in the IDSS m-software is calculated according to the formula

$$T_{life\_vul}^{(m)} = \frac{T_v^{(m)}}{k^{(m)}}, \tag{22}$$

where $T_v^{(m)}$ – the time required by the IDSS cyber protection subsystem m-th response software that closes the vulnerability, from the moment it is detected, $k^{(m)}$ – a factor reflecting the effectiveness of the IDSS cyber protection subsystem in eliminating vulnerabilities from m-th software.

Transitions from states S_{2m} $(m \in 1 \ldots M)$ and S_{3m} $(m \in 1 \ldots M)$ in state S_1 low intensity

$$\mu_m = \frac{1}{T_{close}^{(m)}}, \tag{23}$$

which, taking into account (21) and (22) levels

$$\mu_m = \frac{2k^{(m)}}{T_v^{(m)}}. \tag{24}$$

The resulting Markov chain is described by the vector of the initial probability distribution of finding in different states

$$P(0) = \begin{bmatrix} 1 & 0 & \ldots & 0 \end{bmatrix}, \tag{25}$$

and the transition matrix:

$$P_{tr}(t)=\exp(Qt),$$

$$Q=\begin{bmatrix} 1-\lambda_1 & \lambda_1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 1-\sum_{m=1}^{M} P_{SP}^{(m)}\lambda_2 & P_{SP}^{(1)}\lambda_2 & \dots & P_{SP}^{(M)}\lambda_2 & 0 & \dots & 0 \\ 0 & \mu_1 & 1-(\mu_1+\lambda_3) & \dots & 0 & \lambda_3 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \mu_M & 0 & \dots & 1-(\mu_M+\lambda_3) & 0 & \dots & \lambda_3 \\ 0 & \mu_1 & 0 & \dots & 0 & 1-\mu_1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \mu_M & 0 & \dots & 0 & 0 & \dots & 1-\mu_M \end{bmatrix}, \quad (26)$$

where Q – matrix of intensities of transitions between states of the chain; t – the current time counted from the beginning of the conflict.

Taking into account (17), (20), (21) and (25), this transition matrix took the form:

$$P_{tr}(t)=\exp(Qt),$$

$$Q=\begin{bmatrix} 1-\frac{1}{T_{ps}} & \frac{1}{T_{ps}} & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 1-\sum_{m=1}^{M}\frac{N_{av\_conf}^{(m)}}{T_{vul}} & \frac{N_{av\_conf}^{(1)}}{T_{vul}} & \dots & \frac{N_{av\_conf}^{(M)}}{T_{vul}} & 0 & \dots & 0 \\ 0 & \frac{2k^{(1)}}{T_v^{(1)}} & 1-\left(\frac{2k^{(1)}}{T_v^{(1)}}+\frac{1}{T_{nv}}\right) & \dots & 0 & \frac{1}{T_{nv}} & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \frac{2k^{(M)}}{T_v^{(M)}} & 0 & \dots & 1-\left(\frac{2k^{(M)}}{T_v^{(M)}}+\frac{1}{T_{nv}}\right) & 0 & \dots & \frac{1}{T_{nv}} \\ 0 & \frac{2k^{(1)}}{T_v^{(1)}} & 0 & \dots & 0 & 1-\frac{2k^{(1)}}{T_v^{(1)}} & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \frac{2k^{(M)}}{T_v^{(M)}} & 0 & \dots & 0 & 0 & \dots & 1-\frac{2k^{(M)}}{T_v^{(M)}} \end{bmatrix}. \quad (27)$$

Probability distribution at time t since the beginning of the conflict

$$P(t)=P(0)P_{tr}(t). \quad (28)$$

The probability of finding IDSS in a reliable state on n-th conflict steps

$$P_{find\_rel}(t)= =1-\sum_{m=1}^{M} P_{3m}(t). \quad (29)$$

The probability of IDSS finding in a reliable state for the entire time of the conflict is equal to the arithmetic average between the probabilities of finding the IDSS in a reliable state at each step of the conflict

$$P_{find\_rel\_conf}= =\frac{\int_0^{T_{conf}} P_{find\_rel}(t)\,dt}{T_{conf}}, \quad (30)$$

where T_{conf} – duration of the conflict. Taking into account (28), (29), formula (30) is transformed to the form

$$P_{find\_rel\_conf}=\frac{\int_0^{T_{conf}}\left(1-\sum_{m=1}^{M}\left(P(0)P_{tr}(t)\right)_{3m}\right)dt}{T_{conf}}. \quad (31)$$

To find the probability of IDSS reliability, the mathematical model should be simplified by removing transitions from states S_{3m} $(m\in 1\dots M)$ in state S_1, having thus made states S_{3m} $(m\in 1\dots M)$ absorbing.

The vector of the initial distribution of probabilities of finding in different states remains unchanged $P(0)=$ $=[1\ 0\ \dots\ 0]$, and the transition matrix is transformed to the form:

$$P_{tr}(t)=\exp(Qt),$$

$$Q=\begin{bmatrix} 1-\frac{1}{T_{ps}} & \frac{1}{T_{ps}} & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 1-\sum_{m=1}^{M}\frac{N_{av\_conf}^{(m)}}{T_{vul}} & \frac{N_{av\_conf}^{(1)}}{T_{vul}} & \dots & \frac{N_{av\_conf}^{(M)}}{T_{vul}} & 0 & \dots & 0 \\ 0 & \frac{2k^{(1)}}{T_v^{(1)}} & 1-\left(\frac{2k^{(1)}}{T_v^{(1)}}+\frac{1}{T_{nv}}\right) & \dots & 0 & \frac{1}{T_{nv}} & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \frac{2k^{(M)}}{T_v^{(M)}} & 0 & \dots & 1-\left(\frac{2k^{(M)}}{T_v^{(M)}}+\frac{1}{T_{nv}}\right) & 0 & \dots & \frac{1}{T_{nv}} \\ 0 & 0 & 0 & \dots & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & 0 & \dots & 1 \end{bmatrix}. \quad (32)$$

The probability of destabilization of IDSS during the conflict

$$P_{destab} = \sum_{m=1}^{M} P_{3m}\left(T_{conf}\right), \quad (33)$$

and the probability of reliability of IDSS, that is, the probability of not falling into a state of destabilization during the conflict, according to the same

$$P_{rel} = 1 - \sum_{m=1}^{M} P_{3m}\left(T_{conf}\right), \quad (34)$$

and taking into account (28)

$$P_{rel} = 1 - \sum_{m=1}^{M} \left(P(0)P_{tr}\left(T_{conf}\right)\right)_{3m}. \quad (35)$$

The above mathematical expressions described the process of functioning of intelligent decision support systems in conditions of antagonistic conflict.

5. 4. Evaluation of the effectiveness of the proposed mathematical models

The results of a computational experiment using the proposed set of mathematical models of the functioning of intelligent decision support systems are presented in the form of 205 pages of results. In this study, only the generalized results of this computational experiment are presented.

The results of the evaluation of the effectiveness of the set of proposed mathematical models of the functioning of intelligent decision support systems are given in the Table 1.

From the analysis of Table 1, it can be concluded that the proposed set of mathematical models provides an average of up to 20% gain in the efficiency and reliability of calculations in intelligent decision support systems, while ensuring an average level of use of hardware resources.

6. Discussion of the results of the development of a set of mathematical models of the functioning of intelligent decision support systems

Advantages of the proposed set of mathematical models of the functioning of intelligent decision support systems:

– comprehensively assess the state of operation of intelligent decision support systems (expressions (1)–(35)), compared to studies [2, 5];

– conduct modeling of possible states of functioning of intelligent decision support systems (expressions (1)–(35)), compared to studies [6, 10];

– reconfigure the number of input parameters to simulate the functioning of intelligent decision support systems by using evolving artificial neural networks (expressions (1)–(5)), which achieves an increase in the efficiency and reliability of the obtained decisions and evaluations, compared to studies [8, 15];

– adjust the number of input channels of destructive influence for their accurate assessment by using queuing theory (expressions (8)–(12)), compared to studies [7, 17];

– reduce the computational complexity of modeling destabilizing effects on intelligent decision support systems (expressions (1)–(35)) by using probabilistic and statistical approaches, compared to studies [12, 14];

– adjust the input parameters of the models by adjusting the parameters of the membership function of evolving artificial neural networks (expressions (1)–(5)), which achieves an increase in the accuracy of modeling the state of functioning of intelligent decision support systems, compared to studies [13, 16].

Table 1

A generalized comparative assessment of the effectiveness of the proposed set of mathematical models of the functioning of intelligent decision support systems

Model group	Basic methods	Efficiency under uncertainty	Accuracy	Efficiency class	Interpreting (Explainability)	Computational data requirements
Optimizing	Linear/dynamic programming	Low: require clear parameters and system limitations	High (allows to accurately determine the optimum)	Discrete	High: have a transparent logic for solving tasks	Low: only model parameters are required
Probabilistic, statistical	Bayesian networks, regressive analysis	Medium: work with risks and probabilities	Average: Strong dependence on data sampling	High	High: It is easy to establish the influence of factors on work efficiency	Average: representative statistics required
Expert (Knowledge bases)	Logical inference, fuzzy logic (Fuzzy Logic)	High: effectively simulate the human decision-making process	Average: limited by expert qualifications	High	Very high	Low to the data itself, high to the participation of experts
Machine learning (classical models)	Random Forest, SVM, Gradient boosting	High: High ability to detect hidden patterns	Very high for structured data	High	Average	High to volume and markup data
Neural networks (Deep learning)	MLP, CNN, LLM	Very high: ability to process unstructured data	Maximum on complex tasks	Variable	Low (black box "problem)	Critically high requirements for the GPU and data volume
Evolutionary	Genetic algorithm, evolutionary algorithms	Very high: ability to process unstructured data	Very high for structured data	Low	Average	Critically high requirements for the GPU and data volume
Proposed mathematical models (hybrid approach)	Artificial neural networks, MSS, probability theory	High	High (allows to accurately determine the optimum)	Average	High	Average hardware requirements

The disadvantage of the proposed set of mathematical models of the functioning of intelligent decision support systems should include the need for additional mathematical transformations when working with heterogeneous input parameters for modeling the state of intelligent decision support systems.

The proposed set of mathematical models of the functioning of intelligent decision support systems allows:

– conduct modeling of the process of assessing the state of functioning of intelligent decision support systems under the influence of several sources of destabilizing influence;

– determine effective measures to increase the efficiency of intelligent decision support systems under the complex influence of several destabilizing factors;

– comprehensively assess the state of functioning of intelligent decision support systems, etc.

Limitations of the study are the need to take into account the delay time for collecting and providing information from sensors (sensors) of intelligent decision support systems.

The proposed mathematical models 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. A model for forecasting the state of intelligent decision support systems was developed. The originality of the model consists of:

– comprehensive assessment of the state of functioning of intelligent decision support systems due to multi-level assessment, which achieves an increase in the reliability of modeling their state to an average of 15%;

– reconfiguring the number of input parameters for modeling the functioning of intelligent decision support systems due to the use of evolving artificial neural networks, which achieves an increase in the efficiency and reliability of the obtained decisions and evaluations by an average of up to 18%.

2. A model of the dynamics of detection and elimination of software vulnerabilities has been developed. The originality of the proposed model is:

– setting the number of input channels of destructive influence for their accurate assessment due to the use of queuing theory;

– to reduce the computational complexity of modeling the destabilizing effect on intelligent decision support systems by using probabilistic and statistical approaches, which achieves a reduction in the number of computational operations to an average of 12%.

3. A mathematical model of the functioning of intelligent decision support systems in the conditions of an antagonistic conflict was developed, the originality of which is:

– setting the input parameters of the models due to setting the parameters of the membership function of evolving artificial neural networks, which achieves an increase in the accuracy of modeling the state of functioning of intelligent decision support systems by an average of up to 13%.

– modeling of possible states of possible states of functioning of intelligent decision support systems.

4. Modeling of the proposed set of mathematical models of the functioning of intelligent decision support systems was carried out. In the course of modeling, it was established that an average of up to 20% gain is ensured in the efficiency and reliability of calculations, while ensuring an average level of use of hardware resources.

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; **Vladyslav Shostak**: Methodology; Writing; Writing – review & editing; **Oleg Sova**: Writing – original draft; **Viktor Pokaliuk**: Writing – review & editing; **Oleksandr Yefymenko**: Resources; Data Curation; **Olesia Zhuk**: Validation; Data Curation; **Elena Odarushchenko**: Software; Validation; Data Curation; **Roman Lazuta**: Methodology; Formal analysis; Visualization; **Bohdan Molodetskyi**: Software: Programming, software development; designing computer programs; implementation of the computer code and supporting algorithms; testing of existing code components; Validation; Data Curation; **Yevhen Sudnikov**: 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. Dahiya, A., Gupta, B. B. (2021). A reputation score policy and Bayesian game theory based incentivized mechanism for DDoS attacks mitigation and cyber defense. Future Generation Computer Systems, 117, 193–204. https://doi.org/10.1016/j.future.2020.11.027
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. Morales-Sáenz, F. I., Medina-Quintero, J. M., Reyna-Castillo, M. (2024). Beyond Data Protection: Exploring the Convergence between Cybersecurity and Sustainable Development in Business. Sustainability, 16 (14), 5884. https://doi.org/10.3390/su16145884
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. Shmatko, O., Yevseiev, S., Dudykevych, V., Milevskyi, S., Solnyshkova, S., Havrylova, A. et al. (2024). Development of a method for synthesizing an information-analytical system for assessing the level of information transmission channels protection. Eastern-European Journal of Enterprise Technologies, 2 (9 (128)), 36–43. https://doi.org/10.15587/1729-4061.2024.302495
16. Zarreh, A., Wan, H., Lee, Y., Saygin, C., Janahi, R. A. (2019). Cybersecurity Concerns for Total Productive Maintenance in Smart Manufacturing Systems. Procedia Manufacturing, 38, 532–539. https://doi.org/10.1016/j.promfg.2020.01.067
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