UDC 004.81
DOI: 10.15587/1729-4061.2026.352032

THE CREATION OF A METHODOLOGY FOR INTELLIGENT ASSESSING AND MANAGING THE SECURITY STATE OF COMPLEX SYSTEMS

Hennadii Miahkykh
Adjunct
Institute of Information and Communication Technologies and Cyber Defense*
ORCID: https://orcid.org/0000-0003-4491-5395

Oleg Sova
Corresponding author
Doctor of Technical Sciences, Professor Head of Center
Center of Simulation Modeling*
E-mail: soy135@ukr.net
ORCID: https://orcid.org/0000-0002-7200-8955

Olha Salnikova
Doctor of Science in Public Administration, Senior Research Fellow, Honored Worker of Science and Technology of Ukraine, Professor**
ORCID: https://orcid.org/0000-0002-7190-6091

Oleksandr Zhuk
Doctor of Technical Sciences, Professor, Head of Department
Department of Communication Technologies and Cyber Protection*
ORCID: https://orcid.org/0000-0002-3546-1507

Iraida Stanovska
Doctor of Technical Sciences, Professor
Department of Higher Mathematics and Modeling Systems
Odesa Polytechnic National University
Shevchenko ave., 1, Odesa, Ukraine, 65044
ORCID: https://orcid.org/0000-0002-5884-4228

Yevheniia Arkhypova
PhD, Associate Professor**
ORCID: https://orcid.org/0000-0002-1640-1488

Yuliia Vakulenko
PhD, Associate Professor
Department of Information Systems and Technologies
Poltava State Agrarian University
Skovorody str., 1/3, Poltava, Ukraine, 36003
ORCID: https://orcid.org/0000-0002-6315-0116

Oleksii Nalapko
Doctor of Philosophy (PhD)
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

Dmytro Balan
Senior Lecturer***
ORCID: https://orcid.org/0000-0002-6714-8718

Vitaliy Bereza
Lecturer***
ORCID: https://orcid.org/0009-0006-1758-3523

*National Defence University of Ukraine
Povitrianykh Syl ave., 28, Kyiv, Ukraine, 03049
**Department of Theory and Practice of Management
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
Peremohy ave., 37, Kyiv, Ukraine, 03056
***Department of Information Systems and Technologies
Military Institute of Telecommunications and Informatization named after Heroes of Krut
Knyaziv Ostroz'kykh str., 45/1, Kyiv, Ukraine, 01011

Complex technical systems are the object of the study. The problem that is solved in the study is an increase in the level of security of complex technical systems. The originality of the study consists in:

– comprehensive assessment of the security state of complex technical systems due to multi-level assessment using the theory of artificial intelligence;

– reduced error in assessing the security state of a complex technical system due to the human factor due to the verification of the parameters of a complex technical system;

– selection of the best individuals in bio-inspired algorithms, due to the use of an improved genetic algorithm, which achieves an increase in the efficiency and reliability of the obtained decisions and evaluations;

– make accurate decisions by individually adjusting the actions of agents in each bio-inspired algorithm;

– eliminating the conflict between agents in improved bio-inspired algorithms, which increases the efficiency and reliability of decisions made regarding the security state of complex technical systems;

– implementation of deep learning of knowledge bases of agents of each bio-inspired algorithm, due to the method of deep learning, which achieves an increase in the efficiency and reliability of assessments and control effects on the security state of complex technical systems.

Modeling of the proposed methodology was carried out, during which it was established that increasing the security of complex technical systems is achieved by increasing the efficiency of decision-making at the level of 15–17% due to the use of additional procedures and ensuring the reliability of decisions made at the level of 0.91.

This study can be used in practice when taking into account the delay time for collecting and proving information from sensors (sensors) of complex technical systems

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

Received 24.11.2025
Received in revised form 12.01.2026
Accepted 05.02.2026
Published 27.02.2026

How to Cite: *Miahkykh, H., Sova, O., Salnikova, O., Zhuk, O., Stanovska, I., Arkhypova, Y., Vakulenko, Y., Nalapko, O., Balan, D., Bereza, V. (2026). The creation of a methodology for intelligent assessing and managing the security state of complex systems. Eastern-European Journal of Enterprise Technologies, 1 (3 (139)), 24–34. https://doi.org/10.15587/1729-4061.2026.352032*

1. Introduction

The rapid technical development of mankind is leading to the continuous improvement of technical systems, which are becoming more complex and hierarchical [1, 2]. Complex technical systems are actively used to solve a wide range of tasks, such as [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 elements of complex technical systems, etc.

The main features of the functioning of complex technical systems of various functional purposes are [4, 5]:

– constant growth in the volume of information circulating in the middle of complex technical systems and between the systems themselves;

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

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

– imperfection of mechanisms for ensuring the security of complex technical systems during their functioning.

Taking into account the above, one of the options for increasing the efficiency of the functioning of complex technical systems is the development of a methodology for intellectual assessment and management of the security state of complex technical systems.

That is why research on the development of new approaches (or the improvement of existing ones) to intellectual assessment and the management of the security state of complex technical systems is relevant.

2. Literature review and problem statement

The work [6] proposes to use Bayesian hierarchical networks to determine the quantitative assessment of the level of cybersecurity risks in complex technical 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 information system and does not take into account qualitative factors that affect the cybersecurity of the information system.

Work [7] proposed a security certification methodology developed for complex technical systems to enable various stakeholders to evaluate security solutions for large-scale deployments in complex technical systems automatically. The methodology supports transparency regarding the level of safety in complex technical 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. This model has a flexible architecture; however, the proposed model also has disadvantages, including the accumulation of evaluation errors during the fuzzification and defuzzification procedures.

Work [9] proposes a model of resource allocation in complex technical systems under conditions of insufficient information about the development of the operational situation. In the specified model, mechanisms for the distribution of resources in complex technical systems 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. And also takes into account the operational situation and allows to predict the state of complex technical systems, 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 for assessing the functioning of the state of complex technical systems.

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 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.

The work [15] proposed to consider the cybersecurity of the 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.

Work [17] presents an approach to evaluating input data for complex technical 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. For the tasks of assessing the state of functioning of the state of complex technical systems in conditions of risk and uncertainty, the use of neuro-fuzzy expert systems is justified.

Work [20] states that the use of a combination of using different strategies for applying metaheuristic algorithms. The disadvantages of this approach are the insufficient efficiency of heterogeneous data processing when several metaheuristic algorithms are used together to evaluate the functioning of complex technical systems.

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

– assessment of the security of complex technical systems is carried out only at a separate level of their functioning, or only at a separate element of complex technical systems;

– with a comprehensive approach to assessing the security of complex technical systems, as a rule, one or two components of the process of their functioning are considered. This does not allow to fully assess the impact of management decisions on the further level of security of complex technical systems.

– 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 security of complex technical systems and their management;

– the above approaches for assessing the security state of complex technical systems use different mathematical apparatus. This requires appropriate mathematical transformations, which in turn increase computational complexity and reduce the accuracy of assessing the security state of complex technical systems, etc.

That is why further research should be directed to the development of theoretical provisions on increasing the level of security of complex technical systems.

3. The aim and objectives of the study

The aim of the study is to increase the level of security of complex technical systems due to the development of a methodology for intellectual assessment and management of their condition. This will allow a comprehensive and multidimensional assessment of the security state of complex technical systems at different levels of their functioning (individual elements) for the development of subsequent management decisions. Also, it will make it possible to develop (improve) the software of modern and promising complex technical systems by integrating the proposed methodology into the corresponding software.

To achieve the aim, the following objectives were set:

– to propose the structure of the methodology of intellectual assessment and management of the security state of complex technical systems;

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

4. Materials and methods

Complex technical systems are the object of the study. The hypothesis of the study is the possibility of increasing the level of security of complex technical systems due to the development of a methodology for intellectual assessment and management of the security state of complex technical systems. The subject of the study is the process of assessing and managing the security state of complex technical systems.

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

– is a general scientific method of analysis – for decomposing problematic issues of assessing the level of security of complex technical 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 assessing the level of security and managing the level of security of complex technical systems when they perform tasks as intended;

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

– advanced genetic algorithm – to select the most suitable individuals for the bio-inspired algorithms used in the study. This increases the reliability and efficiency of the operation of the specified algorithms when assessing the security state of complex technical systems and managing their level of security;

– artificial immune systems – to assess the level of security of complex technical systems. This allows flexible assessment of the level of security of complex technical systems for existing and promising destructive factors;

– is an improved wolf pack algorithm – for determining control solutions, for managing the level of security of complex technical systems. The specified improved algorithm ensures a high level of efficiency of decision-making while ensuring the given reliability.

As a sophisticated technical system for modelling, the present study adopted a system for communication and informatization 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 system and information systems – defence operation.

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.

5. The results of the research on the development of an approach to assessing and managing the security state of complex technical systems

5. 1. The structure of the methodology of intellectual assessment and management of the security state of complex technical systems

The method of intelligent assessment and management of the security state of complex technical systems consists of the following sequence of interrelated procedures:

Action 1. Entering output data into a complex technical system.

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

– the number of electronic warfare (EW) that affect a complex technical system (both own and enemy);

– the number of cyber-influencing tools that affect a complex technical system;

– intensity of cyber influence on a complex technical system;

– type of cyberattacks that act on a complex technical system;

– spectral-energy parameters of obstacles of EW means affecting a complex technical system;

– the number of means of fire damage that act in the lane of functioning of a complex technical system;

– intensity of fire impact on a complex technical system, etc.

Action 2. Verification of parameters of a complex technical system.

At this stage, with the help of an improved bio-inspired algorithm [19], the parameters of a complex technical system are verified. In case of detection of deviations from the input data, the output data is adjusted using the results of the bio-inspired algorithm.

Action 3. Determination of destabilizing factors affecting a complex technical system. In the specified action, the initial identification of the type and parameters of destabilizing factors that affect the functioning of a complex technical system takes place

$$CBT_{\mu}=\begin{cases}\left\langle F^{(i)}_{jL_{\mu}R_{\mu}},CBT_{L_{\mu}},CBT_{R_{\mu}}\right\rangle, \text{if } \#\mu\geq 2,\\ \mu, \qquad\qquad\qquad\qquad\qquad \text{if } \#\mu=1.\end{cases} \tag{1}$$

where $\mu=\{0,\ldots,m\}$ – the original set of class labels of destabilizing factors affecting a complex technical system, $L_{\mu}\subsetneq\mu$ – an arbitrarily generated or defined subset; $\mu\left(\#L_{\mu}<\#\mu\right)$, $R_{\mu}=$ $=\mu\backslash L_{\mu}$ – left classification subtree, $CBT_{R_{\mu}}$ – right classification subtree, $F^{(i)}_{jL_{\mu}R_{\mu}}$ – a nodal detector trained on the elements of a set $\left\{\left(x_l,0\right)\middle|\overline{c}_l\in L_{\mu}\right\}_{l=1}^{M}\bigcup\left\{x_l,1\middle|\overline{c}_l\in R_{\mu}\right\}_{l=1}^{M}$.

Action 4. Modeling possible scenarios for the functioning of a complex technical system.

In the course of performing the specified procedure, with the help of the polymodel complex of functioning of complex technical systems developed in study [19], possible scenarios for the subsequent formation are simulated.

Action 5. Initial assessment of the security state of the functioning of complex technical systems.

At the specified stage, the initial assessment of the security state of complex technical systems takes place using the evaluation method proposed in study [19].

Action 6. Determination of control effects on the level of security of complex technical systems.

On the basis of the initial data obtained from the previous actions of the methodology, the formation of appropriate control influences takes place to increase the security of a complex technical system. For this purpose, an advanced bio-inspired algorithm developed in study [19] is used.

Action 6. 1. Selection of the best people from the population. In the course of performing the specified action, the best persons from the population are selected using the improved genetic algorithm proposed in the study [19].

Action 6. 2. Correcting the actions of each agent in a multi-agent algorithm.

In order to increase the efficiency of determining the security controls of complex technical systems, it is necessary to coordinate the actions of all agents in the multi-agent algorithm. That is why it is proposed to use conflict-oriented search [11] to increase the effectiveness of the solutions found by each of the agents.

This approach is especially relevant in conditions where a complex technical system operates in the condition of a shortage of computing resources with the simultaneous influence of a set of destabilizing factors on it.

Conflict-oriented search is two-level. At the upper level, the specified approach operates with various partial solutions, and at the lower level – carries out the planning of individual trajectories of agents. By partial solution is meant a set of trajectories satisfying some set of constraints imposed on agents that may contain conflicts. Let's consider the specified approach in more detail.

Action 6. 2. 1. Individual planning of the movement of agents in the population.

Individual trajectories of agents in a multi-agent algorithm, planned independently, are as follows:

$$\pi_b=\left\{\left(A\to B,\sqrt{5}\right),\left(B\to F,\sqrt{11}\right)\right\},$$

$$\pi_g=\left\{\left(D\to E,2.0\right),\left(E\to C,2\sqrt{2}\right)\right\}. \tag{2}$$

However, if both agents begin to simultaneously perform the planned trajectories, they will collide. At the same time, it is not possible to attribute the place of collision to any one vertex or edge of the graph.

Action 6. 2. 2. Determination of the type of conflict between agents in a multi-agent algorithm.

The conflict occurs between the actions of agents and its presence depends on at what points in time the agents in the multi-agent algorithm will begin to carry them out. So, let's denote the conflict as follows.

Set $\left\langle i,j,\left(a_i,t_i\right),\left(a_j,t_j\right)\right\rangle$ is a conflict denoted as *InConflict*$((a_i, t_i), (a_j, t_j))$ in those cases when

$$\exists t \in \left[t_i, t_i + a_{iD}\right] \cap \left[t_j, t_j + a_{jD}\right] : InCollision \begin{pmatrix} i, j, \\ a_{i\varphi}\left(t - t_i\right), \\ a_{j\varphi}\left(t - t_j\right) \end{pmatrix}. \quad (3)$$

The difficulty of verifying the existence of a conflict between a pair of actions a_i and a_j depends on the form of the agents i, j, and also from the corresponding functions of movement $a_{i\varphi}$, $a_{j\varphi}$. In the conducted model experimental studies, agents are modeled by radius disks r, and when performing movement actions, agents move straight along the edge of the graph at a constant speed.

In the general case where agents have an arbitrary body shape and can also move in curvilinear trajectories at a changing speed, the task of determining the conflict between a pair of actions is non-trivial.

To verify the existence of a conflict between a pair of actions, it is necessary to find the minimum distance between agents, which is achieved in the process of performing these actions. And therefore, the approach proposed in work [19] can be used. This approach allows the calculation of the minimum distance between a pair of agents, given the initial positions and directions of movement

$$\left\| \left(a_{i\varphi}(0) + v_i \tau\right) - \left(a_{j\varphi}(0) + v_j \tau\right) \right\| = r_i + r_j, \quad (4)$$

where $a_{k\varphi}(0)$ – initial position of the agent, v_k – motion speed vector, r_k – agent radius, $k = i, j$.

This expression can be converted to a quadratic form

$$\left(x \cdot x\right)\tau^2 + 2\left(x \cdot y\right)\tau + x \cdot y - \left(r_i + r_j\right)^2 = 0, \quad (5)$$

where $x = a_{i\varphi}(0) - a_{j\varphi}(0)$, $y = v_i - v_j$.

By calculating the roots of this equation, it is possible to determine whether the sum of the radii of the agents will exceed the minimum distance between them and at what time. D used to denote the discriminant of the equation, and τ_1 and τ_2 as roots of the equation. All possible solutions to this equation are considered below:

– $D < 0 : \nexists \tau_1, \tau_2$ – there is no conflict in the actions of agents, since the distance between agents never becomes less than $2r$. This situation is possible only in those cases when the agents move along parallel lines, or one of the agents expects and has a zero speed vector;

– $D = 0 : \tau_1 = \tau_2$ – there is only one point in time when the distance between the agents is $2r$. That is, in the process of performing actions, agents approach the distance $2r$. This case is not a conflict, because for a conflict to exist, the distance between agents must be strictly less than $2r$;

– $D > 0 : \tau_1 \neq \tau_2$ – there is a time interval (τ_1, τ_2) during which the distance between agents is less than the sum of their radii. Conflict occurs if this interval has an intersection with a time interval when both agents perform appropriate actions: $\left(\tau_1, \tau_2\right) \cap \left[\max\left(t_i, t_j\right), \min\left(t_i + a_{iD}, t_j + a_{jD}\right)\right] \neq \varnothing$.

It is worth noting that in order to apply this approach, it is necessary that both actions start simultaneously. Therefore, in those cases when agents begin to perform their actions at different moments of time, the position of the agent, which begins its action earlier, shifts to the position in which it will be the second agent at the time of the start of the action. Agent i begins to do its action at a time t_i, and the agent j – at the moment t_j. If to assume that the agent i starts doing its action earlier: $t_i < t_j$, then to verify the existence of a conflict between actions (a_i, t_i) and (a_j, t_j) agent position i it is necessary to shift to $a_{i\varphi}(t_j - t_i)$. So, for $O(1)$ it is possible to clearly determine the existence of a conflict between a pair of actions.

Action 6. 2. 3. Checking the presence of conflicts between a pair of agent trajectories.

By having a procedure to check for conflicts between a pair of actions, it is possible to check for a conflict between a pair of trajectories. To determine the conflict between a pair of trajectories π_b and π_g, it is necessary to consider them in the form of a sequence of pairs of actions and moments of time: $\pi_b = \{(A \to B, \sqrt{5}), (B \to F, \sqrt{11})\}$, $\pi_g = \{(D \to E, 2.0), (E \to C, 2\sqrt{2})\}$. When comparing each possible combination of action pairs, it is necessary to check $(\left|\pi_b\right| + \left|\pi_g\right|)^2$ a couple of actions where $|\pi|$ – the number of actions that make up the trajectory π. However, conflict between agents is possible only in cases where appropriate actions:

– intersect in time

$$t_i \leq t_j < t_i + a_{iD} \wedge t_j \leq t_i < t_j + a_{jD}. \quad (6)$$

– can intersect in space

$$\min\_dist\left(a_i, a_j\right) < 2r. \quad (7)$$

In other words, if one action begins after the other has already ended, then a conflict between such a pair of actions is impossible. Conflict is also impossible if the actions of the agents take place in different places of the workspace and therefore the distance between the agents in the process of performing these actions cannot be less than the sum of their radii.

In order to check only those pairs of actions that have a time intersection, the procedure uses two counters n and m, which indicate the current analyzed action in the trajectory π_i and π_j accordingly. First, both counters indicate the first actions in the trajectories. Then, if the first action of the agent i ends before the first act of the agent j, then the value of the counter increases n and the conflict between the second action of the agent is checked i and the first action of the agent j.

Otherwise, the value of the counter increases m and the conflict is checked between the agent's second action j with the first action of the agent i. The process is repeated and at each step the value of the counter of the trajectory, which action ended earlier, increases. If both actions ended at the same time, then the value of the counter increases m. The process continues until both counters reach values equivalent to the number of actions in the trajectories π_i and π_j. In other words, the procedure works until all actions included in the trajectory are checked π_i and π_j.

Action 6. 2. 4. Calculation of interval limits to eliminate conflict between agents.

Let the conflict be found $InConflict\left(\left(a_i, t_i\right), \left(a_j, t_j\right)\right)$. To eliminate it, it is necessary to impose restrictions on agents I and j, creating two new vertices of the restriction tree – N_i and N_j. Agents in the classical formulation of the problem are subject to species restrictions $\langle i, x, t\rangle$, where x – edge or vertex of a graph G. In the considered formulation of the problem, it is proposed to impose restrictions not on provisions, but on actions.

Moreover, it is not sufficient to prohibit an agent from carrying out an action at only one particular point in time t, because it will be able to implement it at a time $t + \varepsilon$, which will again lead to conflict between the same pair of actions. Therefore, it is proposed to impose restrictions not on isolated moments of time, but on intervals during which agents are unable to perform actions a_i and a_j accordingly. The interval has the form $[t, t^u)$, where t^u –the first point in time when an agent can begin to perform an appropriate action without conflict with the action of another agent.

To eliminate the conflict *InConflict*$((a_i, t_i), (a_j, t_j))$ one of the agents is subject to a set limit $\left\langle k, a_k, \left[t_k, t_k^u\right)\right\rangle$. The restriction prohibits the agent k perform action a_k during the conflict interval $\left[t_k, t_k^u\right)$, where t_k^u – the first point in time when the agent k may start an action a_k without creating a conflict with the action of another agent ($k = i, j$). In case if $k = i$, value t_k^u defined as follows

$$t_i^u = \arg\min_{t\in\left[t_i, t_j + a_{jD}\right]}\left\{InConflict\left(\begin{matrix}(a_i, t_i),\\ (a_j, t_j)\end{matrix}\right) = False\right\}. \qquad (8)$$

Interval $\left[t_i, t_i^u\right)$ is called conflicting because if the agent i will start performing an action a_i at any point in time during the interval $\left[t_i, t_i^u\right)$, then there will be a conflict with the action a_j, what an agent j starts to perform at a time t_j. It is worth noting that if the conflict occurs with an agent, which has already completed its trajectory and is in its target position, then the check *InConflict*$((a_i, t_i), (a_j, t_j))$ will always give value *true*. In this case, the value t_i^u set equal $+\infty$. In other cases, a moment in time t_i^u it is guaranteed to exist and is finite, because in the worst case, the conflict between the analyzed pair of actions will end at the moment of time $t_j + a_{jD}$, that is, when another agent finishes performing its action.

Thus, to eliminate the conflict *InConflict*$((a_i, t_i), (a_j, t_j))$, what is contained in the set of trajectories $N.\Pi$, two new constraint tree vertices are created N_i and N_j, in each of which an additional restriction is added $\left\langle i, a_i, \left[t_i, t_i^u\right)\right\rangle$ and $\left\langle j, a_j, \left[t_j, t_j^u\right)\right\rangle$ accordingly.

To calculate the restrictions imposed on agents to eliminate conflicts, it is necessary to calculate the conflict interval, that is, the time interval during which the agent cannot perform the corresponding action. The procedure for calculating interval limits, like the procedure for identifying conflicts, depends on what form the agents take and what movement model they have. Before describing this approach, let's introduce the following notations:

– P_i, P_j – initial provisions of agents i and j accordingly;

– V_i, V_j – directions of movements of agents i and j accordingly;

– δ – the duration of the waiting period that the agent needs to make to avoid conflict.

To calculate the value δ the following equation must be solved

$$sqEdgeDist(t, \delta) = At^2 + Bt\delta + C\delta^2 + Dt + E\delta + F, \qquad (9)$$

where:

$$A = \left(V_i - V_j\right)^2,\ B = 2\left(V_i^2 - V_i \cdot V_j\right),\ C = V_i^2,$$

$$D = 2\left(P_j + P_i\right)\left(V_j - V_i\right),\ E = -2\left(P_j \cdot V_i + P_i \cdot V_j\right),$$

$$F = \left(V_i - V_j\right)^2 - \left(r_i + r_j\right)^2.$$

The issue to be resolved is the amount of delay that must be made to the agent so that the agents stop colliding and the minimum distance between them reaches $r_i + r_j$.

The amount of delay required is determined by the upper and lower extrema of the ellipse [4]

$$delayRange = center_\delta \pm$$
$$\pm\frac{\sqrt{\left(2BD - 4AE\right)^2 + 4\left(4AC + B^2\right)\left(D^2 - 4AF\right)}}{2\left(4AC - B^2\right)}, \qquad (10)$$

where $center_\delta = \left(BD - 2AE\right)/\left(4AC - B^2\right)$.

The values of the ends of conflict intervals are determined through the expression

$$collisionTimes = \frac{\left(-B\left(delayRange\right) - D\right)}{2A}. \qquad (11)$$

Since the actions of the agents are finite, it is also necessary to take into account the moments of the end of the actions of the agents. When movements of agents i and j begin in t_i and t_j and end in t_i' and t_j' accordingly, calculations of the conflict interval are carried out with respect to moments $t_0 = \min(t_i, t_j)$ and $t_{\max} = \min\left(t_i', t_j'\right)$. In cases where $\delta = (t_i - t_j)$ out of range *delayRange*, calculated for (10), there is no conflict between agents.

Action 7. Learning the knowledge bases of the agents of each bio-inspired algorithm. In the specified methodology, two bio-inspired algorithms are used to assess the security state and produce control influences to increase the security of a complex technical system. To increase the efficiency and reliability of the decisions made, the work uses an improved algorithm for deep learning of agents' knowledge bases, which is proposed in the study [19].

Action 8. Determining the amount of necessary computing resources for a complex technical system.

In order to prevent looping of calculations on Actions 1–7 of the specified methodology and increase the efficiency of calculations, the load of a complex technical system 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. Evaluation of the effectiveness of the proposed methodology

5. 2. 1. Theoretical confirmation of the effectiveness of the proposed methodology

Statement 1. It is ensured that the solution is obtained provided that it exists, and also guarantees the correct completion of the work in the absence of a solution.

Proof. Let some state be given $s = \langle cfg, interval\rangle$. This state can be reached at various points in time during a safe state interval s. Let two moments of time be given t_0, t_1, such that: $t_0 \in interval$, $t_1 \in interval$, $t_0 < t_1$. Any action that can be taken from the state s, achieved at a time t_1, can be done from the state s, achieved at the moment of time t_0. This is possible because, having reached the state s at a time t_0, the agent can make a waiting action until the moment t_1. At the same time, the agent of the multi-agent algorithm can always perform an expectation action, because both moments of time belong to the same safe interval. Thus, by reaching the state at the minimum possible time, all possible states of the offspring are generated in the disclosure step, which can be reached from the current state being disclosed. Therefore, having only one moment of time for each safe interval, any states of the descendant are not lost. In this way, finding a solution is guaranteed, provided that it exists.

The correctness of the completion of the work is based on two facts. First, each state can be disclosed no more than once. After removing a state from the OPEN list, it is added to the CLOSED list and can no longer be added to the OPEN list for rediscovery. Second, the number of states is finite. First, in the initialization step, for each vertex $v \in V$ one state is created with a safe interval $[0, +\infty)$.

Then, each constraint from the set *Cons* imposed on the waiting action can divide one safe interval into two subintervals and result in two states instead of one. So, the total number of states is absorbed into the value $|V| + |Cons|$. Thus, having a finite number of states, each of which can be solved no more than once, the work will be completed for a finite number of iterations even in those cases when the solution to the problem does not exist.

Statement 2. Each solution found has the minimum possible cost.

Proof. The proof of this statement is essentially a consequence of the proof of Statement 1. The cost of the trajectory of the time equivalent of reaching a state corresponding to the target position at which the safe interval has an infinite duration. Due to the fact that any state is reached at the minimum possible moment of time, the trajectory of the minimum possible cost is found when reaching the target state.

Let P – multiple multi-agent planning tasks, P^+ – a subset of all multi-agent planning tasks that have solutions, and P^- – a subset of all non-solution multi-agent scheduling tasks.

For any task p from the plural P^+ there are many solutions $\Pi(p)$. The set of solutions is also divided into two subsets

$$\Pi(p) = \Pi_{opt}(p) \cup \Pi_{subopt}(p),$$

where $\Pi_{opt}(p)$ – a subset of all optimal solutions, and $\Pi_{subopt}(p)$ – subset of all suboptimal solutions:

$$\forall \Pi \in \Pi_{opt}(p), \forall \Pi' \in \Pi(p): cost(\Pi) \leq cost(\Pi'),$$

$$\forall \Pi \in \Pi_{subopt}(p), \forall \Pi' \in \Pi_{opt}(p): cost(\Pi) > cost(\Pi'). \quad (12)$$

Definition. Let a set of optimal solutions be given $\Pi_{opt}(p)$ some task that needs to be solved p, and also a couple of interval constraints $\left\langle i, a_i, \left[t_i, t_i^u\right)\right\rangle$ and $\left\langle j, a_j, \left[t_j, t_j^u\right)\right\rangle$. Let's call a pair of constraints consistent if any optimal solution satisfies at least one of the constraints:

$$\forall \Pi \in \Pi_{opt}(p), \forall \pi_i, \pi_j \in \Pi: \left(a_i, t_i'\right) \notin \pi_i,$$

$$\forall t_i' \in \left[t_i, t_i^u\right) \vee \left(a_j, t_j'\right) \notin \pi_j, \forall t_j' \in \left[t_j, t_j^u\right). \quad (13)$$

In other words, if a pair of constraints is consistent, then no solution from the set $\Pi_{opt}(p)$ cannot include both actions carried out at times belonging to conflict intervals on which an agreed pair of constraints has been imposed.

Lemma 1. For arbitrary conflict *InConflict*$((a_i, t_i), (a_j, t_j))$, restrictions $\left\langle i, a_i, \left[t_i, t_i^u\right)\right\rangle$ and $\left\langle j, a_j, \left[t_j, t_j^u\right)\right\rangle$ is an agreed pair of constraints.

Proof. Let some partial solution be given Π, which contains a conflict *InConflict*$((a_i, t_i), (a_j, t_j))$. To eliminate this conflict, it is necessary to impose restrictions on one of the agents involved in the conflict, or $\left\langle i, a_i, \left[t_i, t_i^u\right)\right\rangle$, or $\left\langle j, a_j, \left[t_j, t_j^u\right)\right\rangle$.

It can be assumed that this pair of restrictions is not agreed upon, that is, there is such a non-conflict solution:

– in which agent i performs action a_i at some point t_i' during the interval $\left[t_i, t_i^u\right)$;

– agent j performs action a_j at some point t_j' during the interval $\left[t_j, t_j^u\right)$ and at the same time, actions arise that lead to the emergence of a conflict.

It is known that if the agent i will start taking action a_i at the moment t_i, and the agent j will start taking action a_j at the moment t_j, this will lead to the emergence of a conflict. Therefore, by synchronously shifting the moments of the beginning of both actions, the conflict between actions will remain: *InConflict*$((a_i, t_i + \delta), (a_j, t_j + \delta))$, $\forall \delta \in R$. However, the displacement of the moment of the start of the action for the agents i and j can be different. Let's enter the notation $\delta_i = t_i' - t_i$ and $\delta_j = t_j' - t_j$. Let's content the moments of the start of actions by the value min (δ_i, δ_j).

The situation when $\delta_i \leq \delta_j$ but let's shift the moments t_i' and t_j' by magnitude $-\ \delta_i$. In this case, the agent j will start taking action a_j at a time t_j, and the agent i – at the moment $t_i' - \delta_i$. At the same time, the moment of the start of the action by the agent i belongs to the interval $\left[t_i, t_i^u\right)$, because, firstly, the situation in which is considered $t_i' \in \left[t_i, t_i^u\right)$, secondly, $t_i' = t_i + \delta_i$ and $\delta_j \leq \delta_i$, so $t_i + \delta_i - \delta_j \geq t_i$.

The assumption made at first indicates that between actions $\left(a_i, t_i'\right)$ and $\left(a_j, t_j'\right)$ there is no conflict, therefore, between actions $\left(a_i, t_i' - \delta_j\right)$ and (a_j, t_j) there is no conflict either. However, this statement contradicts Definition 5, which states that t_i^u – the first point in time when the agent i can take an action a_i no conflict with action a_j, what an agent j begins to act at a moment in time t_j. The resulting contradiction proves that several constraints given according to Definition 5 are consistent.

Let an arbitrary multi agent planning problem be given p, what has a solution, $p \in P^+$, and also some solution of the specified task, which is denoted as Π_{CCBS}.

Theorem 1. $\forall p \in P^+: \Pi_{CCBS} \in \Pi_{opt}(p)$ – the solution found for any problem to be solved is optimal.

Proof. The root of the constraint tree is created during initialization N_0, which contains a set of trajectories planned independently. The root of the tree does not contain any constraints, hence any solution from the set Π_{opt}, first, has a value not less than the value of the original partial solution $cost(N_0.\Pi)$, secondly, satisfies all its limitations due to their absence.

If a set of trajectories $N_0.\Pi$ contains no conflicts, the necessary solution has been found. Otherwise, a set of trajectories $N_0.\Pi$ contains at least one conflict *InConflict*$((a_i, t_i), (a_j, t_j))$. Two new constraint tree vertices will then be created N_1, N_2, containing restrictions $\left\langle i, a_i, \left[t_i, t_i^u\right)\right\rangle$ and $\left\langle j, a_j, \left[t_j, t_j^u\right)\right\rangle$, imposed on agents i and j accordingly.

At the same time, any solution from the set $\Pi_{opt}(p)$ satisfies at least one of the restrictions imposed to eliminate this conflict. This statement is a direct consequence of the consistency of the constraints imposed (Lemma 1). Since any optimal solution satisfies at least one of the constraints, its cost cannot be lower than the minimum cost among the available alternative partial solutions

$$\forall \Pi \in \Pi_{opt}(p): cost(\Pi) \geq \min\left(cost\left(N_1.\Pi\right), cost\left(N_2.\Pi\right)\right).$$

It is assumed that these statements are fulfilled in the step k the main cycle of the algorithm. Let's show that they are also performed at the step $k + 1$.

In step $k + 1$, the vertex will be removed from the OPEN list N, which contains the solution of the lowest value of all that is in *OPEN*. Let in the decision $N.\Pi$ conflict found *InConflict*$((a_l, t_l), (a_m, t_m))$. To eliminate it, two new vertices of the constraint tree will be created N_l, N_m, which contain one additional restriction each $\left\langle l, a_l, \left[t_l, t_l^u\right)\right\rangle$ and $\left\langle m, a_m, \left[t_m, t_m^u\right)\right\rangle$.

If in the plural $\Pi_{opt}(p)$ there are solutions that satisfy sets of constraints *N.cons*, then they will satisfy at least one of the restrictions added N_l*.cons*, N_m*.cons*. Therefore, their cost cannot be less than the minimum cost among the new created partial solutions

$$\forall \Pi \in \Pi_{Nopt}(p): cost(\Pi) \geq \min\left(cost(N_l.\Pi), cost(N_m.\Pi)\right),$$

where $\Pi_{Nopt}(p)$ – a subset of all optimal solutions satisfying constraints *N.cons*. Since the cost of all optimal solutions is equivalent, this inequality holds for any optimal solution

$$\forall \Pi \in \Pi_{opt}(p): cost(\Pi) \geq \min\left(cost(N_l.\Pi), cost(N_m.\Pi)\right).$$

Peaks N_l and N_m are added to the OPEN list, so

$$\forall \Pi \in \Pi_{opt}(p): cost(\Pi) \geq \arg\min_{N' \in OPEN}\left\{cost(N'.\Pi)\right\},$$

where $\arg\min_{N' \in OPEN}\left\{cost(N'.\Pi)\right\}$ – the minimum value peak from the OPEN list.

If a set of trajectories $N.\Pi$ does not contain conflicts, then the desired solution has been found. Given inequality

$$\forall \Pi \in \Pi_{opt}(p): cost(\Pi) \geq \arg\min_{N' \in OPEN}\left\{cost(N'.\Pi)\right\},$$

where $\arg\min_{N' \in OPEN}\left\{cost(N'.\Pi)\right\}$ – this is the top *N*, and also determining the set of all optimal solutions Π_{opt}, decision $N.\Pi$ has the same value as any solution with $\Pi_{opt}: cost(N.\Pi) = cost(\Pi), \forall \Pi \in \Pi_{opt}(p)$, i.e. $N.\Pi \in \Pi_{opt}(p)$.

It is worth noting that the statements on which the proof of Theorem 1 is built, in particular, the fulfillment of the inequality

$$\forall \Pi \in \Pi_{opt}(p): cost(\Pi) \geq \min\left(cost(N_1.\Pi), cost(N_2.\Pi)\right),$$

they are valid only if the algorithm for planning individual trajectories of agents guarantees the stay of the solution of the minimum possible value.

5. 2. 2. Evaluation of the effectiveness of the proposed methodology during a computational experiment

The effectiveness of the method of intelligent assessment and management of the security state of complex technical systems is compared using the – functions, the form of which is given in the Tables 1, 2.

Table 2 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 security of complex technical systems.

From the analysis of Tables 1, 2, 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 1, 2, increasing the security of complex technical systems is achieved by increasing the efficiency of decision-making at the level of 15–17% due to the use of additional procedures and ensuring the reliability of decisions made at the level of 0.91.

Table 1

Effectiveness evaluation of the proposed method of intellectual assessment and management of the security state of complex technical systems according to the criterion of prompt decision-making

Function name	Metrics	Canonical algorithm of a swarm of particles	Ant colony algorithm	Black widow algorithm	Gray wolf pack algorithm	Cheetah pack algorithm	Proposed methodology
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	1.62168E-07
B22-2	Average value	400	400.265772	400.7973158	400.265772	400.3986579	398.5315429
	Standard value	4.9898E-08	1.011427534	1.621892282	1.011427535	1.216419212	1.358342398
B22-3	Average value	600.0071815	600.0644622	600.0240021	600.012832	600.031303	598.0449987
	Standard value	0.021632777	0.184980091	0.115606243	0.053463097	0.147011513	0.100164243
B22-4	Average value	826.5653461	827.3281442	823.8789639	826.3000191	826.2668486	823.7693662
	Standard value	9.13817552	8.364210734	11.30806963	8.186625055	9.136107323	9.05921317
B22-5	Average value	900.743876	900.9504411	900.9726169	900.8007883	900.5452042	898.2016312
	Standard value	0.781626306	1.424558753	1.275779755	0.903385622	0.635781924	1.558982565
B22-6	Average value	1888.524629	1874.869967	1876.294359	1847.184924	1888.926953	1835.878175
	Standard value	127.2561383	91.22185049	69.00003268	32.76980351	140.693674	29.32108747
H22-7	Average value	2027.479588	2030.758499	2029.556604	2032.238674	2028.177978	2021.128603
	Standard value	6.106897592	8.027195324	5.81348717	7.446489204	8.003968446	7.197733191
H22-8	Average value	2223.108804	2223.537417	2222.070633	2223.140251	2220.888475	2216.690533
	Standard value	4.749655105	2.963408213	4.895282849	3.995669404	5.451654006	5.337353983
H22-9	Average value	2510.930321	2510.930321	2536.358938	2498.216012	2523.644629	2494.216012
	Standard value	65.93880108	65.93880108	85.778947	48.38585173	77.58997694	44.38585173
C22-10	Average value	2594.615905	2596.833927	2585.256107	2591.210109	2605.304194	2613.308989
	Standard value	48.2013289	49.71807546	57.1034079	56.36586785	42.57395199	32.10382553
C22-11	Average value	2695.981932	2685.587394	2733.855734	2710.621315	2700.168413	2712.332781
	Standard value	116.3652035	110.1475838	146.333679	118.5098748	113.7913849	107.3008673
C22-12	Average value	2857.067086	2858.742176	2854.959949	2861.414681	2859.407788	2855.718769
	Standard value	9.364347909	14.88960231	5.539104327	17.96133754	15.00545163	15.34731781

Table 2

Evaluation of the effectiveness of the proposed methodology according to the criterion of reliability of decision-making

Function name	Metrics	Canonical algorithm of a swarm of particles	Ant colony algorithm	Black widow algorithm	Gray wolf pack algorithm	Cheetah pack algorithm	Proposed methodology
U22-1	Average value	0.66	0.73	0.67	0.68	0.8	0.91
	Standard value	0.7	0.73	0.68	0.69	0.83	0.91
B22-2	Average value	0.7	0.73	0.7	0.71	0.77	0.91
	Standard value	0.71	0.73	0.72	0.72	0.76	0.91
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	0.91
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	0.91
	Standard value	0.61	0.72	0.64	0.74	0.88	0.92
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	0.92
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	0.9
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	0.91
H22-9	Average value	0.64	0.75	0.66	0.69	0.83	0.91
	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	0.91
C22-11	Average value	0.67	0.71	0.69	0.71	0.82	0.91
	Standard value	0.67	0.72	0.68	0.74	0.91	0.91
C22-12	Average value	0.63	0.73	0.65	0.75	0.82	0.91
	Standard value	0.62	0.74	0.66	0.76	0.83	0.91

6. Discussion of the results of the development of the methodology of intellectual assessment and management of the security state of complex technical systems

The advantages of the proposed method of intellectual assessment and management of the security state of complex technical systems are as follows:

– comprehensively assess the security state of complex technical systems due to multi-level assessment using the theory of artificial intelligence (Actions 2, 3, 5), compared to works [2, 5];

– reduce errors in assessing the security state of a complex technical system due to the human factor during the verification of the parameters of a complex technical system (Action 2), compared to works [4, 7];

– conduct modeling of possible security states due to the use of a polymodel complex of functioning of complex technical systems (Action 4), compared to works [6, 10];

– carry out the selection of the best individuals in bio-inspired algorithms, due to the use of an improved genetic algorithm (Action 6. 1), which achieves an increase in the efficiency and reliability of the obtained solutions and evaluations, in comparison with works [8, 15];

– make accurate decisions by individually adjusting the Actions of agents in each bio-inspired algorithm (Action 6), compared to works [7, 17];

– determine the type and duration of conflict in the operation of improved bio-inspired algorithms by using Action 6. 2. 2, which achieves a decrease in the number of computing operations in a complex technical system, compared to works [10, 17];

– eliminate conflicts between agents in advanced bio-inspired algorithms (Action 6. 2. 4), which increases the efficiency and reliability of the decisions made regarding the security state of complex technical systems, compared to works [12, 14];

– attract additional computing resources (if necessary) (Action 8), which achieves the prevention of looping of the methodology's work, compared to research [13, 16];

– carry out in-depth training of the knowledge bases of the agents of each bio-inspired algorithm (Action 7), due to the in-depth training method, which achieves an increase in the efficiency and reliability of assessments and control effects on the security state of complex technical systems, compared to research [12, 17].

The disadvantage of the proposed methodology should include greater computational complexity compared to approaches that use one bio-inspired algorithm at their core.

The proposed technique allows:

– conduct modeling of the process of assessing the security state of complex technical systems;

– identify effective measures to increase the security of complex technical systems;

– comprehensively assess the security state of complex technical systems, etc.

The limitations of the study are the need to take into account the delay time for collecting and proving information from sensors (sensors) of complex technical systems.

The proposed technique 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".

The direction of further research should be considered the creation of new approaches for assessing and managing the security state of complex technical systems.

7. Conclusions

1. The structure of the methodology of intellectual assessment and management of the security state of complex technical systems is proposed. The originality of the proposed structure of the methodology, which is the basis of the methodology of intellectual assessment and management of the security state of complex technical systems, consists in:

– comprehensive assessment of the security state of complex technical systems due to multi-level assessment using the theory of artificial intelligence;

– reduced error in assessing the security state of a complex technical system due to the human factor in the verification of the parameters of a complex technical system;

– modeling of possible security states due to the use of a polymodel complex of functioning of complex technical systems;

– selection of the best individuals in bio-inspired algorithms, due to the use of an improved genetic algorithm, which achieves an increase in the efficiency and reliability of the obtained decisions and evaluations;

– make accurate decisions by individually adjusting the actions of agents in each bio-inspired algorithm;

– eliminating the conflict between agents in improved bio-inspired algorithms, which increases the efficiency and reliability of decisions made regarding the security state of complex technical systems;

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

– implementation of deep learning of knowledge bases of agents of each bio-inspired algorithm, due to the method of deep learning, which achieves an increase in the efficiency and reliability of assessments and control effects on the security state of complex technical systems.

2. Modeling of the proposed methodology was carried out, during which it was established that increasing the security of complex technical systems is achieved by increasing the efficiency of decision-making at the level of 15–17% due to the use of additional procedures and ensuring the reliability of decisions made at the level of 0.91.

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 Miahkykh: Conceptualization; Methodology; Project administration; Writing – original draft; Writing – review & editing; **Oleg Sova**: Methodology; Writing; Writing – review & editing; **Olha Salnikova**: Writing – original draft; **Oleksandr Zhuk**: Writing – review & editing; **Iraida Stanovska**: Resources; Data Curation; **Yevheniia Arkhypova**: Validation; Data Curation; **Oleksii Nalapko**: Software; Validation; Data Curation; **Dmytro Balan**: Methodology; Formal analysis; Visualization; **Yuliia Vakulenko**: Software: Programming, software development; designing computer programs; implementation of the computer code and supporting algorithms; testing of existing code components; Validation; Data Curation; **Vitaliy Bereza**: 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. Promyslov, V. G., Semenkov, K. V., Shumov, A. S. (2019). A Clustering Method of Asset Cybersecurity Classification. IFAC-PapersOnLine, 52 (13), 928–933. https://doi.org/10.1016/j.ifacol.2019.11.313
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. Kosko, B. (1986). Fuzzy cognitive maps. International Journal of Man-Machine Studies, 24 (1), 65–75. https://doi.org/10.1016/s0020-7373(86)80040-2
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, 180. 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