The object of this research is artificial immune systems. The problem addressed in the study is improving the responsiveness of cyberattack detection in information systems while ensuring a predetermined level of convergence, regardless of the number of destabilizing factors. The subject of the research is the cyberattack detection process.

A cyberattack detection method for information systems based on artificial intelligence technologies is proposed. The originality of the method lies in the use of additional enhanced procedures that allow:

– initializing the initial population of swarm agents and verifying information system parameters using an improved bat algorithm, which minimizes the error of entering incorrect data concerning the operational information system of military forces;

– performing initial identification of attacks specific to the given information system using a decision tree;

– adapting to the type and duration of cyberattacks through multi-level adaptation of the artificial immune system;

– conducting initial selection of antibodies for each swarm of the artificial immune system using an improved genetic algorithm;

– training general-swarm antibodies using elite-swarm antibodies, thereby enabling deep learning;

– replacing unfit individuals for search through antibody population renewal;

– performing simultaneous solution search in multiple directions;

– calculating the required amount of computational resources in cases where available resources are insufficient for the necessary calculations.

An example application of the proposed method was conducted for cyberattack detection in an operational military force group. The results demonstrated an average increase in detection accuracy by 16%, an average improvement in responsiveness by 12%, and a high result convergence level of 95.23%

Keywords: cyberattacks, decision tree, genetic algorithm, destabilizing factors, military force grouping

UDC 004.81
DOI: 10.15587/1729-4061.2025.329258

DEVELOPMENT OF A METHOD FOR DETECTING CYBER ATTACKS ON INFORMATION SYSTEMS BASED ON ARTIFICIAL INTELLIGENCE TECHNOLOGIES

Salman Rasheed Owaid
PhD, Assosiate Professor, Lecturer of Department
Department of Computer Engineering
Al Taff University College
Karrada str., 3, Karbala, Iraq, 31001
Hennadii Miahkykh
Adjunct***
Elena Odarushchenko
PhD, Associate Professor
Department of Information Systems and Technologies
Poltava State Agrarian University
Skovorody str., 1/3, Poltava, Ukraine, 36003
Svitlana Kashkevich
Senior Lecturer*
Andrii Shyshatskyi
Corresponding author
Doctor of Technical Sciences, Senior Researcher, Professor*
E-mail: ierikon13@gmail.com
Ganna Plekhova
PhD, Associate Professor, Head of Department**
Andrii Hrymud
PhD, Listener***
Serhii Petruk
PhD, Senior Reserher, Deputy Chief of Research Department
Central Scientific Research Institute of Armament and Military Equipment
of the Armed Forces of Ukraine
Povitrianykh Syl ave., 28, Kyiv, Ukraine, 03049
Olena Shaposhnikova
PhD, Associate Professor**
Vitalii Stryhun
Senior Researcher, Senior Test Engineer
Research Laboratory
State Scientific Research Institute of Armament
and Military Equipment Testing and Certification
V. Chornovola str., 164, Cherkasy, Ukraine, 18003
*Department of Intelligent Cybernetic Systems
State University "Kyiv Aviation Institute"
Lubomyra Huzara ave., 1, Kyiv, Ukraine, 03058
**Department of Computer Science and Information Systems
Kharkiv National Automobile and Highway University
Yaroslava Mudroho str., 25, Kharkiv, Ukraine, 61002
***Institute of Information and Communication Technologies and Cyber Defense
National Defense University of Ukraine
Povitrianykh Syl ave., 28, Kyiv, Ukraine, 03049

Received 05.02.2025
Received in revised form 07.04.2025
Accepted date 29.04.2025
Published date 25.06.2025

How to Cite: *Owaid, S. R., Miahkykh, H., Odarushchenko, E., Kashkevich, S., Shyshatskyi, A., Plekhova, G., Hrymud, A., Petruk, S., Shaposhnikova, O., Stryhun, V. (2025). Development of a method for detecting cyber attacks on information systems based on artificial intelligence technologies. Eastern-European Journal of Enterprise Technologies, 3 (9 (135)), 33–39. https://doi.org/10.15587/1729-4061.2025.329258*

1. Introduction

In the development of information technologies, optimization problems – particularly those belonging to the NP-class – are becoming increasingly relevant. As computational complexity grows linearly over time (according to Moore's Law, which states that the number of transistors on a chip doubles approximately every two years), a wide range of opti-

mization tasks can be addressed through the development of new, efficient algorithms and methods [1, 2]. These tasks are typically characterized by non-linearity, multi-extremality, lack of analytical descriptions, complex topology of the feasible solution space, and high computational complexity of the objective functions [3, 4].

The primary approaches used to address such problems are heuristic methods. Although heuristic methods do not guarantee the identification of a global optimum, they enable the derivation of solutions with acceptable responsiveness. When comparing various heuristic approaches, it is concluded that artificial immune systems (AIS) offer a significant advantage over other bio-inspired algorithms and artificial neural networks due to their learning capabilities and memory retention.

The information system of a military operational grouping includes a large number of heterogeneous subsystems and diverse data flows. It is characterized by numerous short-term communication links that vary dynamically based on the operational situation. These connections are difficult to predict and include many possible entry points. Based on modern combat experience, numerous incidents of unauthorized device access – particularly those captured and repurposed by adversaries – have occurred with the intent of launching cyberattacks. These conditions underscore the urgent need for scientific approaches to ensure cybersecurity in rapidly evolving operational environments within the area of responsibility of military forces.

Given the limitations of existing metaheuristic algorithms, the authors of this study have selected artificial immune systems as the foundational mathematical apparatus for implementing cybersecurity measures in the information systems of military operational groupings.

Artificial immune systems are intelligent computational models and algorithms inspired by the functioning principles of the human immune system. They are characterized by self-organization, learning, memory, adaptability, robustness, and scalability [1–4]. By simulating the immunological processes of the human immune system, AIS have been developed as effective tools for conducting scientific research and solving engineering problems. These include optimization tasks [5], data mining from diverse sources [6], image recognition [7], and anomaly detection in computer networks, the Internet of Things (IoT), and industrial control systems [8].

Most AIS and their modifications are based on four core models or theories [1]: clonal selection, negative selection, danger theory, and the artificial immune network model. The artificial immune network model is based on the immune network theory, which posits that immune cells act as a mutually reinforcing network constructed through the matching of antibody paratopes and idiotopes. As a result, interactions occur not only between antibodies and antigens but also among the antibodies themselves, which may lead to mutual suppression.

Nevertheless, existing scientific approaches to the synthesis and functioning of artificial immune networks still suffer from limited accuracy and convergence. This is due to several factors:

– the significant role of human involvement during the initial configuration of AIS;

– the abundance of heterogeneous information sources that must be analyzed and processed during AIS operation;

– AIS operate under uncertainty, which results in processing delays and false positives, especially in the presence of insufficient input data;

– a large number of destabilizing factors that influence the functioning of AIS.

These challenges drive the need to introduce a variety of strategies to improve convergence speed and detection accuracy of AIS in cyberattack detection tasks. One promising direction involves the enhancement of AIS through the combination, comparison, and development of new usage procedures.

2. Literature review and problem statement

In [6], the authors proposed the use of Bayesian hierarchical networks to quantify cybersecurity risk levels in mission-critical information systems. However, this approach is limited by its reliance on a predefined statistical distribution and restricted model extensibility. These limitations impose constraints on the architecture of the information system and fail to account for qualitative factors that affect cybersecurity.

In [7], a security certification methodology was developed for information systems to enable stakeholders to automatically evaluate security decisions in large-scale deployments. This methodology supports transparency by providing a certification label as a key outcome. However, its limitations include the inability to update knowledge bases with new threats and challenges in generalizing and analyzing diverse network data types.

Study [8] introduces a model that integrates fault tree analysis (FTA), decision theory, and fuzzy logic to determine the root causes of cyberattack failures. This model was applied to assess cybersecurity risks in contexts such as e-commerce websites and enterprise resource planning (ERP). While the model is flexible, its main drawback lies in the accumulation of errors during the fuzzification and defuzzification processes.

In [9], a resource allocation model for automated command-and-control systems under operational uncertainty is proposed. The model incorporates cyberattack impacts and uses conflict, assistance, and indifference relations in multi-objective optimization. Although effective in capturing dynamic scenarios and building utility functions, the model cannot handle heterogeneous metrics of varying dimensions.

In [10], a hierarchical framework for governance-based control models is examined, emphasizing threats to critical cyber-physical systems integral to e-government functions. The system relies on symmetric and asymmetric cryptographic methods, making it unsuitable for cyberattack identification tasks.

In [11], a decision model is developed to help firms select optimal cybersecurity insurance policies, considering limited offerings from one or more insurers. The model systematically evaluates policies based on breach likelihood and associated premiums, fostering a more efficient insurance market. Nevertheless, it cannot adapt to emerging risks or operate in real-time due to rigid assumptions.

In [12], the importance of integrating vulnerability assessments into cybersecurity strategies is highlighted, especially within industrial process control systems. The approach supports critical application protection and resilience against cyber threats. However, it is designed for fixed architectures and lacks real-time adaptability.

Study [13] outlines a risk management process for identifying, assessing, responding to, and monitoring cybersecurity risks at each stage of the protection chain. While based on a continuous Markov chain model, it does not support the simultaneous use of both qualitative and quantitative indicators and lacks adaptability to evolving threats.

In [14], a theoretical-analytical approach is presented to evaluate delays in data transmission caused by cyberattacks, using a moving average method. However, this approach is limited to traffic control systems and cannot be applied to other domains.

In [15], cybersecurity of a system is represented as a graph of transient processes. While this allows the modeling of threat impacts, it supports only single-dimensional variables and does not accommodate the dynamic addition of new threats.

In [16], a game-theoretic approach is proposed for cybersecurity decision-making in advanced manufacturing systems. The method incorporates defense strategies, production losses, and recovery costs into the payoff matrix. Its major limitations include high computational complexity and the inability to process multi-dimensional metrics.

Summarizing the above, the general limitation of these approaches lies in their inability to process heterogeneous data in real time. To address this, various AI-based strategies have been proposed.

In [17], a data assessment method for decision support systems based on artificial intelligence is presented. It clusters and analyzes input data, then trains the system accordingly. However, the method suffers from error accumulation and lacks mechanisms to evaluate the adequacy of its decisions.

Study [18] proposes a data fusion approach from multiple sources using AI techniques. While it enables integration from diverse inputs, it produces low-accuracy results and lacks verification capabilities.

In [19], a comparative analysis of existing decision-support technologies is conducted, including the Analytic Hierarchy Process (AHP), artificial neural networks (ANN), fuzzy set theory, genetic algorithms, and neuro-fuzzy modeling. The study outlines their advantages, disadvantages, and application domains. It concludes that AHP performs well with complete input data but is heavily subjective. For forecasting under uncertainty, fuzzy logic and neural networks are more appropriate.

In [20], a hybrid metaheuristic approach is proposed by combining multiple optimization strategies. However, its drawback is low responsiveness when processing heterogeneous data.

Analysis of studies [9–20] revealed common limitations:

– lack of hierarchical indicator systems for cyberattack detection;

– disregard for available computational resources in detection systems;

– absence of mechanisms to adapt indicator sets in response to evolving threats;

– no deep learning capabilities for knowledge base refinement;

– high computational complexity;

– absence of prioritized search directions.

3. The aim and objectives of the study

The aim of this study is to develop a method for detecting cyberattacks on information systems using artificial intelligence technologies. This approach is expected to enhance the responsiveness of cyberattack detection through artificial immune systems, while maintaining a specified level of reliability and enabling the formulation of subsequent managerial decisions. The results will facilitate the development (or improvement) of software tools for cyberattack detection in information systems.

To achieve this aim, the following objectives were defined:

– to define the set of procedures required for implementing the proposed method;

– to demonstrate an example of applying the method for detecting cyberattacks within the information systems of military operational groupings.

4. Materials and methods

The object of this study is artificial immune systems. The research addresses the problem of improving the responsiveness of cyberattack detection in information systems while maintaining a specified level of convergence, regardless of the number of destabilizing factors. The subject of the study is the process of cyberattack detection, which is implemented using the following components:

– a decision tree classifier for the preliminary identification of cyberattacks, enabling faster configuration of the artificial immune system;

– an enhanced genetic algorithm for the initial selection of antibodies prior to swarm sorting, thereby increasing the reliability and convergence of the generated decisions;

– an improved bat algorithm for preliminary verification of information system parameters, which enhances the accuracy of the artificial immune system's performance;

– an artificial immune system for secondary identification of cyberattacks and the formulation of appropriate countermeasures.

The hypothesis of the study is that it is possible to improve the responsiveness of decision-making in the detection of cyberattacks in information systems while maintaining the required level of identification reliability through the use of an enhanced artificial immune system.

The proposed method was modeled in the Microsoft Visual Studio 2022 (USA) software environment. The modeling task involved detecting cyberattacks in an information system used by a military operational group. The hardware used for the research simulations was based on an AMD Ryzen 5 processor. The type of cyberattack modeled was a distributed denial of service (DDoS) attack.

The following metrics were employed for evaluation:

– IP address distribution metric;

– network resource load metric;

– traffic distribution metric.

To conduct the simulation, traffic streams and request processing by the operational group were emulated using a queuing network model.

Parameters of the enhanced algorithm:

– number of iterations: 50;

– number of swarm individuals: 25;

– feature space range: [–150, 150].

5. Development of a method for detecting cyberattacks on information systems based on artificial intelligence technologies

5. 1. Sequence of procedures for detecting cyberattacks on information systems using artificial intelligence technologies

The proposed method for detecting cyberattacks on information systems using artificial intelligence technologies consists of the following sequence of actions:

Step 1. Input of initial data.

At this stage, initial data about the information system of the operational military group are provided, specifically:

– the number and types of devices that comprise the system;

– the types of data circulating within the information system;

– available computational resources;

– the quantity and type of connections between each element of the system;

– technical characteristics of control and data transmission channels;

– information about the operating environment, etc.

Step 2. Verification of information system parameters.

At this stage, a bio-inspired algorithm is used to verify the parameters of the information system. If deviations from the initially entered data are detected, the input data are adjusted using the output of the bio-inspired algorithm.

Step 3. Identification of destabilizing factors affecting the information system.

This step involves the initial identification of cyberattacks specific to the information system of the operational military group

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

where $\mu=\{0,...,m\}$ – initial set of cyberattack class labels; $L_{\mu}\subsetneq\mu$ – an arbitrarily generated or defined subset; $\mu\left(\#L_{\mu}<\#\mu\right)$, $R_{\mu}=\mu\backslash L_{\mu}$ – left branch of the classification tree, $CBT_{R_{\mu}}$ – right classification subtree, $F^{(i)}_{jL_{\mu}R_{\mu}}$ – node detector trained on the elements of the set $\left\{\left(x_l,0\right)\middle|\overline{c}_l\in L_{\mu}\right\}_{l=1}^{M}\cup\left\{x_l,1\middle|\overline{c}_l\in R_{\mu}\right\}_{l=1}^{M}$.

Step 4. Initialization of the artificial immune system.

At the initialization stage, a population of N candidate antibodies is randomly created: $Ab(t)=\{Ab_1(t), Ab_2(t), ..., Ab_N(t)\}$, where Ab_i is i-th agent (antibody) at iteration t. The affinity of these antibodies is evaluated using the function $Aff()$. At each iteration, each antibody is cloned to generate offspring, after which all clones – except the parent – undergo mutation. Only the clone with the highest affinity is retained.

To improve the accuracy of solving computational problems and the speed of convergence, this study proposes an artificial immune system with deep learning mechanisms for detecting cyberattacks in the information system of a military operational group.

Step 5. Preliminary selection of antibodies.

At this stage, an initial selection of antibodies for each swarm is performed using the enhanced genetic algorithm proposed in [20].

Step 6. Distribution of artificial immune system agents between swarms.

At the swarm update stage, antibodies that are candidate solutions are redistributed between the elite swarm and the general swarm in a 1:5 ratio. Antibodies in the elite swarm undergo an affinity-dependent cloning operator and a self-learning mutation operator, where the search radius is adaptively updated using a specially designed mechanism.

Step 7. Cloning of antibodies.

In this study, the number of clones created from a single parent antibody is determined by its affinity. The higher the affinity of the parent antibody, the more offspring it produces.

Moreover, the number of clones is a nonlinear function of the parent antibody's affinity. The procedure for computing the cloning process of antibodies is outlined below:

$$Aff_{\max}=\max\{Aff(Ab_i(t)), i=1, 2,..., N\}, \quad (2)$$

$$Aff_{\min}=\min\{Aff(Ab_i(t)), i=1, 2,..., N\}, \quad (3)$$

$$Aff^{*}(i)=(Aff(Ab_i(t))-Aff_{\min})/(Aff_{\max}-Aff_{\min}), \quad (4)$$

$$Nc_i(t)=\text{round}((N_{c\max}-N_{c\min})\,Aff(A_{bi}(t))\,n+N_{c\min}), \quad (5)$$

where $N_{c\max}$ and $N_{c\min}$ – the maximum and minimum number of antibody offspring; n – the power coefficient of the control function. All antibodies, including those in both the general and elite swarms, perform this cloning operation once during each iteration.

Step 8. Mutation of antibodies.

Antibodies in the elite swarm have higher affinity and serve as memory cells that respond more aggressively and rapidly during the secondary immune response. Therefore, these elite antibodies play a key role in local search and undergo self-learning mutation. On the other hand, antibodies in the general swarm perform a global search, guided by the elite swarm antibodies. Thus, all general swarm antibodies undergo deep learning to accelerate convergence.

If $Aff(Ab_i(t))<Aff(Ab_i(t))$, then the affinity of a general swarm antibody is lower than that of an antibody selected from the elite swarm. In this case, the general antibody learns from the selected elite antibody. This scenario is described by the following mathematical expression

$$\Delta A_{bi}(t)=\text{rand}^{*}(A_{bj}(t)-A_{bi}(t)). \quad (6)$$

If $Aff(Ab_i(t))<Aff(Ab_e(t))$ the affinity of a general swarm antibody exceeds that of a selected elite swarm antibody but remains lower than the affinity of the best elite antibody. In this case, learning is described as

$$\Delta Ab_i(t)=\text{rand}^{*}(Ab_e(t)-Ab_i(t)). \quad (7)$$

In all other cases, the general swarm antibody performs a deep mutation

$$\Delta Ab_i(t)=\text{rand}n^{*}\lambda_i(t), \quad (8)$$

where rand – a uniformly distributed random variable, rand$n$ – a normally distributed random variable with a mean of 0 and standard deviation of 1, $Ab_e(t)$ – the best elite antibody in terms of affinity, $\lambda_i(t)$ – the search radius of antibody $Ab_i(t)$ on t-th iteration.

In this artificial immune system, a fixed search radius negatively affects both convergence speed and solution accuracy. This is because: if an elite antibody is close to the optimum but its search radius is too large, it may overshoot the optimal point. Conversely, if the search radius is too small, the convergence speed of the system significantly slows down.

Therefore, the search radius $\lambda_i(t)$ should be dynamically updated using the following rule

$$\lambda_i\left(t\right)=\begin{cases}\lambda_i\left(t-1\right), \text{if } Aff\left(Ab_i\left(t\right)>Ab_i\left(t-1\right)\right),\\ \dfrac{\lambda_i\left(t-1\right)}{2}, \text{else } \dfrac{\lambda_i\left(t-1\right)}{2}\geq\lambda_{\min},\\ \lambda_0\left(k\right), \text{otherwise},\end{cases} \quad (9)$$

where λ_{min} – the lower bound of the search radius and is determined by

$$\lambda_0(k)=\begin{cases}\frac{\lambda_0(k-1)}{2}, \text{ if } \frac{\lambda_0(k-1)}{2}\geq\lambda_{min},\\ \lambda_0(0), \text{otherwise.}\end{cases} \quad (10)$$

For each antibody $Ab_i(t)$, in accordance with equations (9) and (10), the initial search radius is defined as λ_0, with its value being half of the threshold value $Th_s(t)$

$$\lambda_0(k)=Th_s/2. \quad (11)$$

Since after executing the suppression operator, the distance between any two antibodies exceeds $Th_s(t)$, the value $\lambda_0=Th_s(t)/2$ ensures maximum coverage of the search space without overlap.

If the affinity of antibody $Ab_i(t)$ improves after mutation, its search radius $\lambda_i(t)$ is retained. Otherwise, $\lambda_i(t)$ is reduced by half:

$$Aff(Ab_i(t))>Aff(Ab_i(t-1)), \quad (12)$$

$$\lambda_i(t)=\lambda_i(t-1). \quad (13)$$

However, the search radius cannot fall below $\lambda_{min}(t)$, as a radius that is too small can significantly slow down the convergence speed. Therefore, if $\lambda_i(t)$ becomes smaller than $\lambda_{min}(t)$, its value is set to $\lambda_0(k)$, which is reduced to half the previous value $\lambda_0(k-1)$. At the same time $\lambda_0(k)$ must not fall below $\lambda_{min}(t)$, if it does, its value is reset to $\lambda_0(k)$.

Step 9. Deep learning of the artificial immune system.

The learning mechanism of the artificial immune system is described as follows

$$p(Ab_j(t))=\frac{Aff^*(Ab_j(t))}{\sum_{i=1}^{N_{elite}} Aff^*(Ab_i(t))}. \quad (14)$$

It is evident that the probability of selection is non-uniform: the higher the affinity of an antibody, the greater its probability of being selected. Therefore, the roulette wheel selection method is used to choose an elite-cluster antibody for training.

Let's suppose the optimal values of a multimodal function vary significantly in affinity. In that case, antibodies with higher affinity are more likely to evolve toward the global optimum, and thus this learning algorithm will demonstrate faster convergence.

Step 10. Antibody suppression the proposed artificial immune system applies a dynamic suppression mechanism, which is described by the following mathematical expressions:

$$D_{max}=\max\{D_{i,j}(t)|i,j=1,2,\ldots,N, i\neq j\}, \quad (15)$$

$$D_{min}=\min\{D_{i,j}(t)|i,j=1,2,\ldots,N, i\neq j\}, \quad (16)$$

$$Th_s(t)=D_{min}+\xi(D_{max}-D_{min}), \quad (17)$$

where $Th_s(t)$ – the threshold value proportional to the similarity of the antibody population, $D_{i,j}$ – the Euclidean distance between the i-th and j-th antibodies at t-th iteration, $\xi\in(0, 1)$ – the control parameter. After applying the suppression operator, a certain number of randomly generated antibodies are added to the population to maintain its size at N.

Step 11. Swarm update.

As is known, some antibodies from the general swarm may achieve higher affinity than those in the elite swarm due to the elitist learning mechanism. Therefore, it is necessary to update the swarm composition by allowing better-performing antibodies from the general swarm to move into the elite swarm.

During swarm updating, all antibodies are sorted by affinity in descending order. The top N_{elite} antibodies become part of the elite swarm, while the remaining ones stay in the general swarm.

It is important to note that after the initial initialization, all antibodies undergo deep learning until the suppression operator is activated. This allows each antibody to evolve within a relatively small region around its position, promoting the search for local optima.

Step 12. Determination of required computational resources of the intelligent decision support system.

To prevent computational looping across Steps 1–11 and to improve computational efficiency, the system load is additionally assessed. If a predefined computational complexity threshold is exceeded, the required number of additional software-hardware resources is determined using the method proposed in [20].

End of the algorithm.

This set of structurally and logically interconnected procedures constitutes the method for detecting DDoS attacks on information systems.

5. 2. Example of applying the proposed method for cyberattack detection in an information system

To evaluate the effectiveness of the proposed method, a simulation was conducted to solve the task of cyber threat detection under the initial conditions specified in Section 4.

The effectiveness of detecting cyber threats using artificial intelligence technologies in the information systems of an operational military unit is compared with the results of studies previously analyzed (Table 1).

The indicators presented in Table 1 were determined empirically, taking into account the experience of using special-purpose information systems during the response to the full-scale military aggression in Ukraine.

Table 1

Evaluation of the effectiveness of the proposed cyberattack detection method

Algorithm reference	Accuracy	Convergence	Responsiveness (sec)	Percentage of system resources used
[6]	77.92 %	80.23 %	5.23E+04	100
[7]	75.71 %	77.4 %	5.72E+04	100
[8]	77.01 %	76.66 %	6.40E+02	100
[9]	76.17 %	81.15 %	5.36E+01	100
[10]	80.31 %	80.67 %	7.07E+02	100
[11]	70.05 %	81.03 %	6.16E+03	100
[12]	70.28 %	75.18 %	5.29E+03	100
[13]	75.24 %	73.12 %	7.04E+02	100
[14]	77.41 %	74.2 %	7.55E+07	100
[15]	75.16 %	74.28 %	5.42E+05	100
[16]	81.44 %	85.9 %	5.56E+04	100
Proposed method	97.3 %	95.23 %	5.13E+04	80

Based on the analysis of Table 1, it can be concluded that the proposed method increases detection accuracy by an aver-

age of 16 % and improves response time by an average of 12%, while maintaining a high convergence rate of 95.23%.

6. Discussion of the cyberattack detection method performance

The advantages of the proposed method are due to the following key aspects:

– verification of information system parameters (Step 2) is performed using the enhanced bat algorithm, which distinguishes this approach from the methods discussed in [6–10]. This allows for minimizing errors in input data related to the status of the operational military information system;

– initial identification of attacks specific to the system is carried out using a decision tree (Step 3), which enhances early-stage detection compared to the methods in [7–11];

– the adaptive capability to the type and duration of the cyberattack is achieved through multi-level adaptation of the artificial immune system (Steps 1–12), in contrast to the approaches in [7–12];

– preliminary antibody selection for each swarm within the artificial immune system is performed using an improved genetic algorithm (Step 5), offering improvements over methods in [11, 13, 15];

– the ability to train general swarm antibodies using elite swarm antibodies enables deep learning (Step 9), which enhances decision-making compared to [9–12];

– the method supports replacement of ineffective search agents by updating the antibody population (Step 11), outperforming techniques from [9, 12, 13, 16];

– the method supports simultaneous solution searches in multiple directions (Steps 1–12, Table 1);

– it also enables the calculation of the required amount of computational resources to be involved in cases where calculations cannot be performed using the currently available computing power (Step 12), which is an improvement over the approaches in [9, 13].

Limitations of the study.

One of the key limitations is the need to account for delays in the collection and transmission of information from the components of organizational and technical systems.

Shortcomings of the proposed method.

The proposed method has the following shortcomings:

– lower accuracy in evaluating individual parameters of cyberattacks;

– loss of decision reliability when searching for solutions in several directions simultaneously;

– lower detection accuracy compared to some other cyberattack detection methods.

However, the proposed method enables:

– identification of the optimal cyberattack detection metric based on the specific information system in use;

– definition of effective measures to enhance cyberattack counteraction within information systems;

– increased processing speed of heterogeneous data while ensuring a given level of decision-making reliability;

– reduced use of computational resources in decision support systems.

The proposed approach is well-suited for protecting information systems that are characterized by a high level of complexity from cyberattacks.

7. Conclusions

1. An algorithm for implementing the method has been defined, which, through additional and enhanced procedures, enables the following:

– verification of information system parameters using an improved bat swarm algorithm, minimizing input errors in the system status data of the operational military group;

– initial identification of attacks specific to the given information system using a classification tree;

– adaptation to the type and duration of a cyberattack through a multi-level adjustment of the artificial immune system;

– preliminary selection of antibodies for each swarm in the artificial immune system using an improved genetic algorithm;

– training of general swarm antibodies by elite swarm antibodies, enabling deep learning capabilities;

– replacement of ineffective antibodies through population updates;

– simultaneous solution searching in multiple directions;

– estimation of the required computing resources in case current resources are insufficient for calculations.

2. A practical example of the proposed method was demonstrated in the detection of cyberattacks on an operational military group information system. The method showed an average accuracy improvement of 16%, response time improvement of 12%, and maintained a high convergence rate of 95.23%.

Conflict of interest

The authors declare that they have no conflict of interest related to this research, including financial, personal, authorship, or any other nature that could have influenced the study and its outcomes presented in this article.

Financing

This research was conducted without financial support.

Data availability

The manuscript has associated data available in a data repository.

Use of artificial intelligence tools

The authors confirm that AI technologies were not used in the preparation of this manuscript.

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. Maccarone, A. D., Brzorad, J. N., Stone, H. M. (2008). Characteristics And Energetics Of Great Egret And Snowy Egret Foraging Flights. Waterbirds, 31 (4), 541–549. https://doi.org/10.1675/1524-4695-31.4.541
20. Litvinenko, O., Kashkevich, S., Shyshatskyi, A., Dmytriieva, O., Neronov, S., Plekhova, G. et al.; 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