

# Model of an intelligent decision support system to ensure cyber resilience of military information systems<sup>\*</sup>

Olena Nehodenko<sup>1,†</sup>, Svitlana Shevchenko<sup>1,\*,†</sup>, Vitalii Nehodenko<sup>1,†</sup>, and Yuliia Zhdanova<sup>1,†</sup>

<sup>1</sup> Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudriavska str., 04053 Kyiv, Ukraine

## Abstract

The article presents a comprehensive model of an intelligent decision support system to ensure cyber resilience of military information systems in dynamic conditions of cyber threats. An analysis of scientific sources on methods and models for increasing the efficiency of detecting and predicting cyber threats in information systems, as well as possible methods for ensuring the cyber resilience of these systems, was conducted. The advantages and disadvantages of existing solutions were identified, and a comparative analysis of three main approaches was conducted, which include classical decision support systems (DSS), intelligent decision support systems (AI+DSS) and autonomous agent systems for ensuring cyber resilience (MAS, Autonomous Cyber Defense Agents). The proposed architecture is based on the mathematical catastrophe theory to describe the nonlinear dynamics of system stability and predict critical transitions in the data flows of the SIEM module, the cluster analysis method, namely the k-Means algorithm for classifying the operating modes of security states from stable to critical, which allows identifying anomalies that can cause catastrophic changes in the system. Statistical and temporal methods are used to predict bifurcation points as indicators of instability in the SIEM module. A multi-objective optimization method is also used, which reflects the DSS component of the system and is responsible for making decisions based on indicators of minimizing risks, time and costs. The system architecture is presented using an activity diagram, a state diagram and a sequence diagram.

## Keywords

Intelligent Information Security Management System (ISIM), Incident Detection System (IDS), SIEM-system, bifurcation points, system stability, Catastrophe Theory, k-means

## 1. Introduction

The protection of military systems is becoming increasingly relevant during a real war, which changes its rules of the game in the arena of information and communication systems security and requires new technical solutions to increase this security. In modern cyberspace, there are a large number of various cyberattacks that negatively affect military information and communication systems and disrupt their ability to adapt and recover from each attack as a whole [1]. But what is significant in this context is the ability of the system to proceed to operate continuously due to the reliability of communication channels and stable information flows [2].

All modern military operations depend on modern cyber defense developments that can counteract real threats and guarantee the resilience of information and communication systems to intense cyberattacks [3]. The use of an information security management system allows you to maintain data confidentiality, ensures continuity of operations and supports overall operational efficiency at all stages of military operations. Information security management systems are also a control unit for detecting, preventing and blocking all possible threats and failures during the planning and implementation of combat missions [4].

In [4], a mathematical catastrophe theory is proposed to ensure the stability of the information security management system. It is found that different types of cyber incidents have their own impact on the stability and equilibrium of the system as a whole. The presence of risk zones on the

<sup>\*</sup> CPITS-II 2025: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2025, Kyiv, Ukraine

<sup>\*</sup> Corresponding author.

<sup>†</sup> These authors contributed equally.

✉ o.nehodenko@kubg.edu.ua (O. Nehodenko); s.shevchenko@kubg.edu.ua (S. Shevchenko); v.nehodenko.asp@kubg.edu.ua (V. Nehodenko); y.zhdanova@kubg.edu.ua (Y. Zhdanova)

ORCID 0000-0001-6645-1566 (O. Nehodenko); 0000-0002-9736-8623 (S. Shevchenko); 0000-0002-7678-9138 (V. Nehodenko); 0000-0002-9277-4972 (Y. Zhdanova)



© 2025 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

plane of the system's equilibrium points, which are critically important during sharp changes in the system states under the influence of cyber incidents, is established [5]. These results allow us to apply the mathematical catastrophe theory to increase the stability of the information security management system, which allows us to predict destabilization processes in the system.

Also important are the results of article [6], which presents the advantages and disadvantages of using a SIEM system using mathematical catastrophe theory to predict, detect, and prevent cyber incidents in integrated military training systems.

An important block for the information security management system is the decision-making stage regarding the identified threats. In article [7], a cluster analysis method was proposed to reduce the subjectivity of expert assessments in the process of identifying cyber threats.

Unfortunately, traditional methods used in information security management systems do not always quickly and accurately make decisions in critical situations in real time, therefore, there is a pressing task of creating an intelligent decision support system (IDSS) to ensure the cyber resilience of military information systems. These intelligent systems are aimed at improving the quality and speed of forecasting, detecting and preventing dynamic and complex cyber threats using modern artificial intelligence technologies [8–10]. Artificial intelligence and machine learning technologies use automated analysis of large amounts of data and predict threats based on real-time anomaly detection [11, 12]. The integration of human-machine interaction should also not be rejected, since military information and communication system operators should participate in making critical decisions, which will reduce the risk of errors that arise during the automated operation of IDSS [13, 14].

## 2. Literature review

A review of modern scientific sources has shown a growing interest in the use of artificial intelligence in information security management systems, which allows analyzing large amounts of data, identifying vulnerabilities, and predicting possible cyber threats [15]. In [8], much attention is paid to deep learning models to increase the reliability of systems and the efficiency of processing multi-level data from various sources. However, the main requirement is systematic training based on the received data in real time, which contributes to the constant improvement of the quality of decision support and response to new cyber threats. In [16], semantic technologies and big data technologies in cyber security are investigated, which allow to increase the security indicators of information systems. Also, one should not forget about the combination of cloud technologies and the operability of peripheral systems, which allows the creation of hybrid architectures that ensure the transition to the creation of scalable, reliable and intelligent systems that are important for performing complex operations [11].

For rapid response to cyberattacks, risk assessment and creation of countermeasures in real time, [17] proposed to combine an ontological knowledge model, cognitive architecture and data analysis. An important component of an intelligent information security management system is a decision-making system, which often does not perceive the coordinated action of several cyber agents which use different ways of penetrating the system. In order for this system to respond to complex attacks in real time, [18] proposed to base the system on hierarchical modeling and Bayesian analysis for dynamically updating models and generating recommendations to ensure efficiency and resilience in real cyberthreat scenarios.

Researchers at the Netherlands Aerospace Center [19] propose a combined approach that combines the integration of artificial intelligence and modeling with simulation (M&S) to create an intelligent decision support system for military systems. This combination allows to increase the accuracy of predictions and the quality of decisions due to the previous results of actions, which are important for commanders during the planning of operations. This method also allows to reduce the cognitive load on military analysts and rapid response to changes in combat situations by creating new scenarios in real time.

The approaches to build intelligent decision-making systems to ensure cyber resilience of military information systems, which are proposed in the works [8, 15–19], of course, have advantages, but in turn also have a number of negative indicators, such as excessive complexity of modeling cognitive processes and scaling in real time, complexity of agent interaction and risks of incorrect autonomous response without taking into account a single context, high dependence on data quality, as well as high complexity of calculations when expanding the functioning of the system, as well as limited realism of simulation in combination with high resource costs and dependence on the accuracy of the models used. All of these approaches (cognitive, Bayesian, stimulation, multi-agent) provide analysis and response to cyberattacks, but do not take into account the dynamic processes that lead to the loss of system stability. This article proposes the use of catastrophe theory and cluster analysis as an analytical center for DSS, which will ensure the transition from reactive to preventive management of cyber resilience of military information systems.

It is advisable to provide a comparative table of the use of different approaches for building an intelligent decision-making system to ensure the cyber resilience of military information systems (Table 1).

**Table 1**  
Comparison of IDSS Approaches for Military Cybersecurity

Approach	Advantages	Disadvantages
Classic decision support systems (DSS)	Structured data analysis; Lack of full automation; Ease of implementation; Suitable for planning, risk assessment, and logistics tasks.	Slow response to cyberattacks in dynamic systems; Low effectiveness in detecting complex anomalies and responding in real time; High demands on operators' skills and abilities.
Intelligent decision support systems (AI+DSS)	Ability to process large amounts of data; Real-time efficiency; Use of machine learning to predict attacks; High accuracy and quick decision-making; Ability to learn from new incidents; Formation of situational knowledge in command centers.	High requirements for quality data; Model updates; Dependence on adversarial attacks; AI black box; Automation bias.
Autonomous agency systems for ensuring cyber resilience (MAS, Autonomous Cyber Defense Agents)	Detection, analysis, and response to cyberattacks autonomously; Response and recovery; Independently predict cyber threats and recover from cyberattacks.	Require a high level of data control; Difficulty of certification in combat conditions; Difficulty in calculating and cyberprotecting agents; High probability of losing "human control" in critical conditions.

### 3. Research methods

The development of an intelligent decision support system model to ensure cyber resilience of military information systems includes the catastrophe theory method to describe the nonlinear

dynamics of system resilience and predict critical transitions in the SIEM module data streams, the cluster analysis method, namely the k-Means algorithm and DBSCAN to classify the operating modes of security states from stable to critical, which allows identifying anomalies that can cause catastrophic changes in the system. Statistical and temporal methods were used to predict bifurcation points as indicators of instability in the SIEM module. A multi-criteria optimization method was also used, which reflects the DSS component of the system and is responsible for decision-making based on indicators of minimizing risks, time and costs. Additionally, machine learning algorithms were used to detect anomalies and build adaptive models of the behavior of the entire system. The architecture and processes of the intelligent decision-making support system for ensuring cyber resilience of military information systems are presented using an activity diagram, a state diagram and a sequence diagram. The latter shows the logic of the analyst's interaction with the intelligent modules of the system.

#### 4. Main material

This article presents the development of an intelligent decision support system (IDSS) model to ensure cyber resilience of military information systems using classical and intelligent approaches to ensure rapid response and decision-making regarding detected cyberattacks. The proposed approach, which is based on the detection of dynamic changes in system states and differs from traditional ones that record events and reactions to already detected cyberincidents, is based on the principles of catastrophe theory. Catastrophe theory is appropriate to use to describe the behavior of complex systems at bifurcation points that occur when parameters change and lead to a sharp loss of stability. This approach involves not only detecting cyber incidents, but also allows predicting their consequences by analyzing state changes in the system [4, 6, 19]. To build a holistic analytical architecture, where all modules interact in real time, a phased approach was used, which consists of data collection and normalization, modeling, clustering, decision synthesis and, finally, quality control of decision-making, in the contour of which a person remains (Human in the loop).

To construct this model, the system is formally represented as a hybrid dynamic system with continuous and discrete blocks that model the state of stability, regime transitions, and decision-making.

The results of scientific research in [4, 6, 19] showed the feasibility of using nonlinear dynamics and mathematical catastrophe theory to build a model of an intelligent decision support system (IDSS) to ensure the cyber resilience of military information systems. This approach provides mathematical prediction of critical transitions under the influence of increasing cyberattacks, load or conflict of systems.

Nonlinear systems depend on initial conditions, as well as on the influence of external factors, which lead to sharp jumps or catastrophes in the stability of the system [20].

The state of nonlinear systems is given by the formula:

$$\frac{dx}{dt} = f(x; a, b) + \xi(t), \quad (1)$$

where  $x(t)$  is an integral variable that shows the state of the system (level of cyberstability);  $a$  and  $b$  are system parameters responsible for the intensity of events, the level of cyber incidents;  $\xi(t)$  shows noise or fluctuations in the data.

In [4], various types of catastrophes and the feasibility of using the “Butterfly” catastrophe type, which shows the transition from a stable to a variable state under the influence of five parameters, are proposed.

The general equation for the “Butterfly” catastrophe has the form

$$V(x) = x^6 + ax^4 + bx^3 + cx^2 + dx, \quad (2)$$

where  $x$  is a variable that determines the state of the system;  $a, b, c$ , and  $d$  are management parameters that correspond to cyber incident categories [4].

To determine the differential equation describing the change in the state of the system, the gradient descent method was used, which is used to find the minimum value of the function, namely, to reduce the potential and achieve a stable state of the system. The formula for the gradient descent step has the form:

$$V x_1 = x_2 - \eta \nabla f(x_2), \quad (3)$$

where  $x_1$  is the new variable value  $x$ ;  $\eta$  is the step variable;  $\nabla f(x_2)$  is the gradient of a function  $f(x)$  at the point  $x_2$ .

Points, where

$$\frac{dx}{dt} = 0, \quad (4)$$

correspond to equilibrium states and depend on the values of the parameters  $a, b, c$ , and  $d$ . In turn, when changing these parameters, the system can enter a state of “catastrophe,” that is, reach bifurcation points. This state is possible when modeling a situation when the number of cyber incidents jumps to critical values, which will lead to system failures.

The critical state of the system can also be indicated using the metric:

$$\Delta_t = \nabla^2 V(x_t; a_t, b_t, c_t, d_t) \rightarrow 0, \quad (5)$$

which shows that the system is losing its equilibrium, the stage of activation of the response subsystem begins.

Mathematical catastrophe theory provides an opportunity to identify complex interdependencies between various cyber incidents and timely detect catastrophic changes in the state of the system. In turn, the gradient descent method, namely the analysis of the potential

$$V(x_t; a_t, b_t, c_t, d_t) \quad (6)$$

allows to identify risk areas in time and prevent changes in the system state.

In real conditions, the process of changing states in military information systems is carried out discretely, therefore, to model these transitions, a clustering method based on features of system behavior was used.

To describe the behavioral profile of the system at a point in time  $t$ , a multidimensional vector is used, which describes all the features that implement the corresponding collected data of the SIEM system, event logs, and telemetry of military subsystems, and is given by the formula:

$$\phi(t) = [\lambda_t, \sigma_t^2, \rho_{1,t}, Sw_t, Kt_t, H_t, \delta_t, p_t, q_t], \quad (7)$$

where  $\lambda_t$  is the number of cyberattacks per unit of time;  $\sigma_t^2$  is the variance of events in a sliding window;  $\rho_{1,t}$  is the autocorrelation;  $Sw_t$  is the distribution asymmetry;  $Kt_t$  is the kurtosis of the distribution;  $H_t$  is the entropy of the state of the system;  $\delta_t$  is the distance to catastrophic state;  $p_t$  is the normalized risk;  $q_t$  is the trust level.

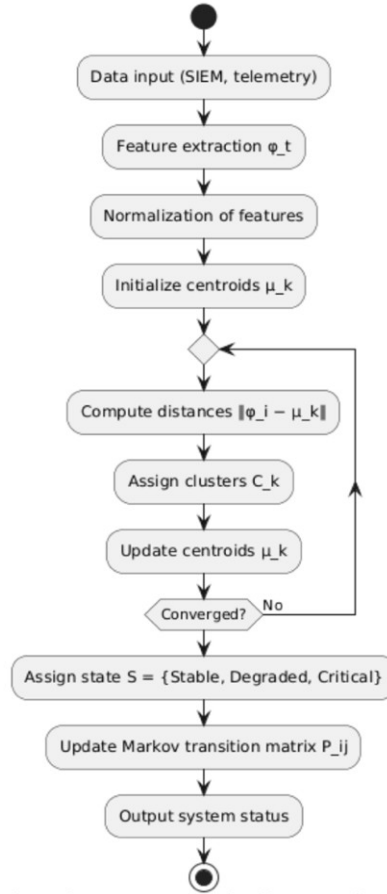
A set of vectors  $\{\phi_1, \phi_2, \dots, \phi_t\}$  forms a set that describes the dynamic behavior of the system at a certain point in time. Using the k-means method [7], the set of vectors is divided into classes with common properties, i.e. clusters

$$S=\{Stable, Degraded, Critical\}. \quad (8)$$

Next, the distances between elements of one cluster are minimized and the distances between elements of different clusters are maximized, that is, the functional of the mean square distances is minimized

$$D=\sum_{k=1}^K \sum_{\phi_i \in C_k} \|\phi_i - \mu_k\|^2, \quad (9)$$

where  $K$  is the number of clusters,  $C_k$  is the set of points in a cluster  $k$ ,  $\mu_k$  is the cluster center. Thus, all vectors of the set  $\{\phi_1, \phi_2, \dots, \phi_i\}$  will receive a cluster label after training the algorithm, which determines the state of the system  $s_t \in S$  with corresponding features, namely the Stable state includes low variance, low autocorrelation, and small entropy; state describes the average value of autocorrelation, increasing variability and increasing normalized risk; the Critical state describes high  $H_t$ ,  $\sigma_t^2$ ,  $p_t$  and decreasing trust  $q_t$ . Figure 1 presents an Activity Diagram that describes the state clustering process, namely how the system learns to determine the states of the system [21].



**Figure 1:** Activity Diagram of the state clustering process—method  $k$ -means (implemented in PlantUML environment)

It is also necessary to take into account that the system may be affected by new cyber incidents that affect the change in the state of the system. Let the system be in a state at some point in time  $s_t \in S$ , then the probability of the system transitioning to the state  $s_{t+1}$  is determined by the formula:



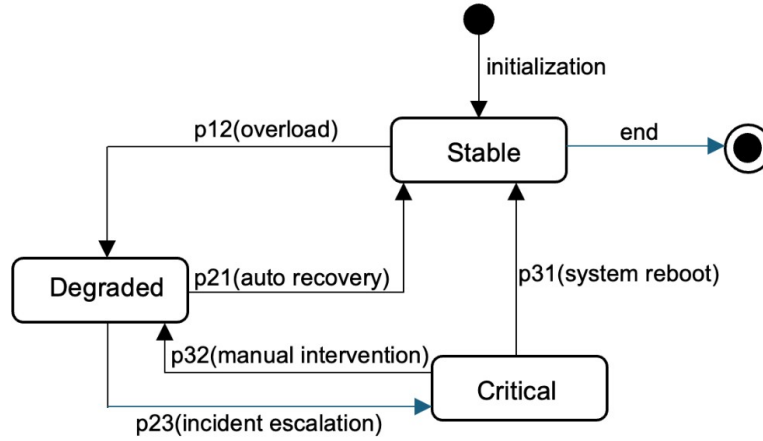
$$P(S_{t+1}=s_j \vee s_t=s_i)=p_{ij}, \sum_j p_{ij}=1, \quad (10)$$

Where the elements  $p_{ij}$  are estimated statistically taking into account historical data:

$$p_{ij}=\frac{N_{ij}}{\sum N_{ij}}, \quad (11)$$

where  $N_{ij}$  is the amount observations during state transitions  $s_i \rightarrow s_j$ .

Figure 2 shows a State Diagram that describes the states of the system depending on the elements  $p_{ij}$ , that determine the rapid response of the subsystem to detected cyberattacks.



**Figure 2:** State Diagram of transition models

The clustering performed using the  $k$ -means method divides all available SIEM system data into behavioral characteristics, each of which plays its own role in the information system. As noted earlier, each cluster has its own center  $\mu_k$ , which shows the state of the system and the distance  $\|\phi_t - \mu_k\|$ , which is a measure of the change in the state of the system [22].

There is a direct connection between clusters and the indicators used in the “Butterfly” type catastrophe. Thus, the Stable state can be obtained at a local minimum of the potential  $V(x)$ , i.e. at a point  $x_s$  at

$$\frac{dV(x)}{dx}=0, \frac{d^2V(x)}{dx^2}>0. \quad (12)$$

With these indicators, the system is in a stable state, where the parameters of the butterfly catastrophe  $a, b, c$ , and  $d$  are subject to minor fluctuations, which does not affect the loss of equilibrium of the system as a whole.

When the Degraded state is detected, the system is exposed to cyberattacks and its stability is compromised, but it still functions within its capabilities. In this region, the potential gradient is weak, which provokes the system to slow down to return to the equilibrium state after the cyberattack is detected. These changes are accompanied by changes in the parameters  $a, b, c$ , and  $d$  by the transition to a new minimum or the appearance of bifurcation points, i.e. the system becomes sensitive to random fluctuations.

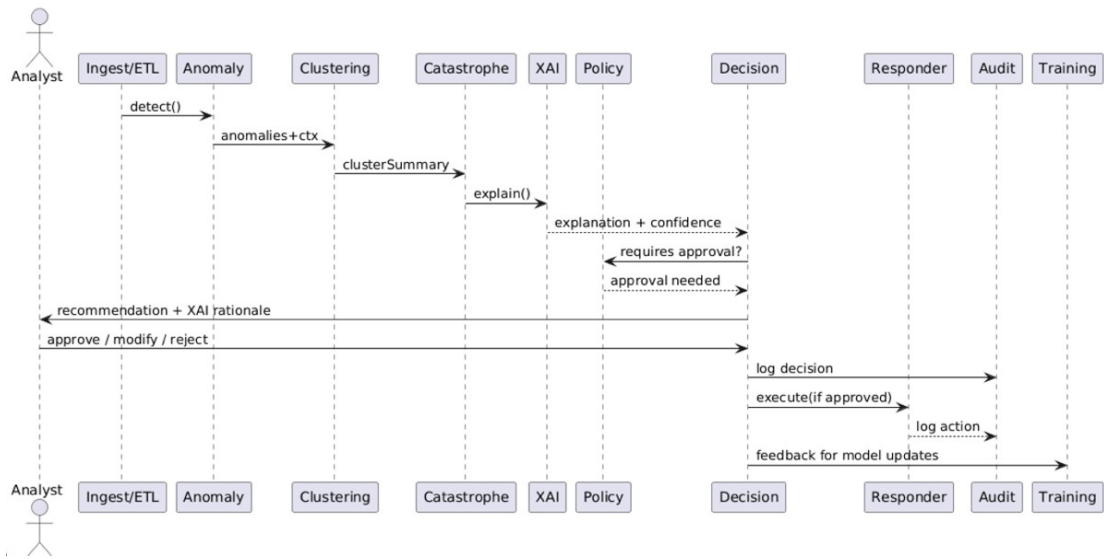
The third state Critical determines the transition of the system into a catastrophic region, which will lead to a catastrophic state, namely a violation of the stability of the cyber system, characterized by a failure or loss of control by the control system. This state is mathematically

shown by a change in the sign of the second derivative  $V''(x)$  and the instability of the energy potential

$$\frac{d^2 V(x)}{dx^2} \rightarrow 0. \quad (13)$$

At this point, the system is at a bifurcation point, which prevents the system from changing its current state. The combination of cluster analysis and catastrophe theory allows us to assess the stability of the system at a given point in time, as well as by calculating the distances to the detected bifurcation points, which make it possible to predict potential transition points between the system states.

The proposed model of an intelligent decision support system combines the interaction of an analyst and automated modules for responding to cyber incidents. Figure 3 presents a Sequence diagram, which shows the response logic of the entire system [22].



**Figure 3:** Sequence diagram “Human in the loop” (implemented in PlantUML environment)

The proposed interaction between humans and artificial intelligence allows us to bring existing systems to a new intellectual level, as well as increase the detection and prediction of cyberattacks, which in turn will increase the accuracy and stability of the system when making decisions in complex operations.

## 5. Conclusions

The mathematical model of the intelligent decision-making system, which is presented in this work, is expedient to use to increase the cyber resilience of military information systems. This model combines nonlinear dynamic modeling, mathematical catastrophe theory, cluster analysis and elements of artificial intelligence into a single decision-making system. Each of the above approaches played an essential role at its stage. Thus, the “Butterfly” type catastrophe allows you to detect transitions between the states of the information system from Stable to Critical, which allows you to detect at early positions the approach of the system to critical or catastrophic states during the impact on the information system of various types of cyber incident

The use of cluster analysis, namely the k-means method, makes it possible to restore the state of the system based on real SIEM data at a certain point in time. To predict the probability of transitions between the states of stability, change and recovery, this model uses a mathematical model of the Markov chain, which allows assessing risks. There are also SOAR-responder and audit



modules to regulate all actions, as well as a training block that allows for constant updating of models based on previous data.

The proposed model of an intelligent decision-making system combines mathematical modeling, learning, and human control, which provides robustness and transparency compared to traditional decision-making systems to ensure the cyber resilience of military information systems.

Further research will be aimed at integrating this model with real simulation systems, as well as addressing the issue of optimizing multi-criteria control parameters to increase the efficiency of decision-making in information security management systems.

## Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

## References

- [1] D. Ormrod, B. Turnbull, Developing a Military Cyber Maturity Model for Multi-Domain Battle Mission Resilience and Success, *Int. J. Cyber Warfare and Terrorism*, 2017. doi:10.4018/IJCWT.2017100101
- [2] A. Hroz dov, et al., The Method of Assessing the Sustainability of the Functioning System based on the Combat Capabilities of the Armies, *None*, 2024. doi:10.58254/viti.5.2024.05.64
- [3] S.S. Savant, S. Sharma, The Role of Internet of Battlefield Things in Modern Warfare: A Cybersecurity Perspective, *None*, 2024. doi:10.36676/jrps.v15.i3.1534
- [4] V. Nehodenko, Application of Mathematical Theory of Catastrophes to Ensure the stability of the Information Security Management System, *Cybersecur.: Educ. Sci. Technol.* 2(26) (2024) 212–222. doi:10.28925/2663-4023.2024.26.692
- [5] S. Gnatyuk, et al., Method for Managing IT Incidents in Critical Information Infrastructure Facilities, in: *Cybersecurity Providing in Information and Telecommunication Systems II*, vol. 3826 (2024) 326–333.
- [6] V. Nehodenko, Modeling Critical States in a SIEM System based on Catastrophe Theory, *Telecommun. Inf. Technol.* 2 (2025) 118–125. doi:10.31673/2412-4338.2025.028289
- [7] S. Shevchenko, et al., Mathematical Methods in Cybersecurity: Cluster Analysis and its Application in Information and Cyber Security, *Cybersecur. Educ. Sci. Technol.* 3(23), 2024, 258–273. doi:10.28925/2663-4023.2024.23.258273
- [8] S. Nabiye va, Integration of Artificial Intelligence into Communication Systems: Enhancing Performance, Adaptability, and Security, in: *Intellectual Resource of Today: Scientific Tasks, Development and Questions*, 2025. doi:10.62731/mcnd-29.08.2025.011
- [9] S. K. Rachapalli, Hybrid AI-Edge Architectures for Mission-Critical Decision Systems, *Int. J. Sci. Technol.* 14(4), 2023. doi:10.71097/ijst.v14.i4.5505
- [10] Y. Kostiuk, et al., Models and Technologies of Cognitive Agents for Decision-making with Integration of Artificial Intelligence, in: *Modern Data Science Technologies Doctoral Consortium (MoDaST)*, vol. 4005 (2025) 82–96.
- [11] D. Virovets, et al., Integration of Smart Contracts and Artificial Intelligence using Cryptographic Oracles, in: *Classic, Quantum, and Post-Quantum Cryptography*, vol. 3829 (2024) 39–46.
- [12] J. Scholtz, Theory and Evaluation of Human Robot Interactions, in: *36<sup>th</sup> Annual Hawaii International Conference on System Sciences*, 2003. doi:10.1109/hicss.2003.1174284
- [13] A. R. Magdenko, et al, 2024. Artificial Intelligence: A New Weapon in the Hands of Cebercriminals and Fraudsters. <https://ir.lib.vntu.edu./handle/123456789/42455>
- [14] L. Leenen, T. Meyer, Semantic Technologies and Big Data Analytics for Cyber Defence, *Int. J. Cyber Warfare and Terrorism*, 6(3) (2016) 53–64. doi:10.4018/IJCWT.2016070105

- [15] M. Adamantis, V. Sokolov, P. Skladannyi, Evaluation of State-of-the-Art Machine Learning Smart Contract Vulnerability Detection Method, *Advances in Computer Science for Engineering and Education VII*, vol. 242 (2025) 53–65. doi:10.1007/978-3-031-84228-3\_5
- [16] S. Shevchenko, Y. Zhdanova, O. Kryvytska, H. Shevchenko, Fuzzy Cognitive Mapping as a Scenario Approach for Information Security Risk Analysis, in: *Cybersecurity Providing in Information and Telecommunication Systems II*, vol. 3826 (2024) 356–362.
- [17] P. Theron, A. Kott. Towards an Active, Autonomous and Intelligent Cyber Defense of Military Systems: the NATO AICA Reference Architecture, in: *Int. Conf. on Military Communications and Information Systems*. 2018. doi:10.1109/ICMCIS.2018.8398730
- [18] S. Huang, C. M. Poskitt, L. K. Shar. Bayesian and Multi-Objective Decision Support for Real-Time Cyber-Physical Incident Mitigation, 2025. doi:10.48550/arXiv.2509.00770
- [19] R. Uetz, et al, You Cannot Escape Me: Detecting Evasions of SIEM Rules in Enterprise Networks, in: *33<sup>rd</sup> USENIX Conference on Security Symposium*, 290, 2024, 5179–5196.
- [20] P. Skladannyi, et al., Modified Delta Maintainability Model of Object-oriented Software. in: *Cybersecurity Providing in Information and Telecommunication Systems*, vol. 3288 (2022) 117–124.
- [21] G. González-Granadillo, et al., Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures, *Sensors* 21 (2021) 4759. doi:10.3390/s211447592
- [22] B. D. Bryant, H. Saiedian, Improving SIEM Alert Metadata Aggregation with a Novel Kill Chainbased Classification Model. *Comput. Secur.* 94(2) (2020). doi:10.1016/j.cose.2020.101817