ISSN 2412-4338

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Є ЧЛЕНОМ МІЖНАРОДНОГО СОЮЗУ ЕЛЕКТРОЗВ'ЯЗКУ

Т Е Л Е К О М У Н І К А Ц І Й Н І Т А І Н Ф О Р М А Ц І Й Н І Т Е Х Н О Л О Г І Ї

Науковий журнал

Виходить щоквартально

Засновано в січні 2003 р.

№ 4 (89) 2025

Київ
Державний університет інформаційно-комунікаційних технологій
2025

Телекомунікаційні та інформаційні технології

Свідоцтво про державну реєстрацію № 20746-10546ПР від 30.04.2014 р. (перереєстрація)

До 2013 р. – **Вісник Державного університету інформаційно-комунікаційних технологій**

Свідоцтво про державну реєстрацію КВ № 6846 від 04.01.2003 р.

Засновник: Державний університет інформаційно-комунікаційних технологій

Журнал є науковим фаховим виданням України –

Наказ Міністерства освіти і науки України від 17 березня 2020 р. № 409

Журнал занесений до Переліку наукових фахових видань України, категорія Б, в яких можуть публікуватися результати дисертаційних робіт на здобуття наукових ступенів доктора і кандидата наук (технічні науки) та доктора філософії за спеціальностями 122, 123, 125, 126, 172.

Редакція може не поділяти думок авторів. Відповідальність за зміст наданих матеріалів несуть автори.

Рекомендовано до друку Вченою радою Державного університету інформаційно-комунікаційних технологій (протокол №15 від 18 грудня 2025р.)

Передплатний індекс: **86479**

Журнал індексується в наукометричних базах Google Scholar, Crossref.

Реферативна інформація видання представлена у загальнодержавній реферативній базі даних «Україніка наукова» та публікується у відповідних тематичних серіях УРЖ «Джерело»

Адреса редакції та видавця: ДУІКТ, вул. Солом'янська, 7, м. Київ, Україна, 03110

Тел.: +380 (93) 095 94 47, +380 (44) 249 25 88

E-mail digitaldut2022@gmail.com . **Сайт:** tit.dut.edu.ua

ЗМІСТ

УДК 004.056:004.942 DOI: 10.31673/2412-4338.2025.048903

Vitalii Nehodenko
Borys Grinchenko Kyiv Metropolitan University, Kyiv
ORCID 0000-0002-7678-9138

Svitlana Shevchenko
Borys Grinchenko Kyiv Metropolitan University, Kyiv
ORCID 0000-0002-9736-8623

Olena Nehodenko
Borys Grinchenko Kyiv Metropolitan University, Kyiv
ORCID 0000-0001-6645-1566

Oksana Zolotukhina
Taras Shevchenko National University of Kyiv, Kyiv
ORCID 0000-0002-3314-417X

THE INTEGRATION OF CATASTROPHE THEORY INTO DECISION-MAKING MODELS FOR INFORMATION SECURITY MANAGEMENT SYSTEMS

Abstract: *The integration of catastrophe theory into the decision-making process in ISMS on the basis of the DSS/IISS practice as well as the use of SIEM platforms and IDS is dealt with. The focus is to detect critical behaviors in the development trend of a cyber threat, which can occur before a rapid change of system state. Cumulative analysis of cyber attack was done based on statistical data for range of 2022-2024. A global growth related with the activity of threats in cybersecurity was found, this necessity leads to the deployment of new decision-making models valuable in information security management systems (ISMS). Technical features of the IDS were investigated because the IDS is an integral component for securing information in the context of the SIEM and ISMS. It has been revealed that IDS make it possible to collect the information on opened vulnerabilities and also information about a suspicious behavior of a user as well, which creates opportunity to identify the nature of an incident. A model to detect indications of potentially risky trends by the use of IDS signals and an approach to the decision making in a Security Information and Event Management under the catastrophe theory. The study of mathematical models was performed, the main figures of merit of the effectiveness of mathematical models used for normalization, filtration, classification, collection, correlation, prioritization and analysis of events, as well as for the generation of various reports, messages, and visual data display for operational and strategic decision-making were determined. A study for system response based on catastrophe theory and its application. Four simulation case studies with different parameters were designed using Python based on the real data set of cyber incidents at months 2022-2024, data of values at months 2022-2024, and allowed changes of parameters during modeling. Guidelines for creating a response model to detected cyber incidents in the ISMS were established.*

Keywords*: Catastrophe theory, information security management system (ISMS), Intrusion Detection System (IDS), SEIM-system, bifurcation points, robustness.*

Негоденко Віталій Петрович
Київський столичний університет імені Бориса Грінченка, Київ
ORCID 0000-0002-7678-9138

Шевченко Світлана Миколаївна
Київський столичний університет імені Бориса Грінченка, Київ
ORCID 0000-0002-9736-8623

Негоденко Олена Василівна
Київський столичний університет імені Бориса Грінченка, Київ
ORCID 0000-0001-6645-1566

Золотухіна Оксана Анатоліївна
Київський національний університет імені Тараса Шевченка, Київ
ORCID 0000-0002-3314-417X

ІНТЕГРАЦІЯ ТЕОРІЇ КАТАСТРОФ У МОДЕЛІ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Анотація: *Робота присвячена актуальній задачі підвищення ефективності процесів прийняття рішень для систем управління інформаційною безпекою. Досліджено інтеграцію теорії катастроф у процес прийняття рішень в ISMS на основі практики DSS/IISS, а також використання платформ SIEM та IDS. Основна увага приділена виявленню критичних поведінкових моделей у тенденціях розвитку кіберзагроз, які можуть виникнути перед швидкою зміною стану системи. Кумулятивний аналіз кібератак був проведений на основі статистичних даних за період 2022-2024 років. Виявлено глобальне зростання, пов'язане з активністю загроз у сфері кібербезпеки, що зумовлює необхідність впровадження нових моделей прийняття рішень, цінних для систем управління інформаційною безпекою (ISMS). Досліджено технічні особливості IDS, оскільки IDS є невід'ємною складовою забезпечення інформаційної безпеки в контексті SIEM та ISMS. Виявлено, що IDS дають можливість збирати інформацію про виявлені вразливості, а також інформацію про підозрілу поведінку користувача, що створює можливість ідентифікувати характер інциденту. Запропоновано модель для виявлення ознак потенційно ризикованих тенденцій за допомогою сигналів IDS та підхід до прийняття рішень в рамках управління інформацією про безпеку та подіями відповідно до теорії катастроф. Проведено дослідження математичних моделей, визначено основні показники ефективності математичних моделей, що використовуються для нормалізації, фільтрації, класифікації, збору, кореляції, пріоритезації та аналізу подій, а також для формування різних звітів, повідомлень та візуального відображення даних для оперативного та стратегічного прийняття рішень. Дослідженно реакції системи на основі теорії катастроф та її застосування. Розроблено чотири симуляційні кейси з різними параметрами за допомогою Python на основі реального набору даних про кіберінциденти за 2022-2024 роки, даних про значення за 2022-2024 роки та дозволених змін параметрів під час моделювання. Встановлені рекомендації щодо створення моделі реагування на виявлені кіберінциденти в ISMS.*

Ключові слова: *Теорія катастроф, система управління інформаційною безпекою (ISMS), система виявлення вторгнень (IDS), система SEIM, точки біфуркації, надійність.*

1. Instruction

Current military information systems are the leading fighting force and the weight of them is given, first of all, by the security of data, which is under the constant threat of cyber attacks from a variety of Internet sources. Intense evolution of the complexity of cyber threats demands for new techniques and tools for forecasting, detecting, analyzing and reacting to them. Based on the statistical data for 2024 of the system for detection of vulnerabilities and response to cyber incidents and cyber attacks of the State Cyber Protection Center (CPC) of the State Service of Special Communications and Information Protection of Ukraine (SSSCIP), had registered slightly more than 3 million events in the field of information security. 28K incidents were related and 1042 cyber incidents were analyzed among such events [1]. This data shows the global increase in the threats' activity in cyber security, Justifying the necessity of integrating new and successful decision making models within the information security management systems (ISMS). It will be integrated with the ISMS along with the SIEM(Security Information and Event Management) platform and the Intrusion Detection System(IDS) for real-time detection and response to cyber-attacks [2]. The SIEM system, meanwhile, monitors and correlates events and offers automatic response to cyberincidents. In this article a functional reference model for the SIEM system is being considered which ensures the possibility of normalization, filtering, classification, collection, correlation, prioritization and analysis of events as well as report, message, and visual data, so as to Quick and educated decisions making. The research [4] introduces the model for detection of ID in the SIEM system, based on information and communication systems (ICS) with multi-level protection grounded on fuzzy set theory. However, this simulation based approach takes no account of the system's dynamic behavior, which results in the manual calibration and the inability to detect the covert attacks because its whole system stability has been compromised. In addition to that, machine learning techniques are also utilized in the functional support for such systems, especially in network anomaly detection [5,6]. However, the main drawback is that existing works target statistical measures of anomaly detection that do not consider dynamical change in the system, thus preventing to evaluate the ef- fect of cyber-attacks on the global stability of a system. IDS systems also log low-level activities that serve as signs of initial cyberattacks that permit prompt response to them. The principal signs of the IDS system include: stability of operation – detection of threats both with the lack false alerts in time and reliability of their revelation, accuracy of detection – the ratio of true detections to all that have been detected. These measures represent the good performance of the IDS system as ISMS infrastructure, as its speed and their right answer to cyberthreats depend from them generally speaking. For efficient

intrusion detection systems(IDS) and intrusion prevention systems(IPS), [7] utilizes the machine learning techniques. Our analysis of scientific articles indicates that although multiple studies are focusing on these systems to predict, detect and prevent cyber incidents, we still lack answers on the stability of the system as well as the predictability of critical transitions of security states of this system. Catastrophe theory is used to find the change points of the behavior of the information security management system in the work [8-9]. A model is developed to measure the effect of cyber incidents on the stability of military ISMS and identify the level of the ISMS stability, using a dataset grouped using several cyber incident detection types. The goal of this study is to incorporate catastrophe theory to decision-making model for information security management system based on SIEM, IDS and IPS system platform. Such an approach ensures a possibility to model sharp transitions of the system from a stable to a critical condition, to single out the limits of critical changes of the element, causing destabilization of the whole information security management system.

2. Features of mathematical tools in the construction of decision mechanisms for ISMS

In present-day environment, cyber incident response time in information security management systems is configured in terms of seconds, in which, therefore, lack of automation will have catastrophic effects. The decision-making module makes the process of when to isolate a node, report some threat or block the access obvious, while SIEM, IDS and IPS systems only give information about cyber incidents and discrepant situations. The primary elements of systems and their roles in implementing ISMS are reported in Table 1.

Table 1

Roles of Key ISMS Components

Component	Role in the System	Key Functions
SIEM (Security Information and Event Management)	Centralized collection, processing, and correlation of security events	Log aggregation Analytics Incident generation Event storage
IDS (Intrusion Detection System)	Detection of suspicious or anomalous activity (passive)	Network traffic analysis Anomaly/pattern detection Alerts
IPS (Intrusion Prevention System)	Real-time response to threats (active)	Blocking attacks Node isolation Traffic filtering
Decision-Making System	Analyzes risk models and incidents to choose appropriate response	State stability evaluation Action selection (MONITOR / IPS / ALERT) Automation
Security Analyst / SOC	Human oversight, verification, and manual control of responses	Incident review Manual intervention Root cause analysis
Knowledge Base / Policies	Framework for decisions, responses, and compliance	Rule definition Compliance assessment Auditing
Users and Assets	Objects of protection and sources of risk	Event sources Systems, services, files Network activity

The decision module needs to consider the nature of the threat, past experience, the dynamism in the state transition of the system, and forecast future effects. Adding these properties, the DMM provides ISMS to respond to cyber incidents influence in a prompt and dynamic manner [10, 11]. There is de-index for the new artificial intelligence type approaches (as machine learning, such as Bayesian game theory and catastrophic, which is able to identify bifurcation point and rapid changes of the state of stability to critical [9]) to construct this module as below. In the on [10,11] authors proposed the architecture of the intelligent SIEM system to detect cyber incidents occurring in databases of the military information and communication systems, and the implementation for an efficient response to incidents which, is based on artificial intelligence, in the SIEM system.

The inspection pointed out several weaknesses in the strategic performance of the SIEM system as follows:

- SIEM is a post-event reactive mechanism;
- the system operates according to rules (rule-governed);
- the number of events has stressed the system, and it is virtually impossible to detect the true threat;
- SIEM does not keep historical data of how events pile up; attacks are multi-layered, chains, APT etc.., SIEM does not see the whole context.)
- standard correlation is small in atypical attacks.

A comparative feature values of the main effectiveness metrics of mathematical model based upon the analysis of scientific publications [12–16] and averaged estimates is also presented in Table 2.

Table 2

Comparison of decision-making methods in ISMS

Criterion	Machine Learning (ML)	Bayesian Networks	Game Theory	Catastrophe Theory
Processing Type	Statistical / training-based	Probabilistic logic	Strategic modeling	Analytical dynamics
Average Decision Time	1.2 – 3.5 sec (depending on model)	2.5 – 10 sec	4 – 12 sec	0.5 – 1.0 sec
Training Requirement	Yes (pre-training)	Yes (structure + CPT)	Strategy formalization	No (parameterized model)
Historical Data Volume	>10,000 events	1,000–5,000 records	Scenarios, strategy matrix	5–20 parameters (incidents/features)
Context Dependency	High	Medium	High	Low (focus on critical points)
Adaptability to New Incidents	Low	Limited	Static	High (state-sensitive)
Accuracy (Instability Detection)	70–90% on training data	65–85%	60–80%	95–99% (with proper configuration)
Decision Interpretability	Low (black-box)	High (graph-based)	Medium	High (bifurcation map)
Catastrophic Change Prediction	Partially possible	Not implemented	Via modeling	Core functionality

It is worth noting the most important metrics employed when comparing these approaches:

1. Time to Response (sec) – time from incident to decision; - Adaptivity - possibility to adapt to new attacks without re-training;
2. Instability Detection - detecting critical transitions/bifurcations;
3. Interpretability - the being explainable of the analytics of the solution;
4. Data Materials - the amount of event histories to be accurate;
5. CPU Efficiency - the amount of time it takes to consume the processor. Table 1 was presented using a Radar Chart (Figure 1) based on Python and Matplotlib/Numpy).

The diagram depicts a strong superiority of catastrophe theory when compared to these techniques in the following important characteristics: the response speed, instability detection, interpretability, flexibility, and efficiency, and it highlights a fit use of its approach in the development of improved ISMS.

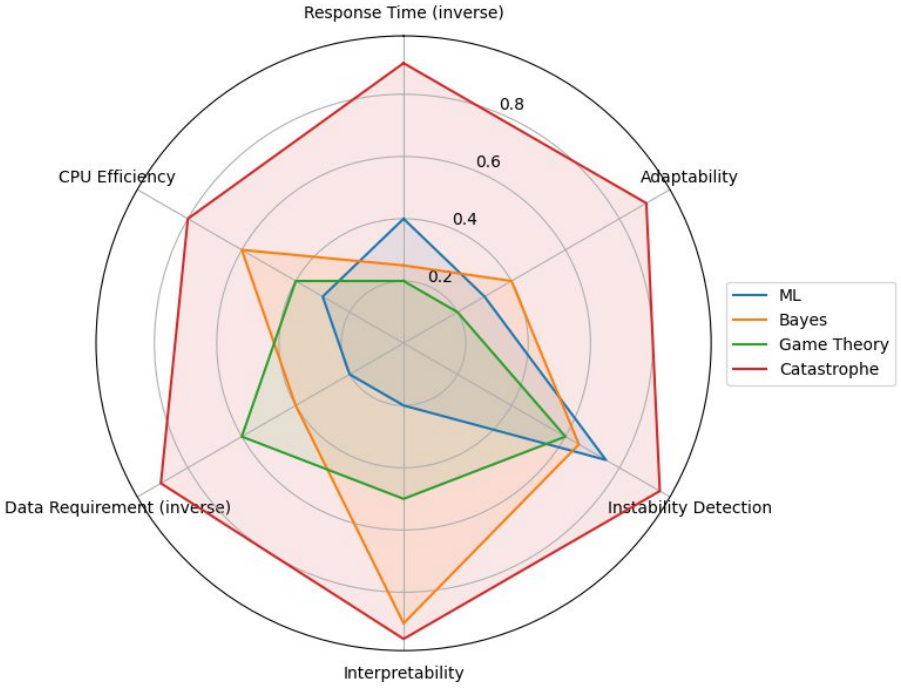

Fig 1. Radar Chart: Decision methods comparison in ISMS

3. Applying to the catastrophe theory for modeling decision-making systems operating

In order to construct a model of the detection of unstable states of the ISMS, which was subjected to the influence of cyber incidents, the mathematical apparatus of the catastrophe theory, designed to describe information systems, which are characterized by a set of parameters, is reasonable to use [14]. These include dynamism (the system is not in the same state twice), inertia (once the state has been reached it tries to stay put), hysteresis (the current state depends on how the system got there), and irreversibility (changing the parameters in the reverse direction does not mean the system will move back to its original state). In modeling complex information systems, these properties are essential, as decisions and risk bearing in information system security have non-equilibrium asymmetric dynamics [15].

To generate a modified model of decision-making, based on the catastrophe theory, the statistics of cyber attacks carried out by means of the cyber incidents realized in 2022 – 2024 were used, as well as the catastrophe of the "butterfly" type was constructed in [9], given by the generalized potential equation

$$F(x) = x^6 + cx^2 + dx,$$

where $x \in R$ the present status of the information system, $c, d \in R$ variable parameters that reflect the influence of various kinds of cyberattacks to the overall system and calculated by the weight coefficients.

Modified gradient descent was used to exhibit all possible effects that can be experienced by the system state x and consequently by the response of the decision-making system

$$x_{t+1} = x_t - \alpha \frac{dF(x)}{dx},$$

$$\frac{dF}{dx} = 6x^5 + 2cx + d,$$

where α, $\alpha \in (0;1)$ - step of change, $x_0 = 0{,}5$ - initial state of the system.

So altering the state of the system in a change of parameters creates transitions from one state in violation of the state of equilibrium. These crossings are determined by the thresholds [17,18,19]:

$$Decision(x_{t+1}) = \begin{cases} monitor, & if \ |x_{t+1}| \le \tau \\ activate\_IPS, & if \ |x_{t+1}| > \tau \\ system\_failure, & if \ x_{t+1} \notin R, \end{cases}$$

де $\tau > 0$.

It is assumed at $|\tau| \in [0;1]$ the system is in a state of equilibrium and it is possible to assume that argument is plausible because in the range from 0 to 1 the system $x, x \in R$ in the model "butterfly" catastrophe fluctuates. As $|\tau| > 1$, is changed the system starts phase of potential bifurcation, and as $|\tau| > 1{,}5$ the white part ("beginning") of the zone of system instability starts. These variations are mathematically due to inflection points of the potential, that is to say, those where the 2nd derivatives are zero. A practically significant explanation that the information system is protected is that under the condition $|\tau| > 1$ porous state, a situation when the total amount of cyber attacks exceeds the ability of the system to maintain the inertia of resistance, and given the probability of critical failure of the entire system). Hence a trade-off between a high sensitivity and stability has to be found since if $|\tau| < 1$ the system would give many false alarms, if $|\tau| > 2$ it might not succeed to detect dangerous changes in time.

Modeling with the aid of Python tools and libraries allowed to find the first day when the response of the decision-making system was with Decision = "ACTIVATE_IPS" :

{
"Date": "2022-04-07",
"x_0 (previous day)": 0.4542,
"c": 0.0,
"d": 3366.4488,
"$\nabla F(x_0)$": 3366.5648,
"x_1 (new state)": -167.874,
"Decision": "ACTIVATE_IPS"
}

In order to determine all possible response states of the decision-making system, 4 simulation cases were performed with a range of parameters, a real world-data consisting of the cyber incident values over the years 2022–2024 and allowed parameter adjustments during the simulation (Fig.2).

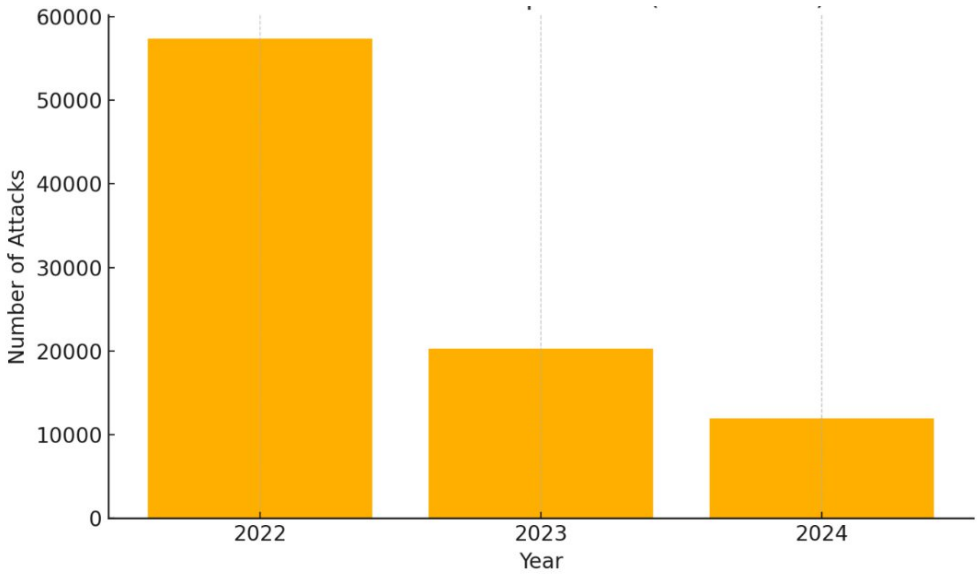

Fig.2 Number of attacks from 2022 to 2024 year

In Table 2 lists the four types of configurations, their main metrics, and the findings identified.

Table 2

Comparative Analysis of Simulation Stages

Stage	Configuration	Metrics	System Output	Conclusion
1	Baseline weights (Malware = 0.9809) Step size α = 0.01	Mean x ≈ 0.48 Δx/day ≈ 0.01 PS activations = 0	MONITOR in 100% of cases	System is stable and fully controlled
2	Malware ×3, Spam ×2 Step size α = 0.05	Mean x ≈ 0.12 Δx/day ≈ 0.03 IPS activations = 0	MONITOR in 100% of cases	State evolves faster but remains within stability zone
3	Synthetic attack: Malware > 500 High weights, no gradient limits	x = NaN ∇F(x) → ∞	System breakdown, catastrophe occurs	Model diverges — critical instability is triggered
4	Moderate attack: Malware ≈ 300 Clipped gradient: ±1000	Mean x ≈ ±18 Δx/day ≈ 1.5 PS activations = 6	ACTIVATE_IPS on each x transition	Quasi-unstable mode — model successfully signals nonlinear risk dynamics

In this document there are steps to implement a decision making algorithm in a cyber incident response system:

1.Input data from SIEM in the form of events (spam, malware, DoS; etc.).

2.Event classification by type (count per period).

3.Estimation of weighting factors for which are more significant.

4.Construction of potential function

$$V(x) = F(x,\alpha),$$

where x - is the state change of the system vector, α is the characteristic vector of the impact coefficients of the system

5. Critical points calculation to determine where the system state changes as:

5.1. solve the equation

$$\frac{dV(x)}{dx} = 0;$$

5.2. determine the real roots

$$R(t) = \left\{x \in R | \frac{dV}{dx} = 0\right\},$$

$$n(t) = |R(t)|.$$

6. Assessment of the system stability to incidents:

$$\Delta n = n(t) - n(t-1),$$

at the $\Delta n \neq 0$ transition to the critical region of the instability of the system.

7. Control commands are enacted based on the state x, the number of critical points $n(t)$), the dynamic Δn and the threshold value τ:

8.

$$Decision(x_{t+1}) = \begin{cases} monitor, & if\ |x_{t+1}| \le \tau \\ activate\_IPS, & if\ |x_{t+1}| > \tau \\ system\_failure, & if\ x_{t+1} \notin R, \end{cases}$$, де $\tau > 0$.

8. The first create an incident in the SIEM system.

9. The response in automatic mode.

The proposed model of decision making of the SIEM system based on catastrophe theory is an analytic shell of the data flow and allows for the detection of critical state changes (transition bifurcations), adapting to the dynamics of cyber threats, as well as combining automated and expert response to detected cyber incidents. Considering the observed values of the decision-making system's response to cyber incidents recorded in the period 2022-2024, it was found that 498 cases (53.3%) were of the monitor type, 426 cases (45.6%) were of the activate_IPS type, and only 10 cases (1.07%) were of the system_failure type. The results obtained indicate that the system was in most cases in a stable state and responded actively to half of the cyber attacks.

4.Conclusion

The new world of rapid actions that change the security dimensions in all aspects of life needs modern and fast cybersecurity solutions. Systems for predicting, detecting, responding and mitigating cyber incidents and for managing the information security risk in such systems are widely covered. Its data is secure, because the ISMS is responsible for securing and ensuring the integrity of data, among other things, a few of which are performed by the systems associated with the ISMS own infrastructure. This system is the overall risk management approach in the IT environment.

The review of scientific sources revealed that much research has been devoted towards systems for prediction and detection of cyber incidents, using various mathematical means to solve the relevant problems. It was also established that there is an information security management system, a certain effective structure, which has separate essential systems supplementing each other and forming together monitoring, data analysis, decision, system reaction, control of all the links, and continuous improvement. Hence, the IDS systems sends data to the SIEM - a system which creates an event. Moreover, a decision making network processes the dynamics and state to produce a decision for further action and the IPS only blocks or responds if activated.

The article is theoretically and mathematically driven and solves how the catastrophe theory can be integrated into a decision-making model for the ISS/ SIEM, iDS and IPS systems (theoretical research output). The model has been verified using Python tools and its libraries (practical part). This model will describe the possible causes of the emergence of a system on the verge and beyond-the-threshold of a system change from a stable to a critical state, and will determine the critical levels of changes, which entail a violation of the stability of the entire system of informational security management. This referred to in studying the pros and cons of the application of mathematical methods in decision-making in ISMS. An algorithm is suggested for decision-making in the systems of reaction on cyber incidents on the base of the catastrophe theory. Based on the results of the model building, it can be concluded the need for the software development to analyze the effectiveness of the control decisions made, with determining the effect of cyber accidents to be automatized and the response to them.

References

1. Annual Report 2024. Operational Service Center for Cyber Incidents of the State Center for Cyber Defense of the State Service for Special Communications and Information Protection of Ukraine. https://scpc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927c88006

2. Jabezand,J., Muthukumar, B.: Intrusiondetectionsystem(IDS): anomaly detection using outlier detection approach. Procedia Computer Science, vol. 48, 338–346 (2015). https://doi.org/10.1016/j.procs.2015.04.191

3. Samokhvalov, Yu., Toliupa, C. Koreliatsyia sobытyi v SIEM-systemakh na osnove nemonotonnoho vыvoda. Zakhyst informatsii, 19(1), 5-9 (2017). https://doi.org/10.28925/2663-4023.2023.20.8192

4. Subach, I., Kubrak, V. Model of cyber incident identification by SIEM for protection of information and communication systems. Cybersecurity: education, science, technique, vol.4(20), 81-92 (2023). https://doi.org/10.28925/2663-4023.2023.20.8192

5. Lee, J., Tang, F., Thet, P.M., Yeoh, D., Rybczynski, M., Divakaran, D.M. SIERRA: Ranking Anomalous Activities in Enterprise Networks. Conference 2022 IEEE 7th European Symposium on Security and Privacy (EuroS&P), vol. 1, 44-59 (2022). https://doi.org/10.48550/arXiv.2203.16802

6. Uetz, R., Herzog, M., Hacklander, L., Schwarz, S., Henze, M. You cannot escape me: detecting evasions of SIEM rules in enterprise networks. Proceedings of the 33rd USENIX Conference on Security Symposium, vol. 290, 5179-5196 (2024). https://www.usenix.org/conference/usenixsecurity24/presentation/uetz

7. Krishnan, P., Jain, K., Aldweesh, A. OpenStackDP: a scalable network security framework for SDN-based OpenStack cloud infrastructure. Journal of Cloud Computing: Advances, Systems and Applications, vol.12(1), 1-42 (2023). https://doi.org/10.1186/s13677-023-00406-w

8. Shevchenko, S., Skladannyi, P., Nehodenko, O., & Nehodenko, V. (2022). Study of applied aspects of conflict theory in security systems. Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 2(18), 150–162. https://doi.org/10.28925/2663-4023.2022.18.150162.

9. Nehodenko V. Application of mathematical theory of catastrophes to ensure the stability of the information security management system // Cybersecurity: education, science, technology. 2024, No. 2(26). 212 – 222. https://doi.org/10.28925/2663-4023.2024.26.692

10. Subach I., Yu., Vlasenko, O.V. Architecture of an intelligent SIEM system for detecting cyber incidents in databases of military information and communication systems // Systems and technologies of communication, informatization and cybersecurity. VITI. 2023. No. 4. P. 82 – 92. https://doi.org/10.58254/viti.4.2023.07.82

11. Z. P. Kubarych. Using artificial intelligence for effective incident response in the SIEM system: qualification work for the degree of Master in the specialty "125 - Cybersecurity" / Z. P. Kubarych. - Ternopil: TNTU, 2023. - 98 p.

12. Goodfellow, I., Bengio, Y., Courville, A. Deep learning: The MIT Press. Genetic Programming and Evolvable Machines, 775 (2016).

13. IBM Security. IBM QRadar SIEM Architecture Overview: Whitepaper. – IBM Corporation, 24 (2021). [Електронний ресурс]. – Режим доступу: https://www.ibm.com/security/security-intelligence/qradar.

14. Splunk Inc. Machine Learning Toolkit Documentation. – 2022. – [Електронний ресурс]. – Режим доступу: https://docs.splunk.com/Documentation/MLApp.

15. Shevchenko, S., Zhdanova, Y., Spasiteleva, S. (2023). Mathematical methods in cybersecurity: catastrophe theory. Cybersecurity Education Science Technique, 3(19), 165-175. https://doi.org/10.28925/2663-4023.2023.19.165175

16. González-Granadillo, G. González-Zarzosa, S. Diaz, R. Security Information and Event Management (SIEM): Analysis,Trends, and Usage in CriticalInfrastructures. Sensors 2021, 21, 4759. https://doi.org/10.3390/s21144759

17. Thom, R. Structural Stability and Morphogenesis, 348 (1975).

18. Poston, T., & Stewart, I. Catastrophe Theory and Its Applications.Physics Bulletin, 491(1996).

19. Strogatz, S.H. (2015*).* Nonlinear Dynamics and Chaos, 802 (2015).