КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА

Кваліфікаційна наукова
праця на правах рукопису

НЕГОДЕНКО ВІТАЛІЙ ПЕТРОВИЧ

УДК 004.056+355.40

ДИСЕРТАЦІЯ

МОДЕЛІ ТА МЕТОДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ВІЙСЬКОВИХ ІНФОРМАЦІЙНИХ СИСТЕМ НА ОСНОВІ ТЕОРІЙ КОНФЛІКТІВ ТА КАТАСТРОФ

Спеціальність 125 Кібербезпека
Галузь знань 12 Інформаційні технології

Подається на здобуття ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ В.П. Негоденко

Науковий керівник:
Складанний Павло Миколайович
кандидат технічних наук, доцент

Київ – 2026

АНОТАЦІЯ

Негоденко В.П. Моделі та методи забезпечення кібербезпеки військових інформаційних систем на основі теорій конфліктів та катастроф. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 125 Кібербезпека. – Київський столичний університет імені Бориса Грінченка, Київ, 2026.

Дисертаційна робота присвячена вирішенню актуального наукового завдання, суть якого полягає в розробці моделей та методів забезпечення кібербезпеки військових інформаційних систем на основі математичної теорії катастроф та теорії конфліктів для моделювання динаміки кіберзагроз, прогнозування критичних переходів станів інформаційної системи та підтримки прийняття рішень щодо підвищення її кіберстійкості.

Наявні підходи для забезпечення кібербезпеки військових інформаційних систем не враховують те, що кіберінциденти мають складну динаміку розвитку та мають вплив на функціонування системи на стратегічному, оперативному та тактичному рівнях. Дані міжнародних досліджень вказують на те, що у секторі оборони та державного управління щороку фіксують значне збільшення кількості інцидентів, при цьому складні атаки типу APT (Advanced Persistent Threat) займають до 30% від загальної їх кількості. Фіксують також, що попередньо зловмисник може перебувати місяцями в мережі, поки його буде виявлено. Така ситуація створює умови до часткової або повної втрати інформаційною системою властивостей конфіденційності, цілісності та доступності, що призведе до змін у функціонуванні військових інформаційних систем.

Сучасні системи моніторингу інформаційної безпеки, зокрема SIEM - системи фіксують щоденно від 100 до 100000 подій безпеки, які часто мають слабку кореляцію між собою. Це ускладнює відстеження впливу кіберінцидентів на різні рівні структури та перешкоджає побудові часових прогнозів, що, зрештою,

зумовлює нелінійну динаміку станів інформаційної системи. Існуючі моделі підтримки прийняття рішень використовують лінійні або статистичні підходи, які не дозволяють оцінити ризики таких критичних переходів в станах системи.

Таким чином, в теорії та практиці забезпечення кіберстійкості військової ІТ-системи виявилися суперечності між:

- об'єктивною складністю та нелінійним характером змін станів військових ІТ-систем і обмеженими можливостями моделей, які базуються на лінійних або статичних підходах до опису процесів кібербезпеки;
- необхідністю прогнозування та завчасного виявлення критичних переходів (точок відмови) військової ІТ-системи в умовах деструктивних впливів та недостатньою спроможністю існуючих методів прогнозувати поведінку системи у кризові моменти;
- потребою у високій швидкості та точності прийняття рішень в умовах реального часу та недосконалістю поточного аналітичного апарату, який не дозволяє ефективно оцінювати ці кіберризики.

Необхідність розв'язання окреслених суперечностей визначає актуальність та доцільність проведення даного дослідження.

У відповідності до поставленої мети дисертаційного дослідження, яка полягає в підвищенні кіберстійкості військових інформаційних систем за рахунок розробки моделей та методів забезпечення кібербезпеки на основі застосування математичної теорії катастроф та теорії конфліктів для аналізу та моделювання складної нелінійної динаміки функціонування систем під впливом кіберзагроз і прогнозування критичних переходів їх станів, було отримано наукові результати:

1. Вперше запропоновано математичну модель впливу кіберінцидентів на стійкість систем управління інформаційною безпекою з використанням катастрофи типу «Метелик», що дозволяє прогнозувати перехід системи до небезпечного стану, яка відрізняється від лінійних моделей оцінювання ризиків тим, що враховує нелінійну динаміку змін станів інформаційної системи та дозволяє виявляти передкризові режими функціонування системи. Використання запропонованої

моделі збільшує в 2,5 рази час попередження про перехід стану системи до критичного.

2. Удосконалено метод кластеризації загроз та уразливостей, який на відміну від методу k-means, враховує часову динаміку кіберінцидентів, що забезпечує високу часову узгодженість (0,985), а використання ковзних часових рядів дозволяє зменшити шум в даних приблизно 85%, що зменшує суб'єктивність експертних оцінок і підвищує об'єктивність управління ризиками у військових інформаційних системах.

3. Вперше запропоновано модель прогнозування критичних переходів, яка забезпечує підвищення рівня кіберстійкості військових інформаційних систем за рахунок інтеграції теорії катастроф у SIEM-системи. На відміну від традиційних підходів моніторингу кіберінцидентів, запропонована модель забезпечує виявлення нестійкі режими функціонування системи та формування сигналів про перехід системи до критичного стану. Використання даної моделі дозволяє SIEM-системі за 2-3 дні сформувати попередження про перехід інформаційної системи до критичного стану.

4. Набув подальшого розвитку метод підтримки прийняття рішень для забезпечення кіберстійкості військових інформаційних систем, який базується на інтеграції математичних моделей, методів аналізу та прогнозування на основі теорій конфліктів та катастроф. Запропонований метод забезпечує комплексне виявлення, класифікацію та прогнозування критичних станів на 15-25% в порівнянні з методами машинного навчання (SVM, Random Forest), що дозволяє своєчасно попереджати розвиток небезпечних кіберінцидентів.

У вступі обґрунтовано актуальність та важливість теми дисертаційного дослідження, сформульована мета та задачі дослідження, визначено основні положення, а також наукову та практичну цінність отриманих результатів та зазначено особистий внесок автора.

У першому розділі проведено аналіз поточного стану дослідження наукової проблеми. Визначено основні компоненти структури та функціональних

особливостей військових інформаційних систем. Проведено аналіз кіберзагроз та уразливостей військових інформаційних систем та визначено їх вплив на рівні функціонування системи. Результати порівняльного аналізу відомих науково-технічних рішень та ідентифікація їхніх функціональних обмежень стали основою для обґрунтування мети дослідження та наукових задач.

У другому розділі проведено аналіз математичної основи стійкості динамічних інформаційних систем на основі теорії катастроф. Встановлено, що інформаційні системи кіберзахисту мають складну нелінійну динамічну структуру, стан яких змінюється під впливом кібератак, внутрішніх збурень чи людських факторів. Проведено моделювання сценаріїв втрати стійкості системи, наявності станів рівноваги та різких переходів між станами системи на основі елементарних типів катастроф. Визначено, що наявність біфуркаційних точок у нелінійних динамічних системах кіберзахисту визначають параметри, які показують інтенсивність атак, затримки в реагуванні на рівень захисту та дозволяють прогнозувати появу катастрофічних змін в системі. Проаналізовано сучасні інформаційні технології, які дозволяють проводити командно-штабні навчання у форматі, де динаміка бойових дій моделюється і відображається в масштабі реального часу. Встановлено, шо небезпечним для даного середовища є наявність конфлікту, що переростає в активну стадію, коли виникають різкі зміни та стрибкоподібні процеси, що пов’язані з інцидентами у інформаційній та кібербезпеці, тому доцільно застосувати теорії катастроф та конфліктів для забезпечення стійкості даних інформаційних систем.

У третьому розділі розроблено математичну модель прогнозування критичних станів систем управління інформаційною безпекою військового призначення на основі теорії катастроф. Запропонована математична модель дозволяє визначити точки рівноваги, критичні пороги стійкості та біфуркації станів, що відповідає фіксації переходів системи від стійкого до нестабільного або критичного стану інформаційної системи. Удосконалено метод кластеризації загроз та уразливостей військових інформаційних систем для встановлення

режимів функціонування системи та переходу між ними. Розроблений алгоритм базується на основі k-means із врахуванням часової динаміки та інтегральних показників критичності стану системи.

За результатами проведених досліджень розроблено математичну модель обробки та захисту інформаційних потоків у військових IT-системах. Модель базується на релевантній вибірці даних про кіберінциденти за період 2020–2024 років, методологічному апараті теорії катастроф та включає покроковий алгоритм її імплементації в архітектуру SIEM-системи.

Удосконалено метод підтримки прийняття рішень для забезпечення кіберстійкості військових інформаційних систем на основі теорії катастроф, теорії конфліктів та кластерного аналізу для прогнозування критичних переходів станів військових інформаційних систем під дією кіберзагроз та уразливостей.

У четвертому розділі проведено комп'ютерне моделювання в середовищі Python математичної моделі катастрофи типу «Метелик» для прогнозування критичних станів системи за допомогою набору кіберінцидентів за 2022-2024 роки. Визначено показники $\Delta T, K_{cov}, FAR\ , I$ для лінійної моделі агрегованого ризику, моделі ранніх попереджувальних сигналів CSD та розробленої математичної моделі катастрофи типу «Метелик». Результати показали, що використання запропонованої моделі збільшує в 2,5 рази час попередження про перехід стану системи до критичного. Проведено імітаційне моделювання удосконаленого методу кластеризації загроз та уразливостей для виявлення переходів між стабільними, змінними та критичними станами інформаційної системи. Здійснено порівняння методів k-means та DBSCAN за допомогою основних метрик, які дозволили показати, що удосконалений метод кластеризації загроз та уразливостей враховує часову динаміку кіберінцидентів, що забезпечує високу часову узгодженість (0,985), а використання ковзних часових рядів дозволяє зменшити шум в даних приблизно 85%. Проведено експериментальне дослідження за допомогою середовища Python для оцінки ефективності моделі прогнозування критичних переходів станів системи при інтеграції з SIEM-системою. На відміну

від традиційних підходів моніторингу кіберінцидентів, запропонована модель забезпечує виявлення нестійких режимів функціонування системи та формування сигналів про перехід системи до критичного стану. Побудовано сценарії реагування системи на кіберзагрози на основі удосконаленого методу підтримки прийняття рішень для забезпечення кіберстійкості військових інформаційних систем. Запропонований метод забезпечує комплексне виявлення, класифікацію та прогнозування критичних станів на 15-25% в порівнянні з методами машинного навчання (SVM, Random Forest), що дозволяє своєчасно попереджати розвиток небезпечних кіберінцидентів.

Дисертація виконувалась в Київському столичному університеті імені Бориса Грінченка.

Результати наукових досліджень були використані на кафедрі інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка в рамках науково-дослідної роботи: «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури» (№0122U200483, КСУБГ, м. Київ).

Також результати досліджень прийняті до впровадження в діяльність Київського столичного університету імені Бориса Грінченка (акт від 09.12.2025 року), Інституту програмних систем Національної академії наук України (акт від 09.12.2025 року), військової частини А2393 (довідка від 05.02.2026.) та Військового інституту телекомунікацій та інформатизації імені Героїв Крут (22.03.2026).

Ключові слова: кібербезпека, захист інформації, ризик, інцидент, загроза, уразливість, інформаційна система, управління інформаційною безпекою, кластерний аналіз, теорія конфліктів, теорія катастроф, кіберстійкість.

ANNOTATION

Nehodenko V.P. Models and methods of ensuring cybersecurity of military information systems based on catastrophe theory and conflict theory. – Qualification scientific work in the form of a manuscript.

Dissertation for the degree of Doctor of Philosophy in specialty 125 Cybersecurity. – Borys Grinchenko Kyiv Metropolitan University, Kyiv, 2026.

The dissertation is dedicated to solving a relevant scientific problem, the essence of which is to develop models and methods for ensuring the cybersecurity of military information systems based on the mathematical catastrophe theory and conflict theory for modeling the dynamics of cyber threats, predicting critical state transitions of the information system, and supporting decision-making to increase its cyber resilience.

Existing approaches to ensuring cybersecurity of military information systems do not take into account the fact that cyber incidents have complex development dynamics and affect the functioning of the system at the strategic, operational and tactical levels. International research data indicate that a significant increase in the number of incidents are recorded in the defense and public administration sectors every year, with complex attacks such as APT (Advanced Persistent Threat) accounting for up to 30% of the total number. It is also recorded that an attacker can be in the network for months before being detected. This situation creates conditions for partial or complete loss of confidentiality, integrity and availability properties of the information system, which will lead to changes in the functioning of military information systems.

Modern information security monitoring systems, in particular SIEM systems, record from 100 to 100,000 security events daily, which often have weak correlation with each other. This makes it difficult to track the impact of cyber incidents on different levels of the structure and prevents the construction of time forecasts, which ultimately leads to nonlinear dynamics of the states of the information system. Existing decision support

models use linear or statistical approaches that do not allow assessing the risks of such critical transitions in the states of the system.

Thus, in the theory and practice of ensuring the cyber resilience of military IT systems, contradictions have emerged between:

- the objective complexity and nonlinear nature of changes in the states of military IT systems and the limited capabilities of models based on linear or static approaches to describing cybersecurity processes;
- the need to predict and early detect critical transitions (failure points) of a military IT system under conditions of destructive influences and the insufficient ability of existing methods to predict the behavior of the system in moments of crisis;
- the need for high speed and accuracy of decision-making in real time and the imperfection of the current analytical apparatus, which does not allow for effective assessment of these cyber risks.

The need to resolve the outlined contradictions determines the relevance and expediency of this study.

In accordance with the stated goal of the dissertation research, which is to increase the cyber resilience of military information systems by developing models and methods for ensuring cybersecurity based on the application of mathematical catastrophe theory and conflict theory for analyzing and modeling the complex nonlinear dynamics of the functioning of systems under the influence of cyber threats and predicting critical transitions of their states, the following scientific results were obtained:

1. For the first time, a mathematical model of the impact of cyber incidents on the stability of information security management systems using a "Butterfly" type catastrophe has been proposed, which allows predicting the transition of the system to a dangerous state, which differs from linear risk assessment models in that it takes into account the nonlinear dynamics of changes in the states of the information system and allows identifying pre-crisis modes of the system's functioning. The use of the proposed model increases the warning time for the transition of the system state to critical by 2.5 times.

2. The method for clustering threats and vulnerabilities has been improved, which, unlike the k-means method, takes into account the temporal dynamics of cyber incidents, which ensures high temporal consistency (0.985), and the use of moving time series allows reducing noise in the data by approximately 85%, which reduces the subjectivity of expert assessments and increases the objectivity of risk management in military information systems.

3. For the first time, a model for predicting critical transitions has been proposed, which provides an increase in the level of cyber resilience of military information systems by integrating the catastrophe theory into SIEM systems. Unlike traditional approaches to monitoring cyber incidents, the proposed model provides for the detection of unstable modes of system operation and the formation of signals about the transition of the system to a critical state. The use of this model allows the SIEM system to generate a warning about the transition of the information system to a critical state within 2-3 days.

4. A decision support method for ensuring cyber resilience of military information systems has been further developed, which is based on the integration of mathematical models, analysis and forecasting methods based on conflict theory and catastrophe theory. The proposed method provides comprehensive detection, classification and forecasting of critical states by 15-25% compared to machine learning methods (SVM, Random Forest), which allows for timely prevention of the development of dangerous cyber incidents.

The introduction substantiates the relevance and importance of the topic of the dissertation research, formulates the goal and objectives of the research, defines the main provisions, as well as the scientific and practical value of the results obtained, and indicates the personal contribution of the author.

The first section analyzes the current state of research on the scientific problem. The main components of the structure and functional features of military information systems are identified. An analysis of cyber threats and vulnerabilities of military information systems is carried out and their impact on the level of system functioning is determined. The results of a comparative analysis of known scientific and technical

solutions and the identification of their functional limitations became the basis for substantiating the goal of the research and scientific objectives.

The second section analyzes the mathematical basis of the stability of dynamic information systems based on the catastrophe theory. It is established that cyber defense information systems have a complex nonlinear dynamic structure, the state of which changes under the influence of cyber attacks, internal disturbances or human factors. The simulation of scenarios of system stability loss, the presence of equilibrium states, and sharp transitions between system states based on elementary types of catastrophes was carried out. It was determined that the presence of bifurcation points in nonlinear dynamic cybersecurity systems determine the parameters that show the intensity of attacks, delays in responding to the level of protection and allow predicting the occurrence of catastrophic changes in the system. Modern information technologies are analyzed that allow conducting command and staff exercises in a format where the dynamics of combat operations are simulated and displayed in real time. It has been established that the presence of a conflict that develops into an active stage, when sharp changes and jump-like processes related to incidents in information and cybersecurity occur, is dangerous for this environment, therefore it is advisable to apply catastrophe theory and conflict theory to ensure the stability of these information systems.

In the third section, a mathematical model for predicting critical states of military information security management systems based on catastrophe theory is developed. The proposed mathematical model allows determining equilibrium points, critical thresholds of stability and bifurcation of states, which corresponds to fixing the transitions of the system from stable to unstable or critical states of the information system. The method of clustering threats and vulnerabilities of military information systems is improved to establish the modes of system operation and the transition between them. The developed algorithm is based on k-means, taking into account time dynamics and integral indicators of the criticality of the system state.

Based on the results of the research, a mathematical model for processing and protecting information flows in military IT systems has been developed. The model is

based on a relevant sample of data on cyber incidents for the period 2020–2024, the methodological apparatus of catastrophe theory, and includes a step-by-step algorithm for its implementation in the architecture of the SIEM system.

A decision support method has been improved to ensure the cyber resilience of military information systems based on catastrophe theory, conflict theory, and cluster analysis to predict critical state transitions of military information systems under the influence of cyber threats and vulnerabilities.

In the fourth section, computer simulation of a mathematical model of a "Butterfly" type catastrophe for predicting critical system states using a set of cyber incidents for 2022-2024 is carried out in the Python environment. The indicators $\Delta T, K_{cov}, FAR$, I for the linear aggregate risk model, the CSD early warning signal model, and the developed mathematical model of the “Butterfly” type catastrophe were determined. The results showed that the use of the proposed model increases the warning time of the transition of the system state to critical by 2.5 times. Simulation modeling of the improved method of clustering threats and vulnerabilities to detect transitions between stable, variable, and critical states of the information system was carried out. The k-means and DBSCAN methods were compared using the main metrics, which showed that the improved method of clustering threats and vulnerabilities takes into account the time dynamics of cyber incidents, providing high time consistency (0.985), while the use of moving time series reduces noise in the data by approximately 85%. An experimental study was conducted using the Python environment to assess the effectiveness of the model for predicting critical transitions of system states when integrated with the SIEM system. Unlike traditional approaches to monitoring cyber incidents, the proposed model provides for the detection of unstable modes of system operation and the formation of signals about the transition of the system to a critical state. Scenarios of the system's response to cyber threats are built on the basis of an improved decision support method to ensure cyber resilience of military information systems. The proposed method provides comprehensive detection, classification and prediction of critical states by 15-25% compared to machine

learning methods (SVM, Random Forest), which allows for timely prevention of the development of dangerous cyber incidents.

The dissertation was carried out at the Borys Grinchenko Kyiv Metropolitan University.

The results of scientific research were used at the Department of Information and Cybersecurity named after Professor Volodymyr Buriachok at the Borys Metropolitan Grinchenko Kyiv University within the framework of research work: “Methods and Models for Ensuring Cybersecurity of Information Processing Systems and Functional Security of Software and Hardware Complexes for Critical Infrastructure Management” (No. 0122U200483, BGKMU, Kyiv).

Also, the results of scientific research have been accepted for implementation in the activities of the Borys Metropolitan Grinchenko Kyiv University (act dated 09.12.2025), of the Institute of Software Systems of the National Academy of Sciences of Ukraine (act dated 09.12.2025), of the military unit A2393 (certificate dated 05.02.2026) and of the Military Institute of Telecommunications and Informatization named after Heroes Krut (act dated 22.03.2026).

Keywords: cybersecurity, information protection, risk, incident, threat, vulnerability, information system, information security management, cluster analysis, conflict theory, catastrophe theory, cyber resilience.

Наукові статті, опубліковані у наукових виданнях, включених на дату опублікування до переліку наукових фахових видань України:

1. Шевченко, С., Складанний, П., Негоденко, О., **Негоденко, В.** (2022). Дослідження прикладних аспектів теорії конфліктів у системах безпеки. *Кібербезпека: освіта, наука, техніка,* No2(18), 150–162. https://doi.org/10.28925/2663-4023.2022.18.150162.

2. **Негоденко, В.** (2023). Дослідження інформаційних конфліктів у системі навчання ЗСУ за допомогою імітаційного моделювання. *Кібербезпека: освіта, наука, техніка*, 4(20), 164–173, https://doi.org/10.28925/2663-4023.2023.20.164173.

3. Шевченко, С., Жданова, Ю., Спасітєлєва, С., Мазур, Н., Складанний П., **Негоденко, В.** (2024). Математичні методи в кібербезпеці: кластерний аналіз та його застосування в інформаційній та кібернетичній безпеці. Кібербезпека: освіта, наука, техніка, 3(23), 258–273. https://doi.org/10.28925/2663-4023.2024.23.258273.

4. **Негоденко, В**. (2024). Застосування математичної теорії катастроф для забезпечення стійкості системи управління інформаційною безпекою. *Кібербезпека: освіта, наука, техніка: електронне наукове видання*, 2(26), 212–222. https://doi.org/10.28925/2663-4023.2024.26.692.

5. Nehodenko, O., Shevchenko, S., **Nehodenko, V**., Zolotukhina, O. (2025). The Integration of Catastrophe Theory into Decision-Making Models for Information Security Management Systems. *Telecommunication and information technologies*, 2025, 4(2025), 20–28. https://doi.org/10.31673/2412-4338.2025.048903.

6. Негоденко, В. (2025). Моделювання критичних станів в SIEM-системі на основі теорії катастроф. *Телекомунікаційні та інформаційні технології*, 2(2025), 118–125. https://doi.org/10.31673/2412-4338.2025.028289.

Наукові публікації, у яких додатково висвітлено результати дисертації:

1. Skladannyi, P., Nehodenko, O., Shevchenko, S., Zolotukhina, O., & **Nehodenko, V.** (2022). Modified delta maintainability model of object-oriented software. Paper presented at the CEUR Workshop Proceedings, 3288, pp. 117–124. (Scopus).

2. **Негоденко, В.** Кластерний аналіз для прогнозування кібератак в інформаційних системах. (2024). *На XI Всеукраїнськиї науково-практичніǐ конференції молодих учених «Інформаційні технології – 2024»*, 248–250.

3. **Негоденко В.**, Негоденко, О. (2024). Методи Data Science для підтримки прийняття рішень щодо прогнозування кібератак в інформаційних системах. *На XIII Міжнародній конференції «ITSec».Безпека інформаційних технологій*, 157–159.

4. **Nehodenko, V.** Impact of cyber incidents on the resilience of the information security management system. *На II Міжнародній науково-практичній конференції «Сучасні аспекти діджиталізації та інформатизації в програмній та комп'ютерній інженерії»*, 226–229.

5. **Негоденко, В**., Шевченко, С., Негоденко, О. Прогнозування кіберінцидентів у SIEM-системі на основі теорії катастроф. *На XII Всеукраїнській науково-практичній конференції молодих учених* «Інформаційні технології – 2025» (IT-2025), 300–302.

6. **Nehodenko, V.,** Shevchenko, S., Zolotukhina, O., Nehodenko, O., Zhdanova, Y. (2025). Model of an intelligent decision support system to ensure cyber resilience of military information systems. Paper presented at the CPITS'II Workshop Proceedings, 4145, 307–315.

7. Shevchenko, S., Zolotukhina, O., Nehodenko, O., Zhdanova, Y., Spasiteleva, S., **Nehodenko, V.** (2025). Research of Information Conflict between Humans and Artificial Intelligence in Information and Cybernetic Systems. Paper presented at the CEUR Workshop Proceedings, 3991, 311–322. (Scopus).

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ВІС – військова іформаційна система

СУІБ – система управління інофрмаційною безпекою

SIEM – Security Information and Event Management ‘система управління інформацією та подіями безпеки’

IDS – Intrusion Detection System ‘система виявлення вторгнень’

IPS – Intrusion Prevention System ‘система запобігання вторгнень’

CSD – Critical Slowing Down ‘алгоритм критичного уповільнення’

DBSCAN – Density-Based Spatial Clustering of Applications with Noise ‘алгоритм кластеризації на основі щільності даних’

ВСТУП

Обґрунтування вибору теми дослідження. Глобальна інформаційна еволюція та інтенсифікація відповідних процесів перетворили інформацію на ключовий стратегічний ресурс військових інформаційно-телекомунікаційних (ІТ) систем. Згідно із звітом оперативного центру реагування на кіберінциденти Державного центру кіберзахисту державної служби спеціального зв’язку та захисту інформації України за 2024 [1] та 2025 роки [2] найактивнішими виявленими кластерами кіберзагроз були UAC-0010, UAC-0006 та UAC-0050 (за класифікацією CERT-UA) саме на державні органи та сили оборони. Усвідомлення критичної важливості захисту інформаційного простору підкріплюється значними бюджетними асигнуваннями для реалізації відповідних інфраструктурних проєктів на міжнародній арені. Прогнозується, що світовий ринок військової кібербезпеки зросте з 19,2 мільярда доларів у 2024 році до 66,3 мільярда доларів до 2034 року, що відображає зростаючу важливість безпечного зв'язку в сучасній війні [3]. Все це детермінує об’єктивну необхідність розробки цілісних систем кіберзахисту та гарантування безпеки критичних даних у ІТ-системах командування та управління, моніторингу розвідки, програмного забезпечення для логістичних дій, комунікаційних мережах та інструментах управління полем бою. Здійснюється перехід до програмно-визначеної безпечної архітектури, інтеграції штучного інтелекту для прогнозування та реагування на загрози.

Підтвердження зазначеного відображається у державних нормативних документах, зокрема наказом 692/нм від 15 жовтня 2025 року відповідно до статті 10 Закону України «Про захист інформації в інформаційно-комунікаційних системах», пункту 4 Порядку розроблення та затвердження профілів безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем, затверджений постановою Кабінету Міністрів України від 18 червня 2025 року №712, підпункт 113 пункту 4 Положення про Міністерство оборони України від 26 листопада 2014 року №671 та з метою підвищення

інформаційної безпеки та кібербезпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем Міністерства оборони України було затвержено Галузевий профіль безпеки систем, де обробляється відкрита, конфіденційна або службова інформація. Даний Галузевий профіль безпеки систем відповідає вимогам міжнародних стандартів і національного законодавства з урахуванням особливостей оборонної галузі [4].

Відповідно до сучасних вимог сьогодення військові ІТ системи побудовані за принципом стійкості, що забезпечує безперервність та безпеку операцій при дії кіберзагроз за рахунок резервування, розділення мереж та шифруванні ліній зв'яку. Але при цьому зростає також розвиток складності самих загроз, які вже більш адаптивні, складні для виявлення та мають комплексно багаторівневу зону атаки. Статичні моделі та класичні методи захисту інформації не завжди враховують динамічний і конфліктний вплив загроз на уразливості інформаційної системи, тому доцільно застосовувати теорію конфліктів, яка дозволяє описати поведінку реагування на кіберзагрози, а також оцінити ефективність різних стратегій щодо забезпечення безпеки інформаційних систем.

Очевидно, що функціонування складних інформаційних систем не є лінійним, характеризується виникненням критичних станів, що можуть зумовити стохастичні переходи від нормативного режиму до стадії часткової або повної відмови. У зазначеному контексті ефективним інструментарієм для розв'язання даної проблеми є математична теорія катастроф, яка дозволяє не тільки виявляти, але і прогнозувати виникнення критичних точок, нестійкості та дестабілізації системи під впливом загроз.

Таким чином, існує необхідність вирішення актуального наукового завдання, сутність якого полягає у дослідженні та розвитку моделей та методів забезпечення кібербезпеки військових інформаційних систем на основі математичної теорії катастроф та теорії конфліктів з метою аналізу динаміки кіберзагроз, прогнозування критичних переходів станів системи та підвищення її кіберстійкості.

Дослідження проблеми забезпечення кібербезпеки інформаційних систем та підвищення їх кіберстійкості представлені у працях багатьох вчених, серед яких В. Бурячок, О. Корченко, О. Юдін, С. Гуцалюк, М. Опірський, Л. Крючкова, R. Ross, V. Pillitteri, U. Franke, J. Brynielsson, T. Alpcan, T. Basar, M. H. Manshaei, R. Thom, E. Zeeman, S. Wiggins, J.P. Hubaux, Q. Zhu, D. Nicol, W. Sanders, K. Trivedi та інші.

Проведений аналіз сучасних наукових досліджень показав, що більшість існуючих підходів використовують статистичні методи, методи машинного навчання або класичні моделі для аналізу та прогнозування стану інформаційних систем при дії загроз. Безперечно, проведення таких досліджень є доцільним та результативним, адже вони зробили вагомий внесок у розвиток наявної бази захисту інформації. Проте дані підходи не враховують конфліктну взаємодію між джерелами кібератак та системою захисту інформаційної системи, а також складну нелінійну динаміку функціонування інформаційних систем, що призводить до виникнення критичних станів системи та втрати їх стійкості.

Таким чином, необхідно вирішити актуальне наукове завдання, яке полягає в розробці моделей та методів забезпечення кібербезпеки військових інформаційних систем на основі математичної теорії катастроф та теорії конфліктів для моделювання динаміки кіберзагроз, прогнозування критичних переходів станів інформаційної системи та підтримки прийняття рішень щодо підвищення її кіберстійкості.

Зв’язок роботи з науковими програмами, планами, темами. Напрям дисертаційного дослідження безпосередньо пов’язаний з реалізацією доктрини інформаційної безпеки України, Стратегії інформаційної безпеки та Стратегії кібербезпеки України. Дисертаційна робота виконана відповідно до планів наукової і науково-технічної діяльності Київського столичного університету імені Бориса Грінченка в рамках науково-дослідної роботи: «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури» (№0122U200483, КСУБГ, м. Київ).

Мета і завдання дослідження. *Мета* дисертаційного дослідження полягає в підвищенні кіберстійкості військових інформаційних систем за рахунок розробки моделей та методів забезпечення кібербезпеки на основі застосування математичної теорії катастроф та теорії конфліктів для аналізу та моделювання складної нелінійної динаміки функціонування систем під впливом кіберзагроз і прогнозування критичних переходів їх станів.

У відповідності до поставленої мети для вирішення наукового завдання в роботі визначено та розв'язано такі *часткові завдання*:

- проаналізовано сучасні підходи забезпечення кібербезпеки військових інформаційних систем та визначено особливості нелінійної динаміки їх станів під впливом кіберінцидентів;
- обґрунтовано доцільність застосування математичної теорії катастроф та теорії конфліктів для моделювання динаміки станів інформаційних системи під впливом кіберінцидентів;
- розроблено математичну модель впливу кіберінцидентів на стійкість систем управління інформаційною безпекою з використанням катастрофи типу «Метелик» та проведено оцінку її ефективності щодо впливу кіберінцидентів на стійкість систем;
- удосконалено метод кластеризації загроз та уразливостей інформаційних систем та проведено порівняльну оцінку його ефективності з класичними методами кластеризації;
- розроблено модель прогнозування критичних переходів станів інформаційної системи при інтеграції з SIEM- системою та проведено оцінку ефективності її застосування для раннього виявлення нестійких режимів функціонування системи;
- удосконалено метод підтримки прийняття рішень для забезпечення кіберстійкості військових інформаційних систем, який включає інтеграцію математичних моделей , методів аналізу та прогнозування на основі теорії

конфліктів для моделювання протидії кіберзагрозам та теорії катастроф для прогнозування критичних станів системи;

- проведено оцінку ефективності удосконаленого методу підтримки прийняття рішень шляхом імітаційного моделювання сценаріїв реагування на кіберінциденти.

Об'єктом дослідження є процес функціонування військових інформаційних систем в умовах деструктивних кібервпливів.

Предметом дослідження є моделі та методи забезпечення кібербезпеки військових інформаційних систем на основі теорій конфліктів та катастроф для аналізу та прогнозування критичних переходів станів інформаційних систем.

Методи дослідження. Для проведення досліджень в дисертаційній роботі використовувалися методи теорії конфліктів, методи теорії катастроф, методи кластерного аналізу; теорія функцій, теорія алгоритмів, теорія складності алгоритмів, теорії ймовірностей та математичної статистики; математичне, комп'ютерне та імітаційне моделювання.

Наукова новизна одержаних результатів полягає в подальшому розвитку і обґрунтуванні методів прогнозування та підтримки прийняття рішень для забезпечення кіберстійкості військових інформаційних систем на основі теорії конфліктів, теорії катастроф та методу кластерного аналізу.

1.Вперше запропоновано математичну модель впливу кіберінцидентів на стійкість систем управління інформаційною безпекою з використанням катастрофи типу «Метелик», що дозволяє прогнозувати перехід системи до небезпечного стану, яка відрізняється від лінійних моделей оцінювання ризиків тим, що враховує нелінійну динаміку змін станів інформаційної системи та дозволяє виявляти передкризові режими функціонування системи. Використання запропонованої моделі збільшує в 2,5 рази час попередження про перехід стану системи до критичного.

2. Удосконалено метод кластеризації загроз та уразливостей, який на відміну від методу k-means, враховує часову динаміку кіберінцидентів, що забезпечує

високу часову узгодженість (0,985), а використання ковзних часових рядів дозволяє зменшити шум в даних приблизно 85%, що зменшує суб'єктивність експертних оцінок і підвищує об'єктивність управління ризиками у військових інформаційних системах.

3. Вперше запропоновано модель прогнозування критичних переходів, яка забезпечує підвищення рівня кіберстійкості військових інформаційних систем за рахунок інтеграції теорії катастроф у SIEM-системи. На відміну від традиційних підходів моніторингу кіберінцидентів, запропонована модель забезпечує виявлення нестійкі режими функціонування системи та формування сигналів про перехід системи до критичного стану. Використання даної моделі дозволяє SIEM-системі за 2-3 дні сформувати попередження про перехід інформаційної системи до критичного стану.

4. Набув подальшого розвитку метод підтримки прийняття рішень для забезпечення кіберстійкості військових інформаційних систем, який базується на інтеграції математичних моделей, методів аналізу та прогнозування на основі теорій конфліктів та катастроф. Запропонований метод забезпечує комплексне виявлення, класифікацію та прогнозування критичних станів на 15-25% в порівнянні з методами машинного навчання (SVM, Random Forest), що дозволяє своєчасно попереджати розвиток небезпечних кіберінцидентів.

Практичне значення одержаних результатів полягає в тому, що в дослідженні запропоновано моделі та методи аналізу та прогнозування критичних станів військових інформаційних систем, які доцільно використовувати для підвищення ефективності попередження та виявлення кіберінцидентів, а також підтримки прийняття рішення під час реагування на кіберзагрози. Розроблену модель прогнозування критичних переходів станів інформаційної системи при інтеграції в SIEM-систему можливо впровадити у центри моніторингу кібербезпеки військових інформаційних систем для формування попередження за 2-3 дні про можливі переходи інформаційної системи до критичних станів, що дозволить швидко реагувати на кіберзагрози. Удосконалений метод кластеризації

загроз та уразливостей сприяє автоматизації обробки та аналізу великих масивів даних у режимі реального часу, що дозволяє підвищити точність визначення режимів функціонування системи у 2 рази для об'єктивної оцінки рівня загроз. Запропонований метод підтримки прийняття рішень дозволяє зменшити кількість хибних спрацювань системи на 62% та підвищити ефективність реагування на кіберінциденти у системах управління інформаційною безпекою військових інформаційних систем.

Результати досліджень прийняті до впровадження в діяльність Київського столичного університету імені Бориса Грінченка (акт від 09.12.2025 року), Інституту програмних систем Національної академії наук України (акт від 09.12.2025 року), військової частини А2393 (довідка від 05.02.2026.) та Військового інституту телекомунікацій та інформатизації імені Героїв Крут (22.03.2026).

Апробація результатів дисертації. Основні теоретичні та практичні результати були представлені та обговорені на наукових конференціях:

1. XI Всеукраїнська науково-практична конференція молодих учених «Інформаційні технології – 2024», 2024 (м. Київ).
2. II Міжнародна науково-практична конференція «Сучасні аспекти діджиталізації та інформатизації в програмній та комп'ютерній інженерії», 2024 (м. Київ).
3. XIII Міжнародна конференція «ITSec»-2024 Безпека інформаційних технологій, 2024 (м. Львів).
4. XII Всеукраїнської науково-практична конференціія молодих учених, 2025 (м. Київ).
5. Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS'II), 2025 (м. Київ).

Публікації. Основні результати дисертації висвітлено у 8 наукових публікаціях, із них усіх у співавторстві: 6 статті (з них 3 у співавторстві) у наукових виданнях, включених на дату опублікування до переліку наукових фахових видань України; 2 статті (з них усі у співавторстві) у періодичних наукових виданнях,

проіндексованих в наукометричних базах даних Scopus і Web of Science Core Collection. Наукові результати дисертації повною мірою висвітлено у наукових публікаціях.

Особистий внесок здобувача. Дисертація є самостійною науковою працею, в якій висвітлено власні ідеї і розробки автора, що дозволили вирішити поставлені завдання. Робота містить теоретичні та методичні положення і висновки, сформульовані здобувачем особисто. Використані в дисертації ідеї чи положення інших авторів мають відповідні посилання і використані лише для підкріплення ідей здобувача.

У статті «The Integration of Catastrophe Theory into Decision-Making Models for Information Security Management Systems» опублікованій у співавторстві, внесок Негоденко В.П. полягає у розробці алгоритму реагування системи прийняття рішень на основі теорії катастроф та визначенні сценаріїв для симуляції з різними параметрами за допомогою Python, що загалом складає 70% тексту статті.

У статті «Математичні методи в кібербезпеці: кластерний аналіз та його застосування в інформаційній та кібернетичній безпеці» опублікованій у співавторстві, внесок Негоденко В.П. полягає в проведенні аналізу і описі етапів задачі кластеризації, вибору міри відстані та міри подібності для об’єктів, які вивчаються, що загалом складає 40% тексту статті.

У статті «Дослідження прикладних аспектів теорії конфліктів у системах безпеки» опублікованій у співавторстві, внесок Негоденко В.П. полягає в проведені аналізу щодо застосування теорії конфліктів для моделювання процесів протидії загрозам у системах безпеки, підготовці висновків щодо використання практичних результатів дослідження, що загалом складає 40% тексту статті.

У статті «Modified delta maintainability model of object-oriented software» опублікованій у співавторстві, внесок Негоденко В.П. полягає в проведенні практичної валідації модифікованої дельта-моделі шляхом аналізу програмних продуктів з відкритим вихідним кодом, що загалом складає 30% тексту статті.

У статті «Research of Information Conflict between Humans and Artificial Intelligence in Information and Cybernetic Systems» опублікованій у співавторстві, внесок Негоденко В.П. полягає в дослідженні проблеми впровадження штучного інтелекту в системах безпеки, встановлені ключових відмінностей між оборонним, наступальним та спрямованим га протидію ШІ в кібербезпеці, що загалом складає 30% тексту статті.

Структура та обсяг дисертаційної роботи. Дисертація складається зі вступу, чотирьох розділів, висновків, списку використаних джерел із 189 найменувань на 21 сторінці і 7 додатків. Загальний обсяг роботи становить 239 сторінок, серед яких 184 сторінок – основного тексту, 34 рисунків і 22 таблиць.

РОЗДІЛ 1. АНАЛІЗ СТАНУ КІБЕРБЕЗПЕКИ ВІЙСЬКОВИХ ІНФОРМАЦІЙНИХ СИСТЕМ В УМОВАХ КІБЕРКОНФЛІКТІВ

1.1. Військові інформаційні системи як об’єкти кіберзахисту

1.1.1. Структура та функціональні особливості військових інформаційних систем

Структура та функціональні особливості військових інформаційних систем суттєво відрізняються від звичайних (цивільних) інформаційних систем як за архітектурною логікою побудови, так і за цільовим призначенням, вимогами до надійності, безпеки та часових характеристик. Ці відмінності зумовлені специфікою середовища функціонування: якщо цивільні системи підтримують бізнес-процеси або адміністративне управління, то військові системи забезпечують управління військами в умовах активної протидії противника. Звичайні інформаційні системи, як правило, будуються на основі корпоративних архітектурних підходів (Enterprise Architecture), орієнтованих на підтримку бізнес-процесів організації. Їх структура зазвичай має трирівневу логіку – рівень представлення, прикладний рівень і рівень даних – із використанням централізованих або хмарних моделей розгортання. Інтеграція здійснюється переважно на інформаційному рівні: системи взаємодіють через стандартизовані інтерфейси, API та сервісні шини даних. Архітектура таких систем гнучка, допускає ітеративну модернізацію та оптимізується відповідно до змін бізнес-вимог. Натомість військові інформаційні системи формуються відповідно до концепції C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance) та пов’язаних архітектурних фреймворків, таких як DoDAF або NAF [5], [6].

У сучасних умовах цифровізації сектору безпеки й оборони військові інформаційні системи (ВІС) розглядаються як складні багаторівневі організаційно-технічні комплекси, що забезпечують підтримку процесів управління військами та

застосування сил в умовах динамічного оперативного середовища. Такі системи формуються на засадах системного підходу та поєднують інформаційні ресурси, програмно-технічні засоби, телекомунікаційну інфраструктуру та суб'єктів управління в єдиному інформаційному просторі. ВІС мають ієрархічну побудову та забезпечують взаємодію стратегічного, оперативного й тактичного рівнів управління. Ієрархічність, в свою чергу, поєднується з розподіленістю, що дозволяє системі функціонувати навіть за часткової втрати окремих елементів.

Відповідно до [7] багаторівнева структура військових інформаційних систем охоплює: організаційний компонент, що є суб'єктом управління, пунктом прийняття рішень та регламентними процедурами; інформаційний компонент, а саме бази даних, інформаційні потоки, засоби накопичення та актуалізації даних; функціональний компонент, що охоплює підсистеми збору, оброблення, аналізу та доведення інформації; технічний компонент, а саме, апаратно-програмні комплекси, мережеву інфраструктуру, засоби зв'язку.

Функціонування військових інформаційних систем охоплює повний цикл управління: від збору первинної інформації до формування управлінських рішень та контролю їх виконання. При цьому влючає основні характеристики, такі як безперервність інформаційних процесів, оперативність оброблення даних, синхронізація інформаційних потоків, інтеграція з системами зв'язку та розвідки.

Окремо варто зазначити здатність військових інформаційних систем функціонувати в умовах активної протидії, що зумовлює підвищені вимоги до живучості, резервування та адаптивності.

У роботі [6] розглядається еволюція архітектурного підходу до побудови систем C4ISR як відповідь на зростаючу складність військових інформаційних середовищ. Ключовою ідеєю є те, що ефективність військових інформаційних систем визначається не стільки окремими технічними рішеннями, скільки узгодженістю їх архітектурної організації. Таким чином, структура ВІС повинна формуватися на основі системної інтеграції операційних потреб, технічних засобів і стандартизованих механізмів взаємодії. Одним із центральних положень є

розуміння архітектури як інструменту подолання фрагментарності військових інформаційних ресурсів. Оскільки історично розвиток військових інформаційних систем відбувався у відомчо-орієнтованому режимі, це призводило до створення ізольованих рішень із обмеженою сумісністю. Основна ідея C4ISR Architecture Framework полягає в тому, що структура великих військових інформаційних систем повинна бути описана не як набір ізольованих компонентів, а як єдина інтегрована архітектура, яка забезпечує визначення ключових бізнес-процесів та функцій, взаємодію між різними підсистемами, стандартизовані правила та формати обміну даними та інтеграцію на рівні процесів, даних, інтерфейсів і технологій.

Такий підхід відповідає сучасним вимогам до військових ІС, що функціонують у складних організаційних та оперативних контекстах, де інформація стає стратегічним ресурсом, а ефективна інтеграція даних і функцій впливає на якість управлінських рішень. Виокремлюють три взаємопов'язані «види» архітектурного опису (views):

– операційний вид (Operational View) – фокусується на діяльностях, інформаційних потоках, логіці виконання завдань у рамках певної місії; у контексті ВІС цей рівень визначає структуру функціональних можливостей системи, що відповідають за підтримку управлінських циклів, він задає основу для розуміння, які саме функції і як будуть виконуватися у ВІС.

– системний вид (Systems View) – перетворює потреби операційного рівня в конкретні системні компоненти, їх взаємозв'язки та характеристики; у контексті ВІС це дозволяє побудувати логічну карту компонентів військової ІС (сервери, мережі, модулі, підсистеми), які реалізують функції Operational View;

– технічний вид (Technical View) – описує стандарти, правила та обмеження, які гарантують інтероперабельність, масштабованість і взаємозамінність компонентів; у контексті ВІС це забезпечує структурно-функціональні вимоги до апаратно-програмних засобів, комунікаційних інтерфейсів і протоколів.

Таке тривимірне розділення дозволяє чітко простежити зв'язок між функціональними вимогами та технічними реалізаціями у будь-якій ВІС, що

особливо важливо для управління складними військовими операціями. Архітектурні продукти в такій архітектурі виступають ключовим посередником між управлінськими вимогами і технічними реалізаціями, дозволяючи розробникам і командуванню бачити, як саме побудована система задовольняє операційні потреби. Ці продукти виконують такі ролі:

– забезпечують узгодженість між різними рівнями опису архітектури;

– визначають структури даних, функціональні зв’язки, технологічні взаємодії;

– слугують інструментом для аудиту та оцінки ефективності структурних рішень.

Забезпечення інтероперабельності між окремими системами, платформами та компонентами досягається через стандартизовані моделі даних, погоджені формати обміну та узгоджені технічні стандарти. Це відповідає вимозі до ВІС бути не просто набором окремих інформаційних підсистем, а єдиним організованим комплексом, здатним взаємодіяти з іншими системами (наприклад, союзницькими, коаліційними або цивільними ІС). Такий принцип є визначальним для сучасних багатонаціональних операцій, де ефективність системного функціонування забезпечується саме через сумісність та інтеграцію.

Оскільки сучасні військові інформаційні системи функціонують у динамічному середовищі кібернетичних загроз і повинні бути здатні реагувати на нові виклики без втрати операційної ефективності, архітектура ВІС повинна бути не статичною, а еволюційною, тобто адаптуватись до зміни вимог, технологій та оперативних умов. Це означає, що структура системи повинна бути побудована так, щоб додавати або оновлювати функціональні модулі без перебудови всієї системи, інтегрувати нові технології та адаптуватись до нових типів загроз та викликів.

ВІС може розглядатись не як ізольована технічна сукупність, а як частина складної соціотехнічної системи управління інформацією, яка еволюціонує під впливом технологічних, організаційних і культурних чинників. З одного боку, базові архітектурні фреймворки (TOGAF, DODAF, NAF) формально

відокремлюють інформаційну складову між бізнес-процесами та технологіями, однак у практиці побудови систем C4ISR та ERP (Enterprise Resource Management) фокус зміщується до технологій, а не до моделювання інформаційних потоків і структур інформаційного управління. В контексті розгляду інформаційного менеджменту як структурного шару системи, а не як допоміжної функції, структура військової інформаційної системи повинна включати архітектуру даних, механізми управління життєвим циклом інформації, правила відповідальності за дані, стандарти метаданих та процедури забезпечення якості інформації.

Еволюційна модель інформаційного менеджменту включає шість стадій розвитку інформаційного управління.

1. Paper-based environment – паперові документи, ізольовані процеси.
2. Digital documents – електронні копії паперової логіки.
3. Shared drives/repositories – спільний доступ, але без семантичної узгодженості.
4. Structured information systems – централізовані бази даних.
5. Integrated enterprise architecture – інтеграція процесів, даних і систем.
6. Intelligent content / knowledge-centric environment – семантична обробка, підтримка прийняття рішень.

Ця модель дозволяє оцінювати рівень зрілості структури військової ІС, визначати, чи відповідає архітектура системи сучасним операційним вимогам, а також формалізувати критерії переходу від розподілених сховищ до інтегрованої архітектури даних.

Така модель може бути використана як індикатор структурної готовності ВІС до кіберконфліктів: системи 1–3 рівнів є фрагментарними та вразливими до порушення цілісності інформації.

Значущою структурною особливістю військових систем є їх мережецентричний характер. Вони інтегрують не лише інформаційні ресурси, а й фізичні бойові компоненти: засоби розвідки, спостереження, радіолокаційні комплекси, безпілотні платформи, системи управління вогнем та засоби зв’язку.

Отже, військова інформаційна система є кіберфізичною системою, в якій інформаційні потоки безпосередньо впливають на кінетичні засоби ураження.

В роботі [8] розглядається підхід до побудови мілітарних систем на основі підходу SoS (system-of-systems) – система із систем: «набір систем або системних елементів, які взаємодіють, щоб забезпечити унікальну можливість, яку жодна зі складових систем не може реалізувати самостійно» [9]. В контексті підходу «Система із систем» військові інформаційні системи (Military SoS) не виступають ізольованими окремими об'єктами, а складають комплекс взаємодіючих підсистем, кожна з яких здатна функціонувати самостійно, але має спільну місію та інтегровану архітектуру. Military SoS визначається як сукупність взаємодіючих підсистем, що мають операційну незалежність, керовану незалежність та емерджентні властивості, що забезпечують цілісне функціонування в контексті військового управління. Це означає, що кожна підсистема може окремо виконувати певні функції (наприклад, сенсори, комунікаційні мережі, командні центри), але в інтеграції вони утворюють єдину інформаційно-аналітичну архітектуру військової системи. В якості ключових структурних ознак Military SoS визначаються наступні:

– незалежність підсистем – кожна підсистема (модуль) здатна працювати автономно, але входить до більш широкої архітектури, що визначає її взаємодію із іншими;

– цілісність та зв'язність – система характеризується чітко визначеними взаємозв'язками між підсистемами, що дає змогу координувати їхню роботу в режимах прийняття рішень, командування та контролю;

– еволюційність структури – можливість адаптації архітектури відповідно до змін у бойовому середовищі та умовах інформаційної взаємодії, це одна з головних функціональних особливостей, що забезпечує гнучкість і масштабованість військових інформаційних систем.

Зважаючи на вищезазначене, інформаційна безпека у військових системах також має системоутворюючий характер. Якщо в цивільних ІС реалізується класична модель конфіденційності, цілісності та доступності, то у військових

системах застосовуються багаторівневі моделі доступу, криптографія військового рівня, сегментація мереж із фізично ізольованими контурами, а також механізми протидії кібероперація̆м. Безпека інтегрується в архітектуру з самого початку, а не додається як окремий функціональний модуль.

1.1.2. Вимоги до кіберстійкості військових інформаційних систем

Однією з базових вимог будь-якої інформаційної системи, зокрема, військової, є гарантування забезпечення трьох ключових властивостей: конфіденційності, цілісності та доступності інформації (CIA) [10]. Дотримання цих властивостей становить фундамент кіберстійкості, бо саме вони спрямовують процес на розробку захисних механізмів, на формування вимог щодо здатності системи протистояти втручанням, несанкціонованому доступу та збереженню її працездатності навіть в умовах активних атак. Кіберстійкість військових інформаційних систем є однією з ключових вимог до сучасних систем управління військами, систем розвідки, зв’язку та бойових платформ. Вона визначає здатність ВІС підготуватися до кібератак, протистояти їм, відновлюватися та адаптуватися до несприятливих умов, стресів, атак або компрометацій, зберігаючи функціонування критичних місій [11].

Як комплексна властивість, кіберстійкість інформаційної системи включає здатність системи до передбачення загроз, до протидії та стійкості до атак, відновлення після інцидентів та адаптації до нових загроз. В контексті ВІС кіберстійкість забезпечує ефективне функціонування військових операцій у кіберпросторі, надійність систем управління військами та збереження боєздатності в умовах кіберконфліктів. Основні вимоги до кіберстійкості ВІС включають (рис.1.1) безперервність виконання військових місій, активний захист і виявлення кібератак, сегментацію та контроль інформаційних потоків, інтероперабельність між військовими системами, здатність до відновлення та адаптації, ситуаційну обізнаність у кіберпросторі та інтеграцію кіберзахисту у життєвий цикл систем.

Забезпечення безперервності виконання місії передбачає збереження здатності системи виконувати критично важливі функції навіть у разі успішних кібератак або технічних збоїв. У сучасних дослідженнях кіберстійкість розглядається не лише як запобігання інцидентам, а як здатність системи функціонувати в умовах ворожого кіберсередовища. Зокрема, у стандарті NIST SP 800-160 [11] кіберстійкість визначається як здатність системи передбачати, витримувати, відновлюватися та адаптуватися до несприятливих умов, атак або компрометації, що впливають на кіберресурси. У контексті військових інформаційних систем така властивість безпосередньо пов’язана з гарантуванням виконання місійних функцій навіть у випадку проникнення противника до інформаційної інфраструктури. Підхід кіберстійкості виходить з припущення, що складні системи можуть бути частково скомпрометовані, тому вони повинні бути здатними продовжувати виконання критичних завдань у деградованому режимі функціонування. Це означає, що навіть за умов втрати окремих компонентів або частини мережевої інфраструктури система має забезпечувати виконання ключових операцій, необхідних для управління військами та ведення бойових дій.

Для військових інформаційних систем забезпечення безперервності місії передбачає збереження працездатності основних функціональних підсистем. До них належать системи управління військами, засоби зв’язку та передачі розвідувальної інформації, а також інформаційні компоненти систем озброєння. Саме ці елементи забезпечують ситуаційну обізнаність, координацію підрозділів та ефективність бойових операцій. Втрата їх функціональності навіть на короткий час може призвести до значного зниження боєздатності. З інженерної точки зору, досягнення такої властивості потребує застосування комплексу архітектурних і технічних рішень. До них належать побудова відмовостійкої архітектури, використання механізмів резервування критичних компонентів, а також реалізація режимів частково деградованого функціонування, у яких система зберігає виконання найважливіших місійних функцій навіть у разі суттєвого зниження продуктивності або доступності ресурсів [11]. Такий підхід дозволяє зменшити

ризики зриву операцій і підтримувати стабільність військових систем управління у складному та конфліктному кіберсередовищі.

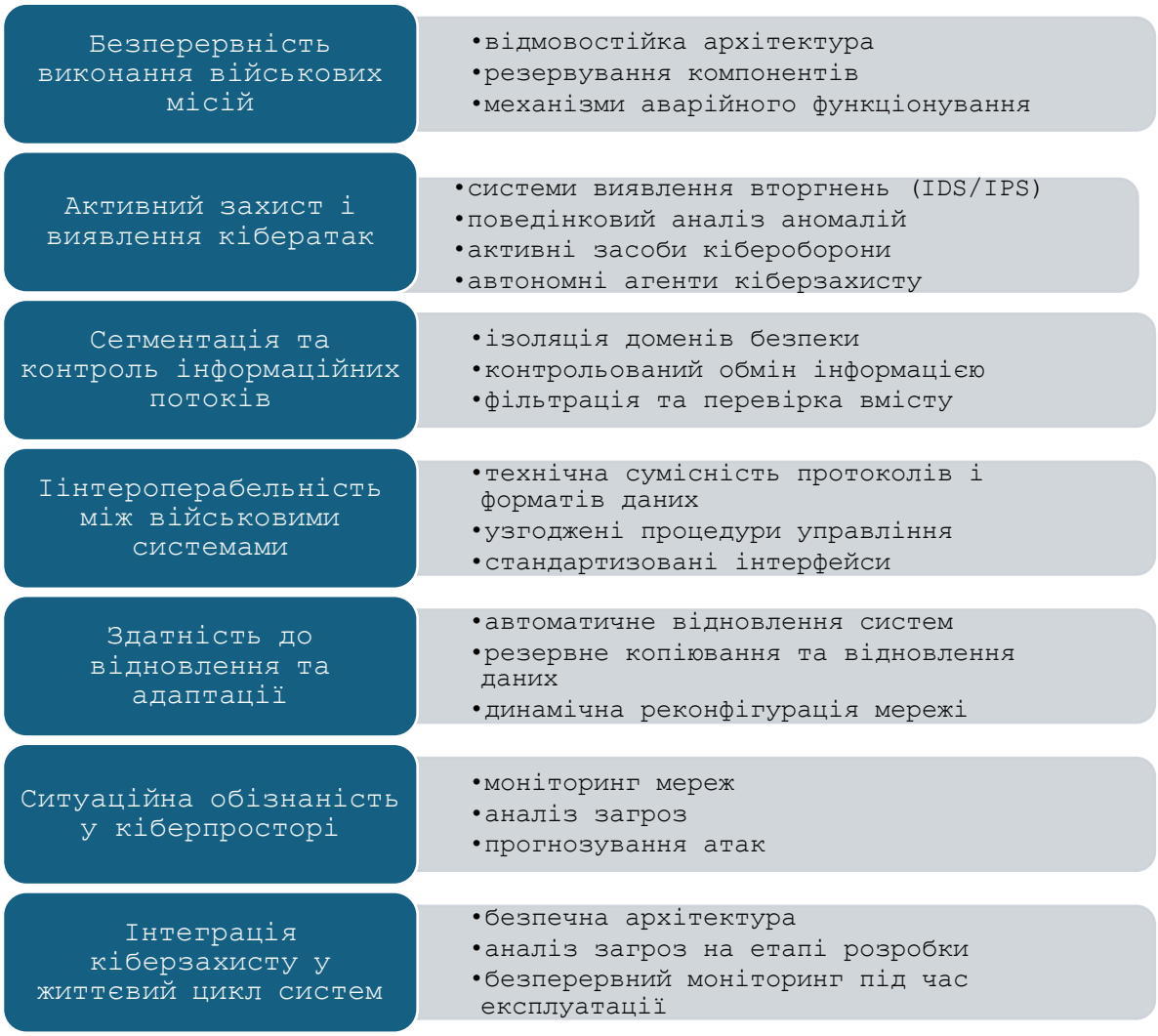


Рис. 1.1. Основні вимоги до кіберстійкості ВІС

Здатність ВІС протистояти кібератакам та своєчасно їх виявляти забезпечує підтримання функціонування систем навіть у середовищі активної протидії противника. У сучасних дослідженнях [12], [13], [14], [15] підкреслюється, що мережі військового призначення функціонують у складному та конфліктному кіберпросторі, де противник постійно намагається проникнути в інформаційну інфраструктуру, вплинути на системи управління, зв’язку та розвідки. Тому ефективний кіберзахист має передбачати не лише запобігання атакам, але й їх

оперативне виявлення та нейтралізацію в режимі реального часу. До основних технологічних засобів реалізації такої здатності належать системи виявлення та запобігання вторгненням (IDS/IPS), інструменти поведінкового аналізу мережевого трафіку та механізми виявлення аномалій, що дозволяють ідентифікувати шкідливу активність навіть у випадках, коли атака не відповідає відомим сигнатурам. Такі системи забезпечують автоматичне виявлення шкідливого програмного забезпечення, аналіз мережевих подій і формування попереджень про можливі інциденти інформаційної безпеки. У наукових дослідженнях НАТО також розглядається концепція активної та автономної кібероборони, що передбачає використання спеціалізованих програмних агентів, здатних самостійно виявляти шкідливу активність у військових мережах і здійснювати відповідні захисні дії. Зокрема, у роботі [16] пропонується архітектура Adaptive Autonomous Secure Cyber Systems (AASCS) – інтелектуального програмного агента, який може патрулювати мережу, аналізувати загрози та реагувати на дії шкідливого програмного забезпечення значно швидше, ніж це здатна зробити людина-оператор.

Військові інформаційні системи функціонують у середовищі з різними рівнями секретності та довіри, що зумовлює необхідність жорсткого контролю обміну інформацією між окремими доменами безпеки. У таких системах мережі зазвичай ізольовані відповідно до рівня класифікації інформації (наприклад, відкриті, службові, таємні), а передача даних між ними повинна здійснюватися лише за суворо визначеними правилами безпеки. Для реалізації цього підходу застосовуються спеціалізовані програмно-апаратні засоби, відомі як Cross-Domain Solutions (CDS). Згідно з визначенням стандартів інформаційної безпеки [16], CDS є контрольованим інтерфейсом, що забезпечує можливість автоматичного або ручного доступу до інформації та її передачі між різними доменами безпеки з дотриманням встановленої політики захисту даних. Основним призначенням таких систем є забезпечення безпечного обміну інформацією між мережами з різними рівнями довіри без ризику витоку секретних даних або проникнення шкідливого програмного забезпечення. Архітектура CDS базується на принципах ізоляції

доменів, контролю інформаційних потоків і багаторівневого аналізу даних. Зокрема, перед передачею інформації здійснюється перевірка її вмісту, фільтрація небезпечних або несанкціонованих даних та застосування політик безпеки, що визначають допустимі типи інформаційних обмінів. Такі механізми можуть включати використання апаратних односторонніх каналів передачі даних, спеціалізованих фільтрів і систем перевірки вмісту. Застосування рішень класу CDS дозволяє забезпечити контрольований обмін інформацією між різними мережами, підтримуючи водночас необхідний рівень захисту та збереження конфіденційності даних у військових інформаційних системах.

Оскільки сучасні військові операції дедалі частіше виконуються багатонаціональними коаліційними силами, інтероперабельність є важливою вимогою кіберстійкості ВІС. У таких умовах інформаційні системи різних держав повинні забезпечувати можливість ефективної взаємодії під час планування та проведення операцій. У документах НАТО інтероперабельність визначається як здатність різних сил, систем і організацій діяти разом узгоджено, ефективно та результативно для досягнення спільних цілей [17]. Досягнення інтероперабельності передбачає узгодження кількох взаємопов’язаних аспектів функціонування військових систем. Насамперед це технічна сумісність, яка забезпечує можливість обміну даними між різними інформаційними системами через стандартизовані протоколи, формати даних та комунікаційні інтерфейси. Важливим є також процедурний аспект, що охоплює узгодження доктрин, тактичних процедур і правил взаємодії між підрозділами різних держав. Крім того, значну роль відіграє людський фактор, пов’язаний із спільною підготовкою персоналу та використанням уніфікованої термінології і процедур управління. Практичним механізмом реалізації цих принципів є міжнародні програми стандартизації обміну даними. Однією з таких ініціатив є Multilateral Interoperability Programme (MIP) [18], спрямована на розроблення стандартів інформаційної взаємодії для систем управління військами (Command and Control). Використання таких стандартів забезпечує узгоджений обмін оперативною

інформацією між національними системами управління та сприяє підвищенню ефективності коаліційних військових операцій.

ВІС повинні не лише протистояти атакам, а й швидко відновлювати функціонування після інцидентів. На відміну від традиційних підходів до інформаційної безпеки, що зосереджені переважно на запобіганні інцидентам, концепція кіберстійкості передбачає можливість функціонування систем навіть у разі часткової компрометації або порушення їх роботи. У ВІС це означає, що після кібератаки або технічного збою система повинна швидко повернутися до штатного або принаймні до частково функціонального стану. Для цього використовуються механізми резервування та відновлення даних, автоматизовані процедури відновлення сервісів, а також засоби динамічної реконфігурації мережевої інфраструктури. Такий підхід дозволяє зменшити час простою систем і підтримувати виконання критично важливих функцій. В свою чергу, динамічна адаптація системи до нових загроз передбачає зміну конфігурації мережі, оновлення політик безпеки та використання інтелектуальних механізмів аналізу інцидентів. Це дозволяє військовим інформаційним системам не лише відновлюватися після атак, а й підвищувати власну стійкість до подібних загроз у майбутньому [19].

Ефективне функціонування військової інформаційної інфраструктури значною мірою залежить від здатності своєчасно виявляти загрози, оцінювати поточний стан мереж і прогнозувати можливі атаки. В [20] кіберситуаційна обізнаність розглядається як процес збирання, аналізу та інтерпретації інформації про стан кіберсередовища з метою підтримки прийняття рішень у сфері кібероборони. Реалізація такого підходу передбачає постійний моніторинг мережевої інфраструктури, аналіз журналів подій та мережевого трафіку, а також використання аналітичних інструментів для виявлення потенційних загроз. Застосування методів інтелектуального аналізу даних і кореляції подій дозволяє ідентифікувати складні багатоступеневі атаки та оцінювати їх можливі наслідки, а системи кіберситуаційної обізнаності можуть використовувати прогностичні

моделі для виявлення тенденцій розвитку загроз і прогнозування майбутніх атак. У документах НАТО підкреслюється, що високий рівень ситуаційної обізнаності щодо кіберзагроз є необхідною передумовою ефективного реагування на інциденти та підтримання стійкості військових інформаційних систем у складному та динамічному кіберсередовищі.

Кіберстійкість повинна закладатися на етапі проєктування систем, а не лише під час їх експлуатації. У стандартах NIST підкреслюється, що кіберстійкі системи повинні створюватися відповідно до принципу secure-by-design, який передбачає формування безпечної архітектури, проведення аналізу загроз і оцінювання ризиків на етапі розробки, а також інтеграцію механізмів моніторингу та реагування протягом усього періоду експлуатації системи [11]. Реалізація такого підходу передбачає застосування методів моделювання загроз, регулярне оновлення політик безпеки та безперервний контроль стану інформаційної інфраструктури.

Таким чином, функціонування військових інформаційних систем в умовах активної дії кіберінцидентів, вимагає більшої уваги до кіберстійкості системи та здатності працювати в умовах постійної зміни станів системи. Тому актуальним постає питання розробки комплексних підходів до забезпечення кібербезпеки, які враховують динамічний характер кіберзагроз.

1.2. Кіберзагрози, уразливості та кіберінциденти у військових інформаційних системах

Функціонування ВІС у сучасному кіберпросторі супроводжується значною кількістю кіберзагроз, уразливостей та потенційних кіберінцидентів, що можуть істотно впливати на стабільність їх роботи та здатність забезпечувати виконання бойових і управлінських завдань. Складність архітектури таких систем, їх інтеграція з різноманітними мережевими сервісами та використання у критично важливих процесах управління військами підвищують вимоги до забезпечення інформаційної та кібернетичної безпеки. Для ефективного забезпечення їх кіберстійкості необхідним є системний аналіз джерел кіберзагроз, характерних

уразливостей та специфіки кіберінцидентів у військовому середовищі. У цьому пункті розглядаються класифікація кіберзагроз і уразливостей, а також особливості кіберінцидентів у військових інформаційних системах.

1.2.1. Класифікація кіберзагроз та уразливостей військових інформаційних систем

Класифікація кіберзагроз та уразливостей ВІС у сучасних умовах охоплює технічні, операційні та людські аспекти, що поділяються за рівнями впливу та сферами застосування (рис.1.2).

Рис.1.2. Класифікація кіберзагроз ВІС

Глушіння сигналу є однією з найпоширеніших загроз для військових комунікаційних систем тактичного рівня [21]. Атака полягає у створенні потужних радіочастотних перешкод, які перекривають робочий сигнал каналів зв'язку або навігації. У результаті підрозділи можуть втратити доступ до систем управління, передачі телеметрії або навігаційних сигналів, що суттєво знижує ситуаційну обізнаність і може призвести до втрати координації між елементами бойових систем [22]. Подібні атаки також часто застосовуються проти безпілотних платформ та тактичних мереж передачі даних.

Спуфінг полягає у навмисному підробленні або підміні інформаційних сигналів з метою введення системи чи оператора в оману. У військових інформаційних системах це може включати підробку навігаційних сигналів (наприклад GPS), ідентифікаційних повідомлень або телеметрії. У результаті системи можуть приймати неправдиві координати, команди або дані про стан об’єктів. У складних мережах управління така атака може призвести до виконання помилкових наказів або втрати контролю над окремими компонентами системи [23].

Викрадення даних є стратегічною кіберзагрозою, спрямованою на несанкціонований доступ до конфіденційної інформації військових систем. Основною метою таких атак є отримання розвідувальних даних, планів операцій, технічної документації або інформації про структуру військових мереж [24]. Подібні атаки часто виконуються в рамках кіберрозвідувальних кампаній та можуть здійснюватися через експлуатацію вразливостей, внутрішні загрози або складні багаторівневі атаки.

Шкідливе програмне забезпечення використовується для проникнення у військові мережі, отримання віддаленого контролю над системами або тривалого прихованого спостереження. Такі програми можуть виконувати функції шпигунства, саботажу або знищення даних. Складні зразки malware, такі як інструменти кіберрозвідки або модульні платформи атак, здатні збирати інформацію, перехоплювати комунікації та передавати їх на сервери управління зловмисника [25].

Фішинг є різновидом атак соціальної інженерії, спрямованих на отримання доступу до захищених систем через обман користувачів. У військовому середовищі такі атаки можуть реалізовуватися у вигляді підроблених електронних листів, веб-ресурсів або службових повідомлень, що імітують офіційні комунікації. Метою є отримання облікових даних, встановлення шкідливого програмного забезпечення або проникнення у внутрішні мережі організації [26]. Фішингові атаки часто

використовуються як початковий етап складних кібероперацій проти державних і військових структур.

Уразливості ВІС обумовлені технічними недоліками архітектури та специфікою використання ресурсів:

застаріла інфраструктура;

відсутність єдиних стандартів;

інтероперабельність;

залежність від цивільної інфраструктури.

Схема на рис.1.3 описує уразливості безпеки та вектори атак, пов'язані з компонентами командування, управління, зв'язку та розвідки системи С3І.

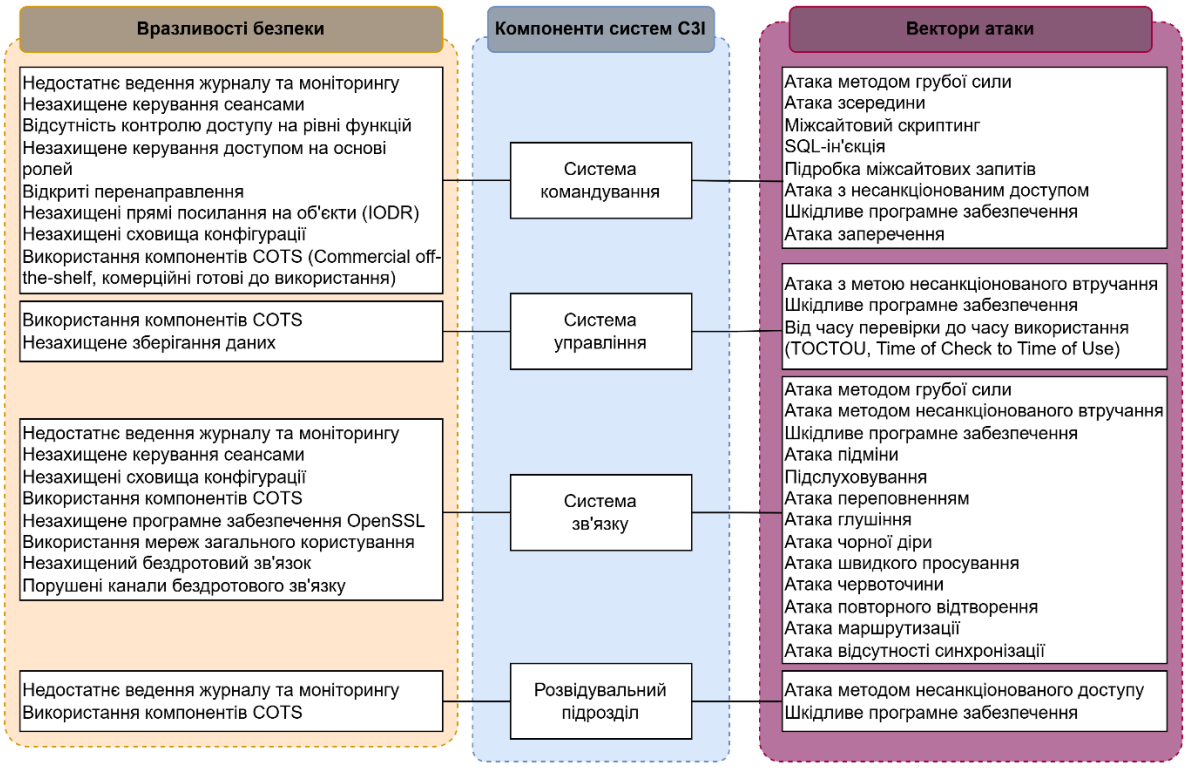


Рис.1.3. Уразливості безпеки та вектори атак, пов'язані з компонентами командування, управління, зв'язку та розвідки системи С3І. Джерело [27].

Сучасні військові операції значною мірою залежать від інформаційно-комунікаційних систем управління, розвідки, навігації та логістики, що робить такі системи критичними цілями для кібероперацій противника. Дослідження

показують, що збільшення залежності військових місій від інформаційних технологій одночасно підвищує і рівень потенційних кіберризиків для бойових операцій [28].

Використання систем, розроблених десятиліття тому, які не пристосовані до сучасних кіберзагроз, є критичною уразливістю для всіх видів транспорту та зв'язку [24], [29]. Значна частина військових систем управління, зв’язку та авіоніки була розроблена тоді, коли кібербезпека не розглядалася як критичний елемент архітектури. Наприклад, стандарт обміну даними MIL-STD-1553, який використовується в авіаційних та космічних платформах понад сорок років, був створений з акцентом на відмовостійкість, а не на захист від кіберзагроз, що створює потенційні можливості для атак на комунікаційні шини та бортові системи [30]. Додатковою проблемою є те, що модернізація таких систем часто ускладнена через апаратні обмеження або відсутність підтримки з боку виробників. Це унеможливлює регулярне встановлення оновлень безпеки та інтеграцію сучасних засобів виявлення атак.

Недостатня уніфікація стандартів кібербезпеки у різних сегментах військової інформаційної інфраструктури створює уразливість у захисті, яка може бути використана противником для проникнення у мережу або перехоплення даних за рахунок того, що системи зв’язку можуть використовувати різні протоколи та криптографічні механізми залежно від типу каналу – наприклад, радіолінії, IP-мережі або супутникові мережі. [31]. Зростаюча залежність військових операцій від супутникових систем і мереж зв’язку робить критично важливим створення узгоджених стандартів кібербезпеки для різних технологічних платформ.

Військові операції, особливо у багатонаціональних коаліціях, передбачають інтеграцію інформаційних систем різних держав, родів військ та типів платформ. Така інтеграція забезпечує обмін даними у реальному часі між системами командування, розвідки та управління. Проте різниця у технічних стандартах, форматах даних та рівнях захисту може значно збільшувати поверхню атаки. Інтеграція систем різних держав у межах спільних операцій вимагає створення

спеціальних архітектур мережевої взаємодії, інакше різниця у протоколах та механізмах безпеки може призводити до появи додаткових кіберуразливостей [32], [29].

Багато військових інформаційних систем частково або повністю покладаються на цивільну інфраструктуру, зокрема комерційні супутникові мережі, логістичні системи, транспортні вузли та телекомунікаційні мережі. Така інтеграція підвищує ефективність військових операцій, але одночасно переносить на військові системи уразливості цивільних технологій. Дослідження кіберризиків для військових систем управління та зв'язку підкреслюють, що використання комерційних компонентів і технологій може створювати додаткові точки проникнення для атак, особливо у глобальних ланцюгах постачання інформаційних систем [33]. Використання комерційних технологій та постачальників у військових системах може призводити до появи нових кіберризиків, пов'язаних із недостатнім контролем над ланцюгами постачання та різним рівнем безпеки компонентів.

Людина залишається найслабшою ланкою в ланцюгу кіберзахисту. Уразливості в цій сфері включають:

когнітивну війну – використання кіберзасобів для впливу на сприйняття, емоції та поведінку людей; сюди відносять маніпуляцію інформацією, дезінформацію та пропаганду, що використовують «упередження істини» (truth bias) [34]

соціальну інженерію – психологічне маніпулювання персоналом для отримання доступу до систем, що часто є ефективнішим за пошук технічних помилок у коді [35].

Еволюція інформаційних технологій, зростання обчислювальних потужностей та інтеграція штучного інтелекту у різні сфери діяльності призводять до суттєвої трансформації кіберзагроз ВІС. Сучасні атаки характеризуються високим рівнем автоматизації, використанням складних ланцюгів компрометації та активним застосуванням комерційних сервісів кіберзлочинності. У результаті кібероперації стають більш масштабними, швидкими та складними для виявлення

і протидії. Аналіз сучасних кіберконфліктів показує, що нові моделі атак дедалі частіше поєднують технічні засоби з інструментами інформаційного впливу та автоматизованої обробки даних [36]. Однією з найважливіших сучасних тенденцій розвитку кіберзагроз є використання штучного інтелекту для автоматизації та масштабування атак. Алгоритми машинного навчання можуть застосовуватися для швидкого аналізу великих обсягів даних, пошуку уразливостей у програмному забезпеченні, генерації фішингових повідомлень та адаптивного шкідливого коду. Крім того, технології генеративних нейронних мереж дають змогу створювати діпфейки – синтетичні аудіо- та відеоматеріали, які можуть використовуватися для інформаційних операцій, дезінформації або соціальної інженерії.

Атаки на ланцюги постачання програмного забезпечення є однією з найбільш небезпечних сучасних кіберзагроз. У таких атаках зловмисники компрометують програмне забезпечення або його компоненти ще на етапі розробки чи розповсюдження, після чого шкідливий код потрапляє до систем користувачів разом із легітимними оновленнями. Це дозволяє одночасно вражати велику кількість організацій та критичних систем. Подібні атаки отримали широке поширення після масштабних інцидентів із компрометацією програмного забезпечення для управління IT-інфраструктурою [37]. Компрометація постачальників програмного забезпечення або апаратних компонентів може призвести до системних ризиків для великої кількості кінцевих споживачів, оскільки шкідливі зміни розповсюджуються разом із легітимними продуктами.

Ще однією важливою тенденцією трансформації кіберзагроз є формування кримінальної моделі Ransomware-as-a-Service (RaaS). У межах цієї моделі розробники шкідливого програмного забезпечення створюють інструменти для атак типу ransomware та надають їх іншим зловмисникам за певну плату або частку від отриманого викупу [38]. Такий підхід значно знижує технічний бар’єр входу у кіберзлочинну діяльність і дозволяє здійснювати атаки ні ВІС навіть особам без глибоких технічних знань.

Реалістичне оцінювання ризиків у таких системах потребує аналізу імовірності та можливих негативних наслідків від порушення основних властивостей безпеки.

1.2.2. Особливості кіберінцидентів у військових інформаційних системах

Особливості кіберінцидентів у ВІС визначаються їхньою державною приналежністю, стратегічним характером наслідків та тісною інтеграцією з конвенційними бойовими діями [35]. Кіберінциденти у військовій сфері можуть класифікуватися залежно від оперативного рівня застосування та масштабу їх впливу на виконання військових місій. Такий підхід базується на загальноприйнятій у військовій науці трирівневій моделі управління – тактичному, оперативному та стратегічному рівнях, яка використовується також при аналізі кібероперацій і кіберрозвідки. Різні рівні характеризуються відмінними цілями атак, часовими горизонтами та масштабом впливу на військові системи управління, зв’язку та інформаційні ресурси [27]. Залежність сучасних військових операцій від інформаційно-комунікаційних систем (CIS) та систем командування, управління, зв’язку й розвідки (C3I) призводить до того, що кіберінциденти можуть безпосередньо впливати на успішність виконання бойових завдань, порушуючи функціонування комунікацій, обробку інформації або управління військами [28]. З огляду на характер впливу на військові системи, кіберінциденти доцільно розглядати у межах трьох основних рівнів.

Кіберінциденти тактичного рівня пов’язані з безпосереднім впливом на конкретні системи або підрозділи, що беруть участь у виконанні бойового завдання. До таких інцидентів належать атаки на локальні мережі підрозділів, системи зв’язку на полі бою, сенсорні системи, безпілотні платформи або системи управління озброєнням. Основною метою подібних атак є порушення доступності або достовірності інформації, що використовується у реальному часі під час бойових дій. Це може включати перехоплення або блокування передачі даних, підміну інформації про розташування сил, компрометацію навігаційних систем або

зараження окремих пристроїв шкідливим програмним забезпеченням. Навіть локальний інцидент такого типу може призвести до втрати ситуаційної обізнаності підрозділу або помилкових рішень на полі бою [27].

Кіберінциденти оперативного рівня охоплюють цілі військові кампанії, угруповання військ або великі сегменти військової інформаційної інфраструктури. Такі атаки зазвичай спрямовані на системи управління операціями, мережі обміну розвідувальною інформацією, логістичні системи або інформаційні платформи планування бойових дій. На цьому рівні кібероперації можуть використовуватися для координації багаторівневих атак, що поєднують проникнення у мережу, тривале приховане перебування в інфраструктурі та поступове порушення функціонування критичних сервісів. Наприклад, компрометація систем управління логістикою або систем обміну розвідувальною інформацією може суттєво вплинути на здатність військ планувати та проводити операції. Дослідження показують, що подібні кіберінциденти здатні змінювати перебіг військових кампаній через порушення інформаційної переваги або координації сил [28].

Кіберінциденти стратегічного рівня спрямовані на критичну інфраструктуру держави або ключові елементи національної системи оборони. До таких цілей можуть належати енергетичні системи, телекомунікаційні мережі, військові супутникові системи, оборонно-промисловий комплекс або національні інформаційні ресурси. Метою подібних атак є не лише безпосереднє порушення функціонування окремих систем, але й досягнення довгострокових стратегічних ефектів, таких як дестабілізація систем управління державою, порушення оборонного потенціалу або підрив довіри до інформаційної інфраструктури. Відомі приклади кібератак на критичну інфраструктуру демонструють, що цифрові операції можуть викликати навіть фізичні наслідки, включаючи пошкодження промислового обладнання або порушення функціонування важливих державних систем [39].

Окремо слід зазначити, що військові кіберінциденти під час повномасштабного вторгнення рф продемонстрували максимальну синхронізацію з кінетичними атаками [35]:

– придушення зв'язку – одночасно з початком вторгнення було здійснено атаку на мережеве обладнання Skylogic (супутник Ka-Sat), що призвело до тимчасової втрати управління підрозділами ЗСУ;

– деструктивне програмне забезпечення (Wipers) – використання програм типу WhisperGate та HermeticWiper, що не просто шифрують дані, а безповоротно знищують завантажувальні записи дисків військових та фінансових установ;

– гібридна розвідка – зараження Android-планшетів військових для перехоплення даних про пересування підрозділів та комунікації через Starlink.

Військові транспортні системи мають специфічну уразливість через залежність від цивільної інфраструктури [29]. Кіберінциденти в цій сфері можуть включати:

– маніпуляцію даними стабільності суден (перекидання кораблів через неправильні розрахунки навантаження);

– дистанційне відключення портових кранів (наприклад, через вразливості в китайських кранах ZPMC) [29];

– блокування залізничного руху шляхом шифрування серверів управління (інциденти в Білорусі та Румунії) [35].

Специфікою кіберінцидентів у ВІС є те, що вони характеризуються використанням складних методів проникнення та прихованої діяльності у мережах. На відміну від традиційних кіберзлочинних атак, операції проти військових систем зазвичай мають довготривалий характер, виконуються висококваліфікованими групами та спрямовані на досягнення стратегічних або оперативних цілей. Такі атаки часто реалізуються у вигляді Advanced Persistent Threat (APT)-кампаній, у яких зловмисники застосовують багаторівневі методи проникнення, тривале приховане перебування у мережі та поступове розширення контролю над

системами [40]. Сучасні ВІС включають мережі управління військами, системи зв’язку, сенсорні платформи та елементи критичної інфраструктури. Це створює складне інформаційне середовище, у якому противник може використовувати різні точки входу, включаючи користувачів, програмне забезпечення, апаратні компоненти та мережеві протоколи. Дослідження кіберзахисту військових систем показують, що ефективні атаки часто поєднують технічні експлойти, соціальну інженерію та маніпуляції з ланцюгами постачання програмного забезпечення [27].

Проведений аналіз основних типів кіберзагроз та уразливостей, які зафіксовані для військових інформаційних систем показав, що кіберінциденти мають тактичний, оперативний та стратегічний рівень впливу, а їх розвиток характеризуються складною динамікою та нелінійними процесами, що ускладнює їх аналіз та прогнозування наявними підходами. Тому необхідно розробити новий підхід для моделювання розвитку кіберзагроз у військових інформаційних системах, що враховує їх складну динаміку.

1.3. Системи управління інформаційною безпекою та SIEM

1.3.1. Архітектура та функції систем управління інформаційною безпекою

Архітектура та функції систем управління інформаційною безпекою (СУІБ) у військових системах класу С3І (командування, управління, зв'язок та розвідка) або C4ISR базуються на багатошаровому підході, що охоплює як етап розробки, так і фазу активної експлуатації. Згідно з фреймворком архітектури C4ISR [5], [6], СУІБ розглядається через три основні призми:

– операційне представлення (Operational View) – описує завдання, оперативні вузли та інформаційні потоки, необхідні для виконання місії, визначаючи вимоги до безпеки обміну даними;

– системне представлення (Systems View) – пов'язує фізичні ресурси (сервери, мережі) з оперативними потребами, впроваджуючи механізми захисту на рівні компонентів;

– технічне представлення (Technical View) – встановлює стандарти (наприклад, ISO/IEC 17799) та конвенції, що регулюють реалізацію захисних функцій.

Сучасна архітектура контролю цифрового суверенітету у військовій сфері включає наступні шари [41]:

– стратегічний шар – визначає політику, правові та етичні межі, забезпечуючи підзвітність та прозорість рішень;

– шар управління та запевнення – фокусується на моніторингу метрик, аудиті та безперервній перевірці дотримання доктрин безпеки;

– шар суверенітету даних та ШІ – забезпечує верифікований контроль над життєвим циклом даних та моделей штучного інтелекту, використовуючи федеративне навчання та криптографічний захист;

– шар кібероперацій та інфраструктури – включає контроль над фізичним обладнанням (мілітарні «хмари», довірене залізо) та безпосереднє виконання оборонних функцій (виявлення аномалій).

Функції управління безпекою поділяються на превентивні (на етапі розробки) та оперативні (під час місії). Етап розробки та проєктування включає [27]:

– аналіз вимог безпеки – використання цифрових сертифікатів, фаєрволів та методів розширення спектра для захисту від перехоплення;

– аналіз впливу атак – прогнозування наслідків кібератак на структуру системи та ефективність управління за допомогою математичного моделювання;

– моделювання загроз – ідентифікація уразливостей (наприклад, у COTS-компонентах або сесіях зв'язку) ще на рівні дизайну архітектури.

Оперативне управління включає:

– виявлення вторгнень – цілісний підхід, що містить чотири фази: виявлення, кореляція, візуалізація та реагування; ВІС використовують ШІ для аналізу журналів подій безпеки в реальному часі;

– криптографічний захист – управління ключами (генерація, розподіл, заміна) для захисту даних у русі та у стані спокою; сюди входить і стеганографія – приховування самого факту передачі інформації у цифрових контейнерах (зображеннях, аудіо) [22];

– контроль доступу – реалізація суворої ієрархії команд через механізми RBAC (рольове керування доступом) та багаторівневу безпеку (MLS), що обмежує доступ до секретної інформації залежно від прав користувача.

Архітектура SIEM-систем (Security Information and Event Management) являє собою комплексну платформу, яка поєднує можливості управління інформацією про безпеку (SIM) – збір та аналіз журналів, та управління подіями безпеки (SEM) – моніторинг і оповіщення в реальному часі [42], [43], [44]. Вона виступає як центральний вузол контролю, що об'єднує розрізнені засоби захисту в єдину систему для виявлення складних загроз. Основні компоненти та етапи роботи SIEM-систем включають:

1. Джерела даних та механізми збору подій. SIEM агрегує дані з широкого спектра джерел у всій інфраструктурі організації. Джерела даних включають мережеві екрани (firewalls), антивіруси, системи виявлення вторгнень (IDS/IPS), сервери, додатки, мережеві пристрої, кінцеві точки (ПК, віртуальні машини), бази даних, хмарні сервіси та зовнішні джерела розвідки загроз (threat intelligence). Механізми збору включають стандартні протоколи (наприклад, Syslog, які дозволяють віддалено пересилати журнали до центрального хабу); агенти (спеціалізоване ПЗ, встановлене безпосередньо на компонентах системи) – збирають збагачені дані, оптимізовані під конкретні типи пристроїв та вектори загроз; API та потоковий збір – використання програмних інтерфейсів для отримання даних з хмарних або веб-сервісів, а також механізми збору потоків трафіку (flow collection).

2. Централізоване зберігання журналів подій. Після збору дані передаються до єдиного сховища для подальшої обробки. На першому кроці вони проходять нормалізацію – перетворення «сирих» логів з різних форматів у єдиний стандартний вигляд, що необхідно для їхнього спільного аналізу. Для зберігання та ретенції сучасні SIEM використовують розподілені бази даних, механізми реплікації та суворі політики зберігання даних (data retention), які визначають термін життя логів. Для забезпечення цілісності для військових мереж пропонується використання Blockchain-enhanced SIEM, де хеші логів зберігаються в блокчейні для запобігання їх видаленню або модифікації зловмисниками чи інсайдерами [45].

3. Механізми кореляції подій. Кореляційний рушій є серцем системи; він зіставляє події з різних джерел для ідентифікації підозрілих патернів. SIEM пов'язує на перший погляд непов'язані події (наприклад, декілька невдалих входів і наступний нетиповий мережевий трафік), що дозволяє виявляти складні багатоетапні атаки, такі як APT (Advanced Persistent Threats). Методи кореляції включають правила, написані експертами, поведінкову аналітику, а також використання ШІ та машинного навчання для створення «базової лінії» нормальної активності та виявлення аномалій.

4. Модулі аналітики та візуалізації. Ці модулі перетворюють масиви даних у зрозумілу для фахівців інформацію. Візуалізація здійснюється з використанням інформаційних панелей з графіками, метриками завантаження ресурсів та картами активності для підвищення ситуаційної обізнаності в реальному часі. Аналітика поведінки (UEBA) включає аналіз дій користувачів та сутностей для виявлення внутрішніх загроз або скомпрометованих акаунтів. Функції розслідування реалізуються з використанням інструментів для автоматичної побудови часових графіків атак, візуального аналізу подій та пошуку першопричини інциденту.

5. Системи сповіщення та реагування. Компоненти, що забезпечують швидку реакцію на підтверджені загрози включають: автоматичну генерацію та надсилання сповіщень (наприклад, на e-mail) команді SOC при виявленні інциденту; засоби

інтеграції з системами оркестрації (SOAR) для автоматичного виконання захисних дій без участі людини (ізоляції уражених хостів, блокування шкідливих IP-адрес або карантину файлів).

1.3.2. Роль SIEM-систем у забезпеченні кібербезпеки військових інформаційних систем

Системи управління інформацією та подіями безпеки (Security Information and Event Management, SIEM) у сучасній сфері кібербезпеки застосовуються для збирання, узагальнення, кореляції та аналізу подій безпеки в IT-інфраструктурі. Зі зростанням складності цифрових загроз виникає потреба у більш розвинених рішеннях SIEM, здатних забезпечувати оперативне виявлення загроз, а також підтримувати механізми автоматизованого реагування і розширені аналітичні інструменти. Роль SIEM-систем у забезпеченні кібербезпеки військових інформаційних систем (зокрема класу С3І – командування, управління, зв'язок та розвідка) є критично важливою, оскільки вони виступають технічним ядром Операційних центрів безпеки (Security Operation Center, SOC) та забезпечують цілісну видимість загроз у режимі реального часу [43], [44].

SIEM у військовій сфері охоплює такі ключові аспекти:

1. Централізація та агрегація даних. Військові системи складаються з великої кількості гетерогенних компонентів: датчиків, БПЛА, серверів, мережевих пристроїв та терміналів супутникового зв'язку. SIEM агрегує журнали подій з усіх рівнів інфраструктури в єдине сховище, що дозволяє уникнути ізоляції даних та спрощує їх аналіз [27]. Отримані дані приводяться до єдиного формату, що необхідно для подальшої кореляції подій, які надходять від різних виробників обладнання та програмного забезпечення.

2. Виявлення складних атак та кореляція подій. Традиційні засоби захисту (антивіруси, фаєрволи) часто не здатні самостійно ідентифікувати багатоетапні атаки, такі як APT (Advanced Persistent Threats). SIEM зіставляє події з різних джерел (наприклад, підозрілий вхід у систему та нетиповий мережевий трафік),

ідентифікуючи складні вектори атак, які окремі інструменти сприймають як безпечні. Сучасні SIEM використовують машинне навчання для створення «базової лінії» нормальної поведінки користувачів та систем, що дозволяє автоматично виявляти аномалії, які можуть вказувати на компрометацію.

3. Забезпечення цілісності логів та криміналістичний аналіз. У військових мережах критично важливо, щоб записи про події не були видалені або змінені зловмисником чи інсайдером. Для посилення захисту військових мереж пропонується використання Blockchain-enhanced SIEM, де хеші логів зберігаються у децентралізованому реєстрі, що гарантує незмінність та верифікованість аудиторського сліду. SIEM також надає детальні дані для проведення розслідувань після інцидентів, дозволяючи відновити хронологію атаки та визначити її першопричину.

4. Ситуаційна обізнаність та швидке реагування. Для військових операцій час виявлення атаки є вирішальним фактором, оскільки затримка може призвести до провалу місії та загибелі людей. SIEM забезпечує безперервне спостереження за станом безпеки, миттєво сповіщаючи аналітиків про критичні інциденти. Інтеграція з системами оркестрації (SOAR) дозволяє SIEM автоматично виконувати дії з реагування, наприклад, ізолювати заражений хост або блокувати шкідливу IP-адресу без участі людини.

5. Відповідність стандартам. Військові ІС повинні відповідати суворим державним та міжнародним стандартам безпеки (наприклад, NIST SP 800-53, ISO 27001, стандарти DoD). SIEM автоматизує процес перевірки відповідності, створюючи звіти на основі реальних подій у мережі.

Потік даних від виявлення до реагування у військовій системі управління інформаційною безпекою може бути представлений послідовністю на рис. 1.4.

Метою першого етапу є своєчасне виявлення підозрілої або потенційно шкідливої активності в інформаційній системі. На етапі виявлення SIEM-система виконує кореляцію подій, що надходять із різних джерел, системи захисту кінцевих точок (EDR) аналізують поведінку пристроїв, а правила виявлення використовують

індикатори загроз із джерел розвідки кіберзагроз для ідентифікації підозрілої активності.

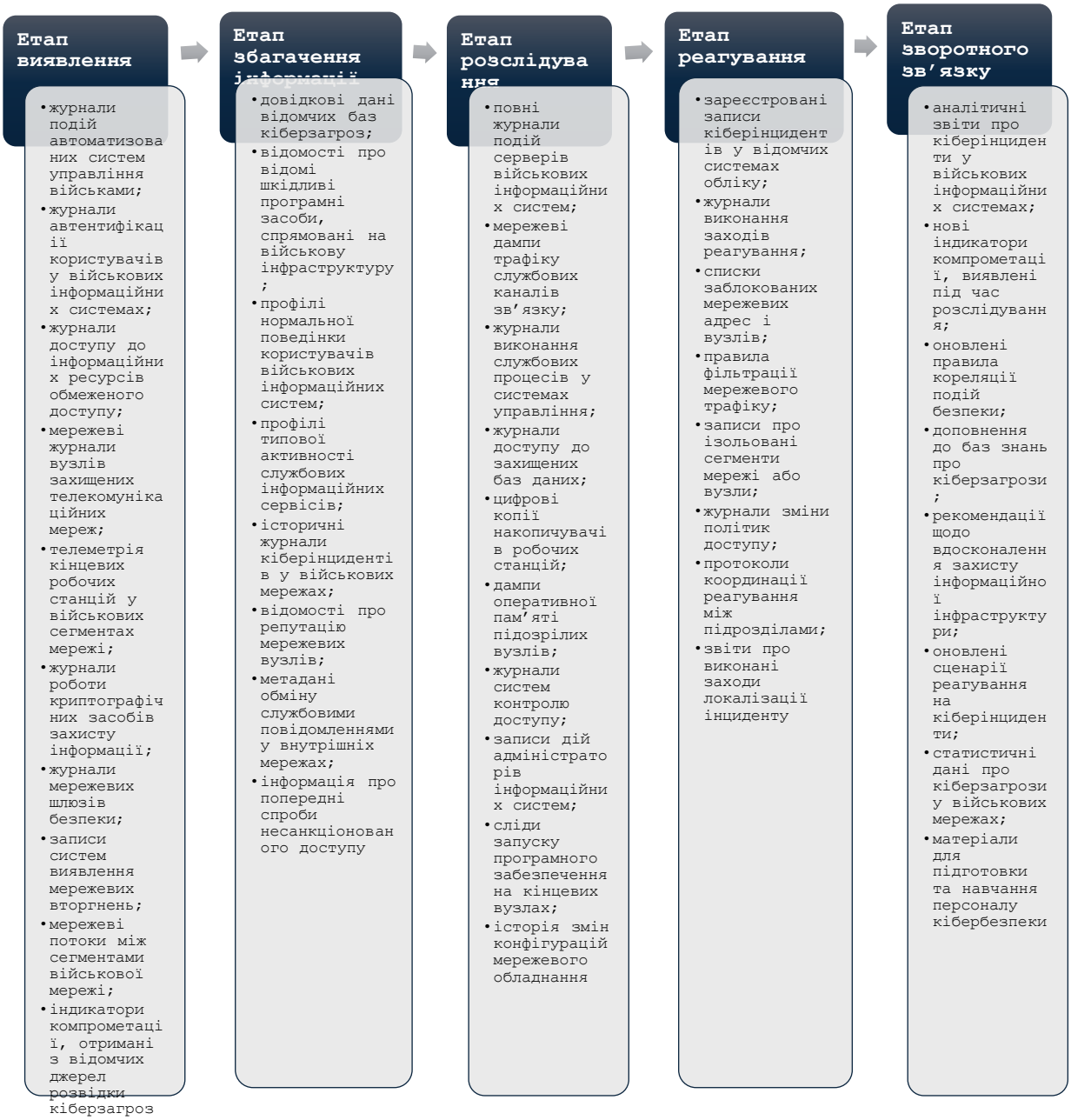


Рис. 1.4. Потік даних від виявлення до реагування
у військовій системі управління інформаційною безпекою

Етап збагачення інформації дозволяє надати додатковий контекст виявленим подіям, що дозволяє точніше оцінити їхню природу та потенційну небезпеку. Платформи оркестрації та автоматизації реагування (SOAR) автоматично

звертаються до зовнішніх баз даних для отримання додаткових індикаторів, а засоби поведінкової аналітики оцінюють рівень аномальності та потенційну небезпечність подій. У результаті формується більш повне уявлення про походження події, її зв’язки та можливі наслідки.

Етап розслідування забезпечує поглиблений аналіз інциденту та встановлення його причин, масштабу і впливу на інформаційну систему. SOAR агрегує інформацію з різних джерел, формує структуровані кейси для аналізу фахівцями SOC та надає попередньо зібраний контекст, що дозволяє значно пришвидшити оцінювання інциденту. Основним завданням є підтвердження або спростування факту атаки та визначення її параметрів.

Метою етапу реагування є локалізація, нейтралізація та мінімізація наслідків кіберінциденту. Використовуючи підготовлені сценарії (playbooks), SOAR автоматично виконує дозволені дії з локалізації інциденту в інтегрованих системах. Засоби EDR (Endpoint Detection and Response) ізолюють скомпрометовані кінцеві пристрої, SIEM реєструє інциденти та забезпечує їх подальше відстеження, а системи розвідки кіберзагроз поповнюються новими даними, отриманими під час реагування.

Етап зворотного зв’язку дозволяє забезпечити удосконалення системи кіберзахисту на основі отриманого досвіду. Після завершення оброблення інциденту результати аналізу використовуються для вдосконалення правил виявлення. Виявлені індикатори інтегруються до платформ обміну розвідданими про загрози, а сценарії реагування SOAR коригуються на основі накопиченого досвіду.

Оборонні SOC (System-on-a-chip), що захищають засекречені мережі, стикаються з унікальними архітектурними обмеженнями. Ізольовані класифіковані мережі (SIPRNet, JWICS) працюють окремо від некласифікованих систем, підключених до Інтернету. Архітектура SOC повинна відображати це розділення за допомогою окремих екземплярів SIEM, окремих розгортань EDR та ізольованих потоків інформації про загрози. Розподілений контроль інформації обмежує доступ

персоналу до конкретних розвідувальних даних або розслідувань інцидентів. Архітектури SOC повинні забезпечувати розподіл за допомогою контролю доступу на основі ролей та окремих робочих процесів щодо інцидентів. Вимоги до відповідності спеціальним вимогам вимагають архітектур SOC, що підтримують збереження секретних доказів, звітування перед розвідувальними службами та процедури розслідування, що відповідають військовим стандартам. Архітектура військового командування повинна підтримувати координацію між кількома командуваннями, видами військ та союзними державами. Моделі федеративної SOC підтримують місцеві командні повноваження, водночас забезпечуючи обмін інформацією через механізми секторальної координації. Процедури ескалації інцидентів визначають, коли розслідування переходять від місцевих оперативних центрів до спільних оперативних груп або коаліційних операцій. Архітектури безпечного зв'язку забезпечують координацію класифікованих інцидентів між організаціями

На основі проведеного аналізу встановлено, що в існуючих системах моніторингу інформаційної безпеки відсутні можливості прогнозування динаміки кіберінцидентів та оцінки переходу системи до критичних станів. Саме тому доцільно інтегрувати математичні моделі аналізу та прогнозування у системи управління інформаційною безпекою для раннього виявлення нестійких режимів функціонування систем.

1.4. Аналіз існуючих підходів до управління ризиками та кіберстійкістю

1.4.1. Традиційні моделі управління ризиками інформаційної безпеки

Управління ризиками інформаційної безпеки є ключовим елементом побудови системи захисту інформації в організаціях. Основна мета цього процесу полягає у виявленні загроз, оцінюванні ймовірності їх реалізації, визначенні можливих наслідків та розробленні заходів мінімізації ризиків. Традиційні моделі управління ризиками базуються на формалізованих методиках аналізу активів,

загроз, уразливостей та потенційного збитку для інформаційних систем [46]. У більшості підходів ризик визначається як комбінація ймовірності реалізації загрози та величини потенційного збитку, що дозволяє визначати пріоритети захисних заходів та оптимізувати витрати на забезпечення інформаційної безпеки [47].

Традиційні моделі ризик-менеджменту інформаційної безпеки зазвичай включають такі основні етапи [46]:

1) ідентифікація активів інформаційної системи;
2) визначення загроз і уразливостей;
3) оцінювання ймовірності реалізації загроз;
4) оцінювання потенційних наслідків;
5) визначення рівня ризику;
6) вибір заходів оброблення ризиків (зменшення, прийняття, передавання або уникнення).

Найбільш поширені традиційні моделі та методики управління ризиками інформаційної безпеки розроблені на основі міжнародних стандартів і методологій, які застосовуються в державному секторі, промисловості та критичній інфраструктурі.

Стандарт ISO/IEC 27005 є одним із найбільш поширених підходів до управління ризиками інформаційної безпеки та входить до сімейства стандартів ISO/IEC 27000 [48]. Він визначає методологію управління ризиками в межах системи управління інформаційною безпекою (ISMS). Модель передбачає такі процеси, як встановлення контексту ризику, ідентифікацію ризиків, аналіз і оцінювання ризиків, оброблення ризиків та постійний моніторинг та перегляд ризиків.

Методологія добре інтегрується із системами управління інформаційною безпекою та дозволяє формалізувати процес управління ризиками в організаціях з жорсткими регламентами, що характерно для військових структур.

Методика NIST SP 800-30 [49] розроблена Національним інститутом стандартів і технологій США та використовується для оцінювання ризиків у

державних і корпоративних інформаційних системах. Методологія передбачає оцінювання ризику на основі двох ключових параметрів: ймовірності реалізації загрози; потенційного збитку від її реалізації. Широко використовується в державних установах і оборонному секторі. Дає можливість системно оцінювати ризики для критичних інформаційних систем і враховує специфіку кіберзагроз національної безпеки.

Метод OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) [50], [51], [52] був розроблений у Carnegie Mellon University і орієнтований на організаційний аналіз ризиків інформаційної безпеки. OCTAVE відрізняється тим, що значна частина аналізу виконується внутрішніми фахівцями організації, а не зовнішніми експертами. Методологія орієнтована на організаційні процеси та управління активами. Може застосовуватися у військових структурах, але менш ефективна для складних технічних систем і мережевих середовищ. OCTAVE передбачає три основні етапи:

1) формування профілів загроз для критичних інформаційних активів;
2) аналіз вразливостей інфраструктури;
3) розроблення стратегії управління ризиками.

Метод CRAMM (Central Computer and Telecommunications Agency Risk Analysis and Management Method) [53] широко застосовується в державних організаціях і великих корпоративних інформаційних системах, забезпечує детальний аналіз інформаційних активів та загроз, що робить її придатною для застосування у великих державних та військових інформаційних системах. CRAMM включає визначення цінності інформаційних активів, аналіз загроз і вразливостей та вибір відповідних заходів захисту.

Модель FAIR (Factor Analysis of Information Risk) – це кількісна модель аналізу ризиків, яка дозволяє оцінювати ризики у фінансових показниках. Вона базується на аналізі факторів, що впливають на частоту виникнення інцидентів і величину можливих втрат. Основною особливістю FAIR є використання кількісних оцінок ризику, що дозволяє інтегрувати процес управління кіберризиками з

економічними показниками діяльності організації [54]. Однак модель орієнтована переважно на економічні показники втрат, що ускладнює її використання в системах, де ключовими є стратегічні або оперативні наслідки.

Аналіз традиційних моделей управління ризиками інформаційної безпеки дозволяє виділити їхні спільні характеристики:

– орієнтація на активи інформаційної системи;

– використання експертної оцінки загроз і уразливостей;

– поєднання якісних і кількісних методів оцінювання ризику;

– формалізований процес аналізу ризиків та інтеграція з системами управління інформаційною безпекою.

Порівняльний аналіз традиційних моделей управління ризиками інформаційної безпеки показує, що більшість із них базуються на подібній логіці: ідентифікації активів, визначенні загроз і вразливостей, оцінюванні ймовірності реалізації загроз та визначенні потенційних наслідків. Основні відмінності полягають у ступені формалізації процедур, типі оцінювання ризику (якісному або кількісному) та сфері практичного застосування. Найбільш придатними для військової сфери є моделі ISO/IEC 27005, NIST SP 800-30 та CRAMM, оскільки вони:

– орієнтовані на державні та критично важливі інформаційні системи;

– підтримують формалізовані процедури управління ризиками, що відповідає вимогам військових організацій;

– дозволяють враховувати широкий спектр загроз – від технічних до організаційних;

– можуть інтегруватися з системами моніторингу кібербезпеки та управління інцидентами.

1.4.2. Обмеження існуючих підходів в умовах кіберконфліктів

У військовому середовищі інформаційні та кіберсистеми стають критичною частиною оперативного управління, бойових операцій і стратегічного контролю. Вони не лише збільшують ефективність дій військ, але й створюють нові вектори для кібератак, які можуть суттєво вплинути на безперервність функціонування військових процесів. При цьому традиційні підходи до управління ризиками інформаційної безпеки виявляють низку суттєвих обмежень у контексті цих складних систем [55].

Однією з основних слабких сторін традиційних моделей оцінювання ризику є висока залежність від експертних оцінок та їх суб'єктивності, що спричинює різний рівень результатів при повторних оцінюваннях і обмежує їх відтворюваність. Це особливо критично в умовах військових операцій, де помилки можуть мати катастрофічні наслідки [56]. Багато традиційних підходів до управління ризиками орієнтовані на статичне оцінювання загроз і уразливостей, тоді як кіберзагрози постійно еволюціонують. Це робить їх недостатньо адаптивними до сучасних сценаріїв кіберконфліктів, де атаки стають більш складними, багаторівневими та непередбачуваними [55]. Традиційні методики ризик-менеджменту часто зосереджуються на виявленні та запобіганні загрозам, але недостатньо уваги приділяють окремому аспекті – кіберстійкості, яка включає здатність системи опиратися, адаптуватися та відновлюватись після успішної атаки. Кіберстійкість є ширшим поняттям, ніж класичне управління ризиками, і включає елементи адаптації та відновлення функцій, що стає вирішальним у військовому контексті. Багато традиційних моделей не пропонують чітких кількісних метрик для вимірювання ризику або рівня стійкості. У військовому середовищі, де конфіденційність, цілісність та доступність даних мають критичне значення, відсутність кількісних показників утруднює порівняння ризиків і обґрунтування управлінських рішень.

Додаткові виклики в контексті військових інформаційних систем включають врахування наступних факторів:

– складність і багаторівневість систем – військові інформаційні системи містять численні взаємозалежні компоненти (від систем управління та зв'язку (С3І) до логістичних і розвідувальних платформ), саме ці системи часто є складними та розподіленими, що створює додаткові уразливості, які не завжди адекватно враховуються у традиційних моделях оцінювання ризику [27];

– інтеграція нових технологій – модернізація військових систем включає впровадження штучного інтелекту, автоматизації та складних кіберфізичних платформ, ці технології створюють нові складнощі у визначенні ризиків та побудові моделей стійкості, оскільки традиційні підходи недостатньо враховують динамічність і невизначеність поведінки таких систем під час атак [57];

– недостатність практичних моделей кіберстійкості – хоча концепція кіберстійкості активно розвивається у науковій літературі, існує відчутний розрив між теоретичними моделями й практичними механізмами застосування в умовах військових операцій, на рівні практичного застосування є потреба у узгоджених моделей, заснованих на реальних сценаріях бойових дій, які могли б оперативно адаптуватися до нових типів загроз.

Таким чином, поточний стан наукових підходів до управління ризиками інформаційної безпеки, хоча і забезпечує основу для ідентифікації загроз та їх оцінювання, має суттєві обмеження в контексті військових інформаційних систем у умовах кіберконфліктів. Ці обмеження включають:

– суб'єктивність і недостатню відтворюваність оцінок ризику;

– статичність традиційних підходів, що не відповідає динаміці сучасних кіберзагроз;

– недостатню увагу до кіберстійкості як окремого феномену;

– відсутність узгоджених кількісних метрик для порівняння рівнів ризику й стійкості;

– недостатню адаптацію моделей для складних багаторівневих систем, характерних для військової сфери.

Для подолання цих обмежень сучасні дослідження пропонують зміщення акцентів від вузького ризик-менеджменту до інтегрованих моделей кіберстійкості, які поєднують виявлення загроз, адаптацію, відновлення та навчання на основі постійного аналізу атак і поведінки систем [55].

На основі проведеного аналізу сучасних підходів забезпечення кіберстійкості інформаційних систем встановлено, що більшість методів використовують експертні оцінки або статичні моделі ризику, які не враховують складну динаміку впливу та розвитку кіберзагроз. Тому необхідно застосовувати математичні методи моделювання, зокрема на основі теорій катастроф та конфліктів, які мають можливості описувати динаміку кіберінцидентів та прогнозувати критичні стани інформаційних систем.

1.5. Постановка наукового завдання дослідження

В сучасному світі актуальною проблемою є забезпечення конфіденційності, цілісності та доступності інформації на всіх рівнях життя. Удосконалення інформаційних систем для захисту вимагають впровадження та використання математичного апарату, який дозволить не лише виявляти загрози, але і прогнозувати їх дію на інформаційну систему.

Динамічні процеси все більше характеризують явище в системах інформаційної безпеки, тому стохастичні моделі не забезпечують в цілому опис їх функціонування та вирішення можливих проблем. Саме тому доцільно застосовувати динамічні моделі, які справляються з даними задачами та базуються на положеннях математичної теорій катастроф та конфліктів.

Динаміка розвитку сучасних збройних сил суттєво змінює характер вимог щодо важливих якостей військовослужбовців, ставить нові завдання щодо їх компетентності. Аналіз досвіду навчань та заходів підготовки особового складу збройних сил провідних країн світу показує, що широке впровадження сучасних

інформаційних технологій та засобів імітаційного моделювання у систему бойової та оперативної підготовки дозволяє досягти значного зниження фінансових витрат при одночасному підвищені якості підготовки військ. При цьому командно-штабні навчання з використанням систем імітаційного моделювання стали найефективнішою формою підготовки командувачів (командирів) та органів управління всіх рівнів.

Проте впровадження інформаційних технологій та систем імітаційного моделювання у процеси бойової та оперативної підготовки вимагає інтеграцію складних інформаційних систем для реалізації всіх поставлених завдань. Такі складні військові системи відповідають за обробку, передавання та аналіз великих об'ємів даних у режимі реального часу. Але при цьому зростає небезпека впливу кіберзагроз, які порушують функціонування систем або призводять до переходу системи в критичні стани.

Більшість існуючих підходів використовують статистичні методи, методи машинного навчання або класичні моделі для аналізу та прогнозування стану інформаційних систем при дії загроз та уразливостей. Проте дані підходи не враховують конфліктну взаємодію між джерелами кібератак та системою захисту інформаційної системи, а також складну нелінійну динаміку функціонування інформаційних систем, що призводить до виникнення критичних станів системи та втрати їх стійкості.

У зв'язку з цим необхідно вирішити актуальне наукове завдання, яке полягає в розробці моделей та методів забезпечення кібербезпеки військових інформаційних систем на основі математичної теорії катастроф та теорії конфліктів для моделювання динаміки кіберзагроз, прогнозування критичних переходів станів інформаційної системи та підтримки прийняття рішень щодо підвищення її кіберстійкості

Мета дисертаційного дослідження полягає в підвищенні кіберстійкості військових інформаційних систем за рахунок розробки моделей та методів забезпечення кібербезпеки на основі застосування математичної теорії катастроф

та теорії конфліктів для аналізу та моделювання складної нелінійної динаміки функціонування систем під впливом кіберзагроз і прогнозування критичних переходів їх станів.

У відповідності до поставленої мети для вирішення наукового завдання в роботі мають бути виконані такі *часткові завдання*:

- проаналізувати сучасні підходи забезпечення кібербезпеки військових інформаційних систем та визначити особливості нелінійної динаміки їх станів під впливом кіберінцидентів;
- обґрунтувати доцільність застосування математичної теорії катастроф та теорії конфліктів для моделювання динаміки станів інформаційних системи під впливом кіберінцидентів;
- розробити математичну модель впливу кіберінцидентів на стійкість систем управління інформаційною безпекою з використанням катастрофи типу «Метелик» та оцінити її ефективність щодо впливу кіберінцидентів на стійкість систем;
- удосконалити метод кластеризації загроз та уразливостей інформаційних систем та порівняти його ефективність з класичними методами кластеризації;
- розробити модель прогнозування критичних переходів станів інформаційної системи при інтеграції з SIEM- системою та оцінити ефективність її застосування для раннього виявлення нестійких режимів функціонування системи;
- удосконалити метод підтримки прийняття рішень для забезпечення кіберстійкості військових інформаційних систем, який включає інтеграцію математичних моделей , методів аналізу та прогнозування на основі теорії конфліктів для моделювання протидії кіберзагрозам та теорії катастроф для прогнозування критичних станів системи;
- оцінити ефективність удосконаленого метода підтримки прийняття рішень шляхом імітаційного моделювання сценаріїв реагування на кіберінциденти.

Висновки до розділу 1

1. Проведено аналіз структури та функціональних особливостей військових інформаційних систем. Встановлено, що військові інформаційні системи є складними багаторівневими технічними та організаційними структурами, які забезпечують процеси управління військами на стратегічному, оперативному і тактичному рівні, які включають організаційні, інформаційні, функціональні та технічні компоненти, що формують суцільний інформаційний простір управління.
2. Встановлено, що забезпечення кіберстійкості даних систем є основною вимогою, яка гарантує конфіденційність, цілісність та доступність інформації, а також здатність систем прогнозувати, протидіяти атакам, відновлюватися після інцидентів і адаптуватися до змін у кіберпростору.
3. Проведено аналіз кіберзагроз та уразливостей військових інформаційних систем та встановлено, що спуфінг, глушіння сигналів, викрадення даних, використання шкідливого програмного забезпечення та фішингові атаки найчастіше використовують зловмисники.
4. Визначено, що сучасні кібератаки реалізуються складними багаторівневими механізмами проникнення, накопиченням в мережах та часто функціонують як розширена постійна загроза (APT).
5. На основі проведеного аналізу визначено пріоритетні напрямки вдосконалення існуючих та розробки нових методів забезпечення кібербезпеки військових інформаційних систем, у межах яких сформульовано наукове завдання, яке полягає в розробці моделей та методів забезпечення кібербезпеки військових інформаційних систем на основі математичної теорії катастроф та теорії конфліктів для моделювання динаміки кіберзагроз, прогнозування критичних переходів станів інформаційної системи та підтримки прийняття рішень щодо підвищення її кіберстійкості.

РОЗДІЛ 2. МАТЕМАТИЧНІ ОСНОВИ АНАЛІЗУ СТІЙКОСТІ ТА КРИТИЧНИХ ПЕРЕХОДІВ У ВІЙСЬКОВИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

2.1. Теорія катастроф як основа моделювання критичних переходів у інформаційних системах

У сучасному світі актуальною проблемою є забезпечення конфіденційності, цілісності та доступності інформації на всіх рівнях функціонування інформаційної системи. Удосконалення механізмів захисту інформаційних систем потребує застосування математичного апарату, що дозволяє не лише формалізувати процеси протидії загрозам та підвищити обґрунтованість прийнятих рішень, але і прогнозувати їх дію на інформаційну систему [58]-[61].

Зростаюча складність систем інформаційної безпеки зумовлює домінування динамічних процесів. Це ускладнює їх моделювання через стохастичні моделі, які не забезпечують в цілому опис їх функціонування та вирішення можливих проблем. Саме тому доцільно доцільно застосовувати динамічні моделі, які справляються з даними задачами та базуються на положеннях математичної теорії катастроф [62]-[74].

2.1.1. Динамічні системи та поняття стійкості інформаційних систем

Розглянемо систему інформаційної безпеки, як динамічну, яка за певних умов втрачає стан рівноваги, змінює стани при русі, що викликає деградації та руйнації, а також відновлюється у іншому стані. Для дослідження таких систем, коли виникають різкі зміни та стрибкоподібні процеси, що пов’язані із впливом кіберінцидентів на інформаційні системи, є логічним застосувати положення теорії катастроф. [59]

Теорія катастроф досліджує поведінку розв’язків рівнянь зі зміною параметрів даних рівнянь [59]. Розглянемо систему з n рівнянь у просторі R^n з координатами $x = (x_1, x_2, \dots, x_n)$:

$$F_i(\psi_j; c_\alpha; t, \frac{d\psi_j}{dt}, \frac{d^2\psi_j}{dt^2}, \dots; x_l; \frac{\partial\psi_j}{\partial x_l}, \frac{\partial^2\psi_j}{\partial x_l \partial x_m}, \dots; \int dx_l, \dots) = 0 \qquad (2.1)$$

де $1 \le i \le n$, $1 \le l, m \le N$, $1 \le \alpha \le k$, $\psi_i(t, x, c_\alpha)$ – розв'язки даної системи, x, t – просторово-часові координати.

Оскільки розв'язки $\psi_i(t, x, c_\alpha)$ описують стан деякої системи, то їх називають змінними стану, а параметри c_α контролюють якісні властивості розв'язків $\psi_i(t, x, c_\alpha)$, тому їх називають параметрами керування. Достатньо важкою є задача знаходження розв'язків $\psi_i(t, x, c_\alpha)$, а також вплив параметрів керування c_α на дані розв'язки. Тому для подальшого дослідження даної системи поетапно спростимо (2.1), припускаючи, що відсутні похідні за часом вищих, ніж перша похідна. Також припускаємо, що похідні за часом представлено в канонічному вигляді, тоді (2.1) набуде вигляду:

$$F_i = \frac{d\psi_i}{dt} - f_i(\psi_j; c_\alpha; t)$$

При умові коли $F_i = 0$ система (2.1) називається динамічною системою. Якщо функції f_i не залежать від часу, то систему (2.1) називають автономною динамічною систему. Але і в даному випадку дана система достатньо складна для подальшого використання. Тому доцільно розглядати функції f_i як негативний градієнт відносно ψ_j деякої функції $V(\psi_j; c_\alpha)$, тобто

$$f_i = -\frac{\partial V(\psi_j; c_\alpha)}{\partial \psi_j}$$

$$F_i = \frac{d\psi_i}{dt} + \frac{\partial V(\psi_j; c_\alpha)}{\partial \psi_j} = 0.$$

Тоді систему (2.1) називають градієнтною системою.

Якщо $\frac{d\psi_i}{dt} = 0$, то система (2.1) перебуває у стані рівноваги, тоді рівняння динамічної системи набуває виду

$$\frac{\partial V(\psi_j;c_\alpha)}{\partial \psi_j} = 0. \qquad (2.2)$$

Теорія катастроф досліджує, як зміна керівних параметрів c_α впливає на рівноважні стани $V_i(c_\alpha)$ потенціалу $V(\psi_j; c_\alpha)$ [59].

В основі теорії катастроф лежать дві форми представлення потенціальних функцій в околі невироджених і вироджених критичних точок.

Припустимо, що система (2.2) перебуває в стані рівноваги та

$$\nabla V = 0.$$

Властивості стійкості рівноваги визначають х власних значень матриці стійкості (матриці Гессе):

$$V_{ij} = \begin{vmatrix} \frac{\partial^2 V}{\partial x_1^2} & \cdots & \frac{\partial^2 V}{\partial x_1 \partial x_n} \\ \cdots & \cdots & \cdots \\ \frac{\partial^2 V}{\partial x_n \partial x_1} & \cdots & \frac{\partial^2 V}{\partial x_n^2} \end{vmatrix}.$$

При умові

$$det(V_{ij}) \neq 0$$

Тобто критична точка є невиродженою, то потенціал функції набуває форми

$$V = \sum_{i=1}^{n} \lambda_i y_i^2, \qquad (2.3)$$

де λ_i – власні значення матриці Гессе, а рівняння (2.3) можна представити у канонічній формі Морса:

$$V = -\tilde{y}_1^2 - \ldots - \tilde{y}_i^2 + \tilde{y}_{i+1}^2 + \ldots + \tilde{y}_n^2 = M_i^n(\tilde{y}) .$$

Функцію $M_i^n(\tilde{y})$ називають морсовим $i-$сідлом, а точки, в яких $\nabla V = 0$ називають критичним або точками рівноваги функції $V(x_1, x_2, \ldots, x_n)$.

Якщо $det(V_{ij}) = 0$, то критична точка є виродженою, що призводить до порушення стійкості стану системи. В даній ситуації доцільно розглянути канонічний розклад Тома, який дозволяє враховувати локальну структуру потенціалу та появу біфуракцій.

Нехай x_0 вироджена критична точка функції $V(x; c)$ при $c = c_0$, тоді в деякому околі точки (x_0, c_0) у просторі $R^n \otimes R^k$ маємо

$$V \cong Cat(l, k) + \sum_{j=l+1}^{n} \frac{\lambda_j(c) y_j^2}{2},$$

де $Cat(l, k)$ – функція катастрофи, яка описує поведінку l змінних у виродженій критичній точці, $\lambda_j(c)$ – власні значення матриці Гессе, k – кількість керівних параметрів [59].

Відповідно l, k визначають тип катастрофи, а саме для малих значень l та k існує скінченний набір простих форм катастроф за Томом для $k < 6$ [59]. Проведений аналіз розкриває канонічні форми Морса та Тома в загальному вигляді потенціальних функцій.

Проведемо аналіз критичних точок функції двох змінних, що дозволить розкрити властивості додаткових видів подій, а особливо потенціали з однією або двома змінними.

Стан системи в будь - який момент часу t визначають за допомогою

$$(x_1, x_2, \ldots, x_n),$$

де x_i – внутрішні змінні, n – скінченне і перебуває під дією

$$(u_1, u_2, \ldots, u_m),$$

де u_j – зовнішні змінні, $m \leq 5$.

Нехай $f(x, y)$ – нескінченно диференційована функція, а також припустимо, що існує критична точка (x_0, y_0), так що

$$f(0,0) = f_x(0,0) = f_y(0,0).$$

Ряд Тейлора для функції f матиме вигляд

$$f(x, y) = \frac{1}{2}(ax^2 + 2hxy + by^2) + O(\|(x, y)\|^3),$$

де

$$a = \frac{\partial^2 f}{\partial x^2}, h = \frac{\partial^2 f}{\partial x \partial y}, b = \frac{\partial^2 f}{\partial y^2}.$$

Крива, що задається рівнянням

$$ax^2 + 2hxy + by^2 = F,$$

визначає конічну поверхню при $F - const$.

Якщо $ab - h^2 > 0$, маємо еліпс при умові, що $aF > 0$, або не має дійсних точок, при умові $aF < 0$.

Якщо $ab - h^2 < 0$, то маємо гіперболу. Враховуючі дані умови, можна визначити види критичних точок функції $f(x, y)$.

Якщо позначити

$$\Delta = \frac{\partial^2 f}{\partial x^2}\frac{\partial^2 f}{\partial y^2} - \left(\frac{\partial^2 f}{\partial x \partial y}\right)^2,$$

то

$\Delta > 0$, $\frac{\partial^2 f}{\partial x^2} < 0$ - маємо максимум функції $f(x, y)$,

$\Delta > 0$, $\frac{\partial^2 f}{\partial x^2} > 0$ - маємо мінімум функції $f(x, y)$,

$\Delta > 0$ – маємо функцію $f(x, y)$, виду сідло.

Важливо відзначити також, що в околі невиродженої критичної точки функцію $f(x, y)$ можна апроксимувати еліптичним параболоїдом у випадку максимуму або мінімуму або гіперболічним параболоїдом у випадку сідлової точки.

Функції є структурно нестабільними при $\Delta = 0$, оскільки існують функції, які близькі до даних при $\Delta > 0$ та $\Delta < 0$. У цьому випадку всі три частинні похідні другого порядку дорівнюють нулю в початку координат, а також функція $f(x, y)$ вироджена як в напрямку x, так і в напрямку y. З іншого боку, можна припустити, що

$$f_{xx} f_{yy} = (f_{xy})^2$$

за умови, що не всі похідні зникають окремо.

За умови $ab - h^2 = 0$ маємо повний квадрат $|ax^2 + 2hxy + by^2|$, а також

$$f(x,y) = \pm\frac{1}{2}(px + qy)^2 + \varepsilon,$$

де $p = \sqrt{|a|}$, $q = \sqrt{|b|}$.

Форма розкладу передбачає обертання осей для задання новими координатами u, v у вигляді

$$u = \frac{px+qy}{\sqrt{(p^2+q^2)}}, v = \frac{qx-py}{\sqrt{(p^2+q^2)}}.$$

Частинні похідні першого та другого порядку функції f відносно змінних на початку задаються як

$$\frac{\partial f}{\partial u} = \frac{\partial f}{\partial v} = \frac{\partial^2 f}{\partial v^2} = \frac{\partial^2 f}{\partial u \partial v} = 0,$$

де

$$\frac{\partial^2 f}{\partial u^2} = \pm(p^2 + q^2) \neq 0.$$

З даних умов випливає, що функція має максимум або мінімум в напрямку змінної u, але не відомо, що відбувається з функцією в напрямку координати v.

Нехай

$$w = usin\theta + vcos\theta,$$

тоді

$$\frac{df}{dw} = sin\theta\,\frac{\partial f}{\partial u} + cos\theta\,\frac{\partial f}{\partial v} = 0,$$

$$\frac{d^2 f}{dw^2} = sin^2\theta\,\frac{\partial^2 f}{\partial u^2} + 2sin\theta cos\theta\,\frac{\partial^2 f}{\partial u \partial v} + cos^2\theta\,\frac{\partial^2 f}{\partial v^2} = sin^2\theta\,\frac{\partial^2 f}{\partial u^2}.$$

За даних умов ряд Тейлора для функції f зводиться до вигляду

$$f = \frac{v^3}{3!}\frac{\partial^3 f}{\partial v^3} + \frac{v^4}{4!}\frac{\partial^4 f}{\partial v^4} + \ldots$$

Отриманий результат можна поширити на будь – яку скінченну кількість змінних. Нехай задано функцію

$$f(x_1, x_2, \ldots, x_n),$$

де n – незалежні змінні, яка має критичну точку на початку координат.

Формуємо матрицю Гессе для визначення характеру критичних точок для функції $\mathrm{f}(\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_\mathrm{n})$. Якщо ранг визначника дорівнює n, а саме

$$rank\ H_f(x_0) = n,$$

а також визначник не дорівнює нулю, тобто

$$det\ H_f(x_0) \neq 0,$$

то існує перетворення координат, що дозволяє записати $f(x_1, x_2, \ldots, x_n)$ у вигляді

$$f = e_1 x_1^2 + e_2 x_2^2 + \ldots + e_n x_n^2 + \varepsilon,$$

де $e_i = \pm 1$, що дозволяє визначити тип даної системи.

При $rank\ H_f(x_0) = n - r$, для $r > 0$ функція набуде вигляду

$$f = e_{r+1} x_{r+1}^2 + e_{r+2} x_{r+2}^2 + \ldots + e_{r+n} x_{r+n}^2 + \varepsilon.$$

Нестабільність стану обмежується змінними $x_1, x_2, \ldots, x_n$, при цьому іншими можна знехтувати. Отриманий результат називають «Лемою розщеплення» [60].

Нехай маємо гладку функцію

$$f: R^n \to R,$$

критичну точку x_0, таку що

$$\nabla f(x_0) = 0,$$

та гессіан функції в критичній точці:

$$rank\ H_f(x_0) = n - r$$

має дефект $r > 0$.

Дана лема вказує, що кількість видів катастроф не залежать від кількості змінних n стану, а залежать лише від кількості суттєвих змінних стану r (рангом гессіана), який вказує на кількість напрямів, у яких функція вироджується.

При дослідженні інформаційних систем важливо математично і візуально бачити їх представлення. Тому доцільно звернути увагу на математичне і геометричне представлення семи елементарних катастроф.

Нехай $V(x, c)$ – потенціал поверхні, який залежить від стану x і від параметрів c тоді рівняння рівноваги набуде вигляду

$$\nabla_x V = 0.$$

Множину сингулярностей S, така що $S \subseteq M$ та складається з усіх вироджених критичних точок V, в яких

$$\nabla_x V = 0 \text{ та } \Delta \equiv det\{H(V)\} = 0,$$

де $H(V)$ – матриця частинних похідних другого порядку.

Проєктується S вниз у простір керування C, при цьому виключаючи змінні стану з рівнянь, які визначаються. Визначено множину біфуркацій B, яка є множиною всіх точок простору керування C, в яких змінюється форма V. Наступним кроком є визначення форми V для кожної точки в C. Таким чином отримали алгоритм аналізу катастроф у теорії Рене Тома [59], який описує процес виділення із потенціалу $V(x, c)$ поверхню рівноваги M, множину сингулярностей S та множину біфуркацій B, що дозволить в подальшому класифікувати катастрову та визначити її вдастивості.

2.1.2. Біфуркації у нелінійних динамічних системах кіберзахисту

На стан нелінійних динамічних систем кіберзахисту впливають зовнішні та внутрішні фактори, як інтенсивність кібератак, рівень уразливості, засоби захисту, час реагування на дані атаки, які призводять до зміни параметрів керування системи кіберзахисту, а також змінюють режими функціонування та появу біфуркацій, що впливає на стійкість системи кіберзахисту.

Для військових інформаційних систем велику небезпеку несуть катастрофічні біфуркації, які створюють різкий перехід між станами, а також не дозволяють швидке повернення до стану рівноваги системи. Теорія катастроф, а саме катастрофи деяких типів максимально відображають дані переходи в інформаційних системах кіберзахисту.

Перш ніж розпочати дослідження деяких типів елементарних катастроф, доцільно розглянути поняття точки біфуркації у нелінійних динамічних системах.

Нехай задано динамічну систему

$$\frac{dy}{dt} = f(y, \lambda), \qquad (2.4)$$

де $y \in R^n, \lambda \in R^p, \lambda$ – керуючий параметр.

Припустимо, що рівняння (2.4) має фіксовану точку рівноваги

$$(y, \lambda) = (y_0, \lambda_0),$$

в якій виконується умова

$$f(y_0, \lambda_0) = 0.$$

Розглянемо лінійне векторне поле

$$\frac{d\xi}{dt} = D_y f(y_0, \lambda_0)\xi, \quad \xi \in R^n,$$

тоді $D_y f(y_0, \lambda_0)$ не має власних значень на уявній осі. Тоді за теоремою про неявну функції існує єдина функція $y(\lambda)$ така, що

$$f(y(\lambda), \lambda) = 0$$

для λ, яка достатньо близька до λ_0, та

$$y(\lambda_0) = y_0.$$

Отже, для параметра λ, який є достатньо близьким до λ_0, точка рівноваги є гіперболічною та зберігає тип стабільності. В протилежному випадку можуть створюватись чи знищуватися фіксовані точки рівноваги, виникати залежна від часу поведінка (періодична, квазіперіодична або хаотична динаміка). Тому, чим більше власних значень на уявній осі, тим більш можливе порушення стабільності [60].

Припустимо, що $D_y f(y_0,\ \lambda_0)$ має єдине нульове власне значення, тоді локальна орбітальна структура системи в околі точки (y_0, λ_0) задається рівнянням

$$\frac{dx}{dt} = f(x, \mu),$$

де $x \in R^1, \mu \in\ R^p$, $\mu = \lambda - \lambda_0$ та визначає біфуркаційну поведінку системи. Отже, точка (y_0, λ_0) називається точкою біфуркації динамічної системи

$$\frac{dy}{dt} = f(y, \lambda),$$

якщо в околі параметра λ_0 існують значення $\lambda_1 \neq \lambda_2$, при яких динамічні системи

$$\frac{dy}{dt} = f(y, \lambda_1)$$
$$\frac{dy}{dt} = f(y, \lambda_2)$$

не є топологічно еквівалентними.

Розглянемо деякі випадки існування точок біфуркації за певних умов, що дозволить більш глибше розкрити умови існування точок біфуркацій та їх властивості.

Розглянемо векторне поле

$$\frac{dx}{dt} = f(x, \mu) = \mu - x^2,\ x \in R^1, \mu \in R^1.$$

Тоді множина всіх фіксованих точок рівноваги

$$\mu = x^2$$

задається параболою на площині $\mu - x$ (Рис.2.1).

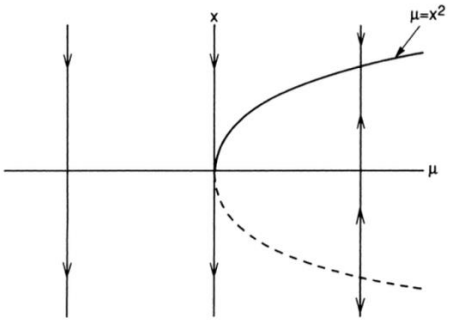


Рис. 2.1. Діаграма біфуркації сідло-вузол

Як видно на Рис. 2.1 стрілки вздовж вертикальних ліній позначають потік вздовж напрямку x. Таким чином, для $\mu < 0$ не має фіксованих точок рівноваги, і векторне поле зменшується в напрямку x. В протилежному випадку, для $\mu > 0$ існують дві фіксовані точки, одна з яких є стійкою.

При цьому точка $(x, \mu) = (0,0)$ є точкою біфуракції, а значення параметра $\mu = 0$ називають значенням біфуракції. Нормальна форма для біфуркації *сідло-вузол* задається рівнянням

$$\frac{dx}{dt} = \mu \pm x^2.$$

Для визначення *транскритичної* біфуркації розглянемо векторне поле виду

$$\frac{dx}{dt} = f(x, \mu) = \mu x - x^2, x \in R^1, \mu \in R^1.$$

Тоді множина всіх фіксованих точок рівноваги

$$x = \mu$$

задається прямою на площині $\mu - x$ (Рис.2.2).

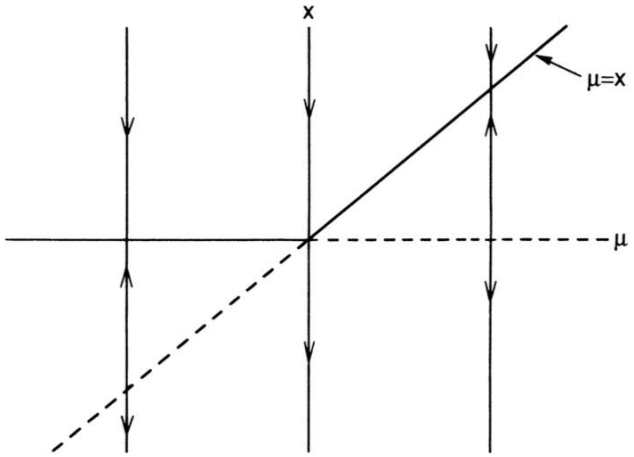


Рис. 2.2. Діаграма транскритичної біфуркації

Для даного типу існують дві фіксовані точки рівноваги при $\mu < 0$, а саме $x = 0$, що є стабільною, а також нестабільна точка $x = \mu$. Дані точки зливаються при $\mu = 0$. При $\mu > 0$ має зворотній варіант, а саме стабільною стає точка $x = \mu$. Нормальну форму для транскритичної біфуркації задають рівнянням

$$\frac{dx}{dt} = \mu x \mp x^2.$$

Для визначення біфуркації типу *вилка* розглянемо векторне поле виду

$$\frac{dx}{dt} = f(x, \mu) = \mu x - x^3, x \in R^1, \mu \in R^1.$$

Множина всіх фіксованих точок рівноваги Рис.2.3 задають рівнянням

$$x^2 = \mu.$$

В даному випадку точка $x = 0$ є стабільна фіксована точка, а для

$\mu = 0$ виникають дві інші стабільні фіксовані точки, що задаються як $x^2 = \mu$.

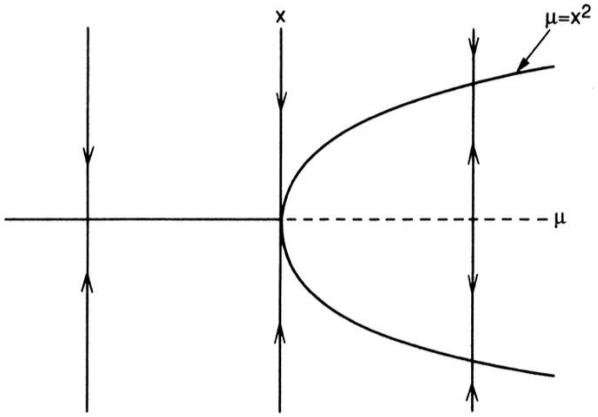


Рис. 2.3. Діаграма біфуркації типу вилка

Нормальну форму для біфуркації типу вилка задають рівнянням

$$\frac{dx}{dt} = \mu x \mp x^3.$$

Важливо також розглянути випадок негіперболічної фіксованої точки, в якій не відбувається зміни стану динамічної системи, а тому дана точка не є біфуркаційною.

Нехай задано векторне поле

$$\frac{dx}{dt} = f(x, \mu) = \mu - x^3, x \in R^1, \mu \in R^1,$$

для якого множину всіх фіксованих точок рівноваги (Рис.2.4.) задають рівнянням

$$\mu = x^3,$$

де точка $(0,0)$ є єдиною стабільною фіксованою точкою рівноваги [60].

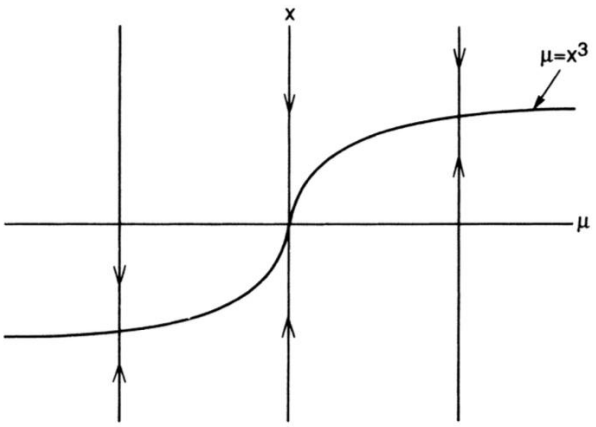


Рис.2.4. Діаграма фіксованих точок для негіперболічного випадку без біфуркації

Фіксування біфуркацій в інформаційних системах дозволяє реагувати на швидке зростання кіберінцидентів, виявляти їх в реальному часі, зменшити перевантаження SIEM – системи, а також попереджувати перехід від точкових кіберінцидентів до масштабних кібератак на всю військову інформаційну систему [61].

2.1.3. Геометричні та аналітичні моделі елементарних катастроф

Розглянемо математичну і геометричну основу деяких відомих типів катастроф для інтерпретації структури біфуркаційних множин, виявлення стійких та нестійких станів, а також критичні межі у просторі параметрів керування, що дозволить попередити кіберінциденти в інформаційних системах.

Нехай потенціал задається рівнянням

$$V(x) = x^3 + ux,$$

тоді поверхня рівноваги M визначає криву *складка*, що задається рівнянням

$$3x^2 + u = 0, \qquad (2.5)$$

множину сингулярностей S можна задати рівнянням

$$6x = 0,$$

де $(0,0)$ – вироджена критична точка, в якій порушується умова рівноваги і спостерігається катастрофа Рис.2.5, геометричне представлення побудовано за допомогою Python.

Множина біфуркацій розділяє простір керування на дві області. Якщо $u > 0$, то рівняння (2.5) не має дійсних коренів, а $V(x)$ не має критичних точок. Якщо $u < 0$, то $V(x)$ має дві критичні точки (мінімум і максимум), що призводить до існування двох станів рівноваги, а саме стійкий та нестійкий.

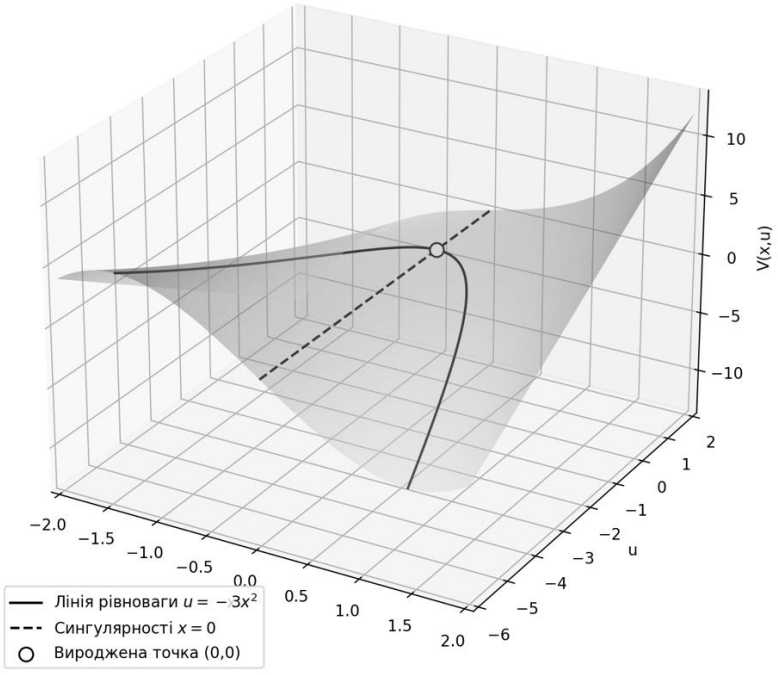


Рис. 2.5 Геометричне представлення катастрофи типу складки для потенціалу $V(x) = x^3 + ux$

У випадку поділу центру притягання на два окремих центри виникає катастрофа *збірки* [58]. Потенціал набуває вигляду

$$V(x) = x^4 + ux^2 + vx, \tag{2.6}$$

тоді поверхня рівноваги M задається рівнянням

$$4x^3 + 2ux + v = 0, \tag{2.7}$$

а множина сингулярностей S має рівняння

$$12x^2 + 2u = 0.$$

Щоб отримати множину біфуркацій, потрібно вилучити змінну x з рівнянь (2.6) та (2.7), після чого отримаємо рівняння

$$8u^3 + 27v^2 = 0.$$

Потрібно зауважити, що в області катастрофи типу *збірки* динамічна система має два стійких стани мінімуму, які розділені нестійким станом максимуму, а поза цією області існує один стійкий стан (Рис. 2.6), геометричне представлення побудовано за допомогою Python.

Потрібно відмітити, що при $u > 0$, якщо v змінювати, то зберігається рівновага стану x системи, але при $u < 0$ відбувається зрушення в поверхні рівноваги M і виникають катастрофічні переходи стану x системи.

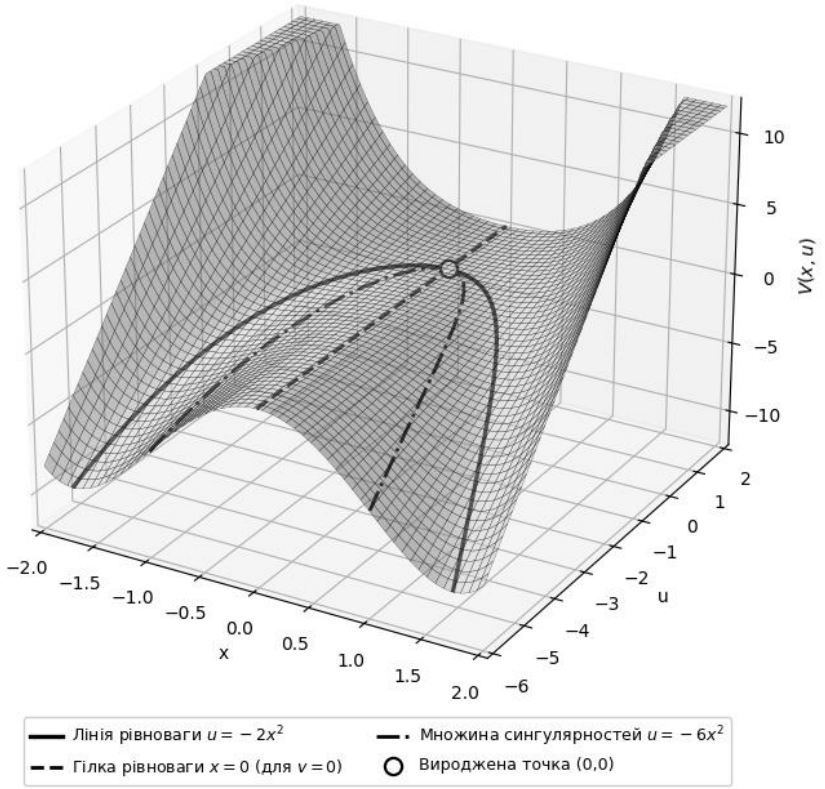


Рис. 2.6 Геометричне представлення катастрофи типу збірки для потенціалу

$$V(x) = x^4 + ux^2 + vx$$

Розглянемо катастрофу з трьома параметрами керування, функція потенціалу якої має вигляд

$$V(x) = x^5 + ux^3 + vx^2 + wx, \qquad (2.8)$$

де u, v, w – параметри керування, які визначають зовнішні умови впливу, x – змінна стану, що описує внутрішній стан системи. Дана потенціальна функція визначає канонічну форму потенціалу катастрофи типу *ластівчин хвіст.*

В свою чергу поверхня рівноваги M задається рівнянням

$$5x^4 + 3ux^2 + 2vx + w = 0, \qquad (2.9)$$

а множина сингулярностей S має рівняння

$$20x^3 + 6ux + 2v = 0. \qquad (2.10)$$

Для геометричного представлення катастрофи типу *ластівчин хвіст* в роботі [58] запропоновано підхід. При цьому множина біфуркацій визначається як проекція множини сингулярностей S поверхні рівноваги, яка задається умовами

$$\frac{\partial V}{\partial x} = 0,$$
$$\frac{\partial^2 V}{\partial x^2} = 0,$$

при цьому змінна x розглядається як параметр, що визначає параметричне представлення поверхні біфуркацій у просторі параметрів керування C.

Важливо відмітити, що при різних значеннях параметрів керування, виникають критичні точки множини біфуркацій B, яка розбиває простір параметрів керування $C = (u, v, w)$ на підмножини з різною кількістю критичних точок.

Розглянемо рівняння множини сингулярностей S

$$\frac{\partial^2 V}{\partial x^2} = 20x^3 + 6ux + 2v = 0$$

та зафіксуємо переріз, який перетинає всі області простору параметрів керування $C = (u, v, w)$ при $v = 0, u < 0$, що спонукає до утворення біфуркацій.

Розглянемо рівняння стаціонарних точок

$$5x^4 + 3ux^2 + w = 0 \qquad (2.11)$$

та визначимо кількість критичних точок, які визначаються в залежності від знаку дискримінанту

$$\Delta = 9u^2 - 20w.$$

Маємо три можливі випадки:

1. Якщо $w > \frac{9u^2}{20}$ та $\Delta < 0$, то рівняння (2.11) не має дійсних коренів, що підкреслює відсутність критичних точок в (2.8).
2. Якщо $0 < w < \frac{9u^2}{20}$, $\Delta > 0$ та $x^2 > 0$, то рівняння (2.11) має два додатних коренів, що визначає наявність чотирьох критичних точок в (2.8), а саме два максимуми і два мінімуми.
3. Якщо $w < 0$ та x^2 має різні знаки, то рівняння (2.11) має дві критичні точки, а саме максимум і мінімум.

Геометричне представлення катастрофи типу *ластівчин хвіст* побудовано за допомогою Python та представлено на Рис. 2.7.

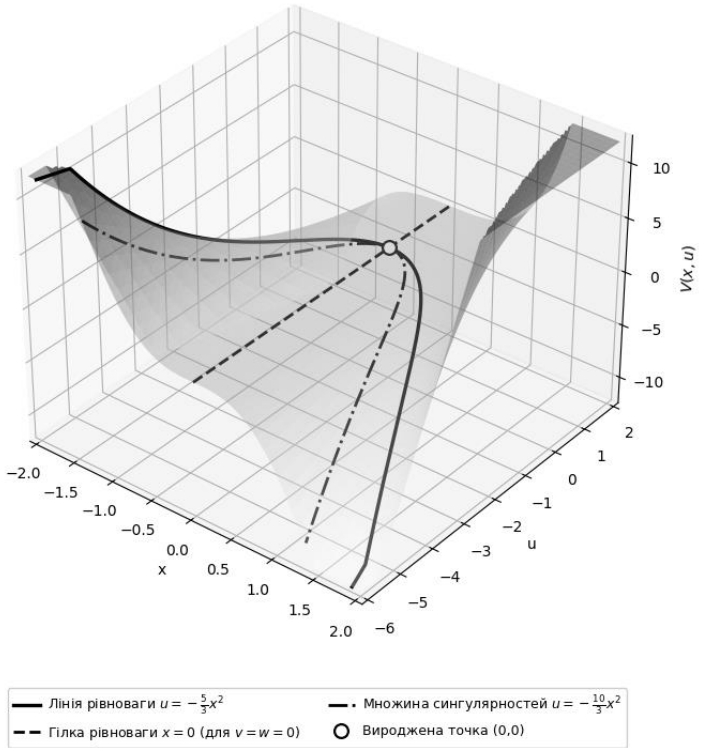


Рис. 2.7 Геометричне представлення катастрофи типу ластівчин хвіст для потенціалу $V(x) = x^5 + ux^3 + vx^2 + wx$

За умови збільшення кількості параметрів керування доцільно розглянути катастрофу типу *метелик,* яка залежить від чотирьох параметрів керування і описує складну структуру множини біфуркації, а також дозволяє моделювати критичні переходи у складних інформаційних системах.

Розглянемо катастрофу типу метелик, функція потенціалу якої має вигляд

$$V(x) = x^6 + tx^4 + ux^3 + vx^2 + wx, \qquad (2.12)$$

де t, u, v, w – параметри керування, які визначають зовнішні умови впливу, а саме t – параметр метелика, зміна якого викликає форму біфуркаційної множини у вигляді метелика, u – визначає симетрію біфуркаційних кривих, v та w – виконують роль, як при катастрофі типу збірки, а x – змінна стану, що описує внутрішній стан системи.

Оскільки простір параметрів керування включає чотири параметри $C = (t, u, v, w)$, тому множину біфуркацій B доцільно дослідити через відповідні перерізи.

В свою чергу поверхня рівноваги M задається рівнянням стаціонарних точок

$$6x^5 + 4tx^3 + 3ux^2 + 2vx + w = 0, \qquad (2.13)$$

а множина сингулярностей S має рівняння

$$30x^4 + 12tx^2 + 6ux + 2v = 0. \qquad (2.14)$$

При $u = 0$ залежно від значень t біфуркаційна крива набуває різних форма, так при $t > 0$ біфуркаційна крива має форму збірки, а при $t < 0$ виникає катастрофа типу метелик з кількома особливими точками, де крива втрачає гладкість.

Параметри керування, які задають рівняння $\frac{dV(x)}{dx} = 0$, визначають стан функціонування системи. Якщо існує один дійсний корінь x_1 рівняння (2.13), який задовольняє рівняння $\frac{d^2V(x_1)}{dx^2} > 0$, то система має стан рівноваги, а саме мінімум потенціалу. Якщо рівняння (2.13) має три дійсні корені x_1, x_2, x_3, для яких виконується умова

$$\frac{d^2V(x_1)}{dx^2} > 0, \frac{d^2V(x_2)}{dx^2} < 0, \frac{d^2V(x_3)}{dx^2} > 0,$$

тоді існують два стани рівноваги, як мінімум потенціалу, а також один стан нестійкої рівноваги, як максимум потенціалу. Також можливий випадок існування п’яти дійсних коренів, при яких три корені відповідають станам рівноваги і два – нестійким [58].

Геометричне представлення катастрофи типу *метелик* побудовано за допомогою Python та представлено на Рис. 2.8.

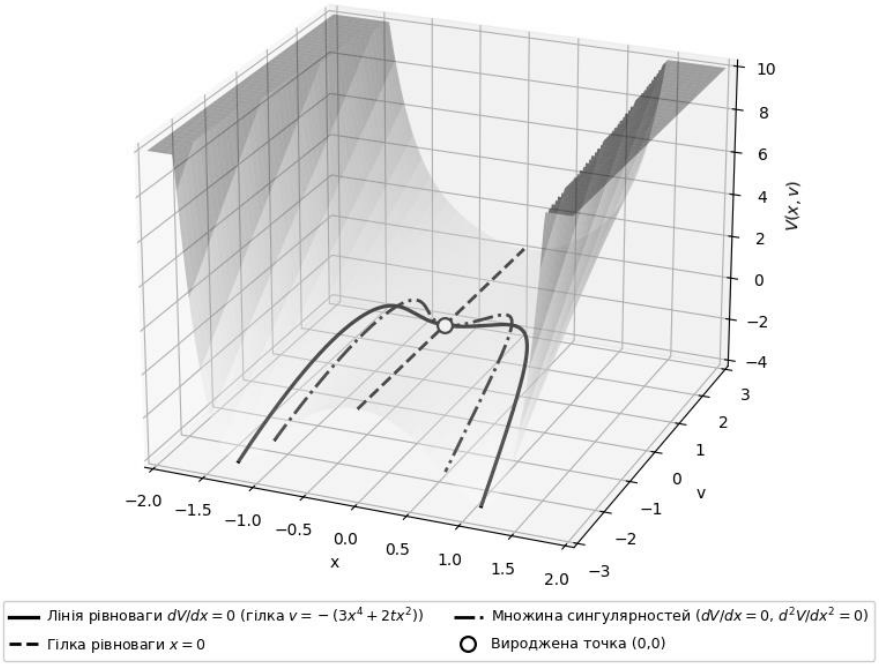


Рис. 2.8 Геометричне представлення катастрофи типу метелик для потенціалу

$$V(x) = x^6 + tx^4 + ux^3 + vx^2 + wx$$

Таким чином, розгляд геометричних типів елементарних катастроф дозволяє показати комплексне дослідження динамічних систем кіберзахисту та перейти до формування прикладних математичних моделей, які здійснюють аналіз, прогнозування та попередження критичних впливів кіберінцидентів у військових інформаційних системах.

2.2. Теорія конфліктів у задачах кібербезпеки військових інформаційних систем

Динаміка розвитку сучасних збройних сил суттєво змінює характер вимог щодо професійно важливих якостей військовослужбовців, ставить нові завдання щодо їх компетентності. Аналіз досвіду навчань та заходів підготовки особового складу збройних сил провідних країн світу показує, що широке впровадження сучасних інформаційних технологій та засобів імітаційного моделювання у систему бойової та оперативної підготовки дозволяє досягти значного зниження фінансових витрат при одночасному підвищені якості підготовки військ. При цьому командно-штабні навчання з використанням систем імітаційного моделювання стали найефективнішою формою підготовки командувачів (командирів) та органів управління всіх рівнів.

2.2.1. Імітаційне моделювання інформаційних конфліктів у військових системах

Високий рівень інтенсивності навчально-бойової діяльності забезпечується, насамперед, за рахунок застосування сучасних систем моделювання бойових дій, які дають змогу командирам та штабам відпрацювати навчальні завдання із залученням мінімально необхідної кількості особового складу, техніки та коштів. За рахунок моделювання майбутніх дій командирам в ході навчань надається можливість виявити системні проблеми та помилки,

проаналізувати їх, вивчити та вдосконалити результати рішень шляхом багаторазових повторень та тренувань із самокритичним підходом. Сучасні інформаційні технології дозволяють проводити командно-штабні навчання у форматі, де динаміка бойових дій моделюється і відображається в масштабі реального часу на робочих стаціях системи імітаційного моделювання відповідно до прийнятих рішень. Але виникають конфлікти взаємодії відповідних підсистем в цілому.

Сутність командно-штабних навчань полягає в тому, щоб за допомогою об'єднання систем імітаційного моделювання на всіх рівнях підготовки військовослужбовців, забезпечити виконання всіх функціональних обов'язків за посадою із зосередженням зусиль на конкретних блоках відповідальності (Рис.2.9).

Сучасні військові системи імітаційного моделювання вимагають створення програмного забезпечення, яке б надало можливість об'єднати всі системи імітаційного моделювання в одну базу даних в реальному часі, а також забезпечити їх безконфліктну взаємодію. Аналіз останніх досліджень і публікацій показав, що моделюванню навчальної діяльності з метою формування та розвитку практичних навичок курсантів (студентів) присвячена велика кількість наукових наробок. Так, у системі інформаційної безпеки дослідження [75] присвячене питанню формування криптографічних навичок студентів, робота [76] описує діяльність студентів у віртуальній лабораторії кібербезпеки.

Науковці у роботі [77] пропонують застосувати міждисциплінарний підхід до формування практичних навичок кібербезпечників. У дослідженні [78] розглянуто програмне забезпечення для імітаційного моделювання, перевірка достовірності та перевірка правильності моделей та також моделювання вхідних даних. Потрібно відмітити, в даній роботі відсутні питання взаємодії у реальних умовах із застосуванням інформаційно-комунікаційних технологій.

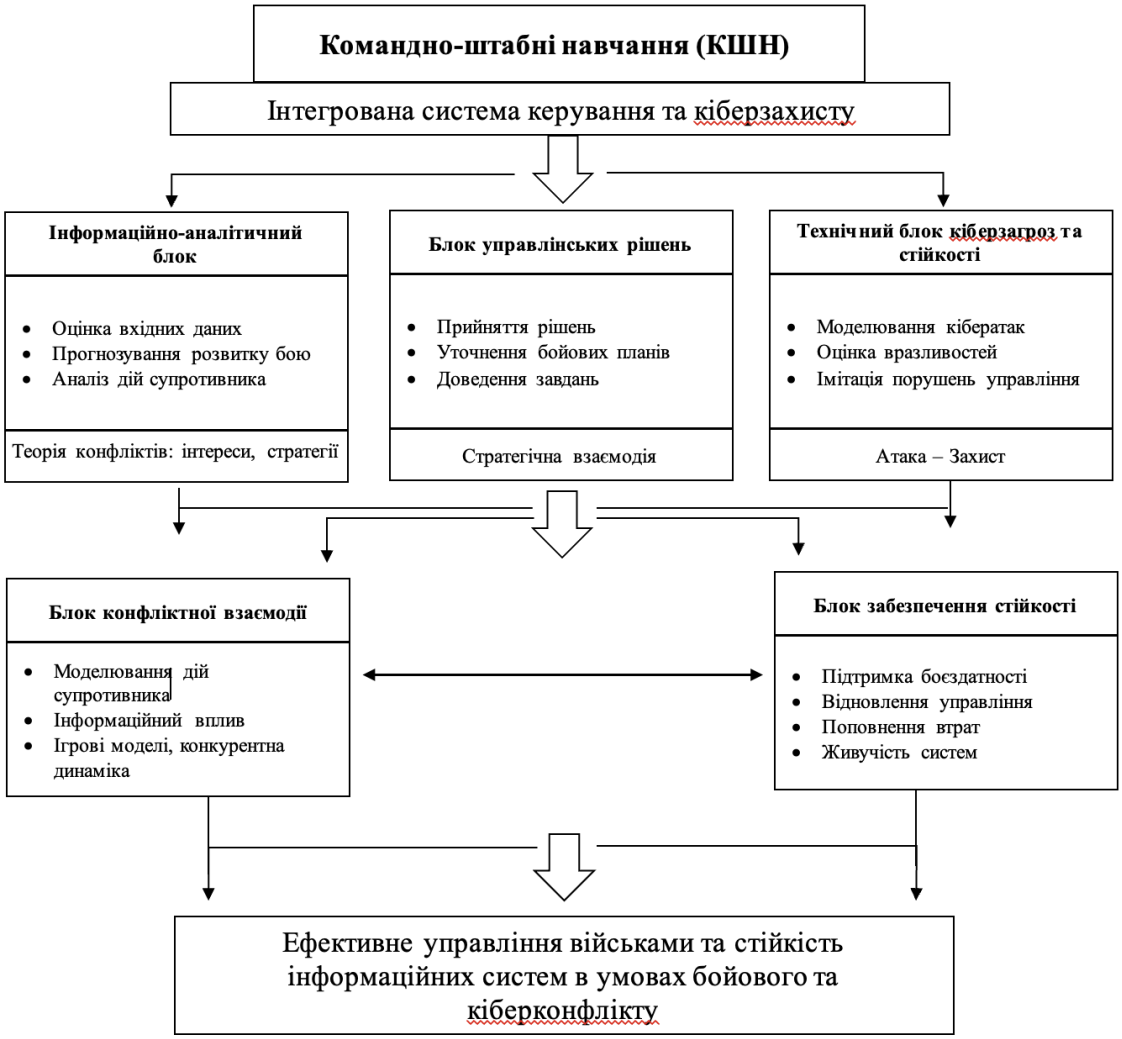


Рис.2.9 Схема взаємодії підсистеми управління в системі імітаційного моделювання на всіх рівнях підготовки військовослужбовців

У статті [79] розкривається питання створення інтегрованої навчально-тренувальної системи оперативної та бойової підготовки військ, що відповідає основним вимогам функціонування Збройних Сил України. У роботі О. Майстренко [80] та Л. Заїка [81] висвітлено питання застосування засобів імітаційного моделювання у процесі підготовки майбутніх офіцерів ЗСУ до виконання службових обов'язків, але при цьому не розкрито технічну реалізацію даних систем. Таким чином, результати огляду наукових наробок свідчать про те, що дана тема є важливою, наразі актуальною. Тому для вибору математичних та

програмних підходів важливим є аналіз сучасних інформаційних технологій, які дозволяють проводити командно-штабні навчання у форматі, де динаміка бойових дій моделюється і відображається в масштабі реального часу на робочих станціях системи імітаційного моделювання відповідно до прийнятих рішень, та визначення інформаційних конфліктіву таких системах [81].

Одним із інструментом покращення результативності підрозділів на полі бою, є застосування систем імітаційного моделювання на будь-якому рівні підготовки військовослужбовців. Організація бойової підготовки у збройних силах США базується на використанні методики Crawl-Walk-Run«повзти-ходити-бігти». Ця методика від простого до складного надає змогу військовослужбовцям покращувати індивідуальні навички і здатність виконувати колективні завдання по мірі виконання календарного плану тренувань підрозділу. Такий метод забезпечує на кожному тренувальному етапі необхідний рівень навченості для переходу на наступний, більш складний рівень. Але підхід до проведення всіх заходів підготовки підрозділу в умовах наближених до реальних не завжди можливий. Обмежені ресурси та час вимагають від командирів креативності, розроблення інноваційних методик проведення тренувань в умовах відмінних від реальних. Досвідчені командири планують та проводять тренування з різними за рівнем управління підрозділами, де поєднується необхідна та оптимальна підготовка у набутті навичок виконувати декілька основних завдань за призначенням. Після розроблення плану дій важливо звертати увагу на те, як проводиться тренувальний захід. В ідеалі, зважаючи на обмежений час і ресурси, всі тренувальні заходи підрозділу краще проводити в умовах, що наближені до реальних. Сучасна технологія моделювання дозволяє бійцям брати участь у безперервному циклі навчання, щоб підтримувати високу бойову готовність, використовуючи економічно ефективні альтернативи моделювання в поєднанні з операціями в реальному часі та навчальними місіями. У США поточний розвиток живих, віртуальних і конструктивних систем Live-Virtual-Constructive (LVC) [79] для тренувань і репетицій місій, а також швидкий розвиток мережевих технологій і

стандартів/архітектур протоколів сприяли створенню синтетичного середовища, де об’єднуються розподілені операції з кількома силами та навчання коаліції стали повсякденною реальністю.

На Рис.2.10 представлена система Live-Virtual-Constructive(LVC), яка складається з трьох складових:

1. На етапі *Live* реальні люди використовують реальні зразки озброєння. Військовослужбовці тренуються на тактичному полі з використанням системи лазерної імітації стрільби (типу MILES). Система імітує знищення противника та навпаки. Призначена для підготовки військовослужбовця під час тактичних занять (навчань).

2. На етапі *Virtual* реальні люди використовують віртуальні зразки ОВТ. Військовослужбовці тренуються на комп’ютерній програмі (типу VBS-3). Система імітує виконання завдань в складі невеликого підрозділу (до роти). Призначена для підготовки молодшого командного складу та підготовки військовослужбовців для їхніх спільних дій у складі підрозділу.

3. На етапі *Constructive* віртуальні люди використовують віртуальні зразки ОВТ. Система використовує математичні розрахунки дій військовослужбовців та ОВТ на місцевості. Дозволяє готувати штаби тактичного рівня, для яких важливо обробляти велику кількість інформації, що інтенсивно приходить з поля боюз метою вироблення рішень.

Таким чином, зв'язок між системами імітаційного моделювання та організацією індивідуальної та колективної підготовки є постійним і невід’ємним процесом тренування військ. Використовуючи практичний підхід до підготовки підрозділів, з залученням систем імітаційного моделювання, підрозділ може одночасно проходити підготовку у реальному та синтетичному середовищі (Synthetic), де Synthetic ─ це комп’ютерне середовище, яке доповнює здобуття реальних навичок особового складу та командного складу шляхом імітації активних об’єктів (entities) та проєкціонування їхніх дій на реальні об’єкти (ОВТ та особовий склад).

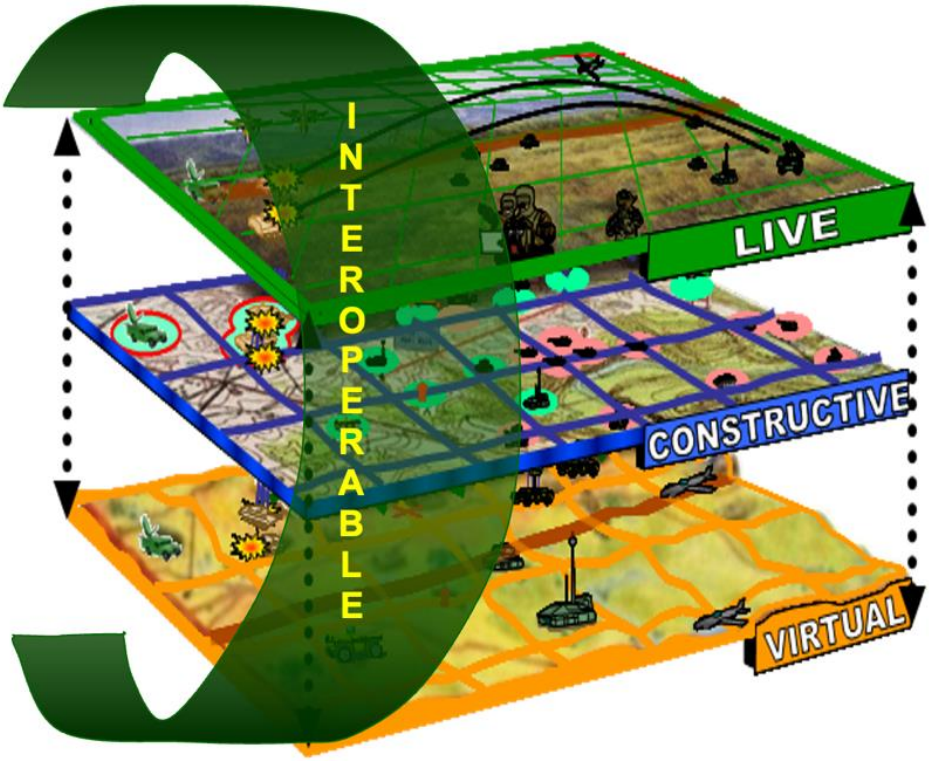


Рис.2.10 Система Live-Virtual-Constructive

Враховуючи досвід проведення підготовки підрозділів ЗС України у Навчальному Центрі підготовки (далі НЦПП) підрозділів на базі МЦМБ протягом 2015-2021років, а також навчальних центрів країн-партнерів (зокрема ЗС США) вирішено удосконалити систему підготовки підрозділів ЗС України у НЦПП шляхом нарощування можливостей систем імітаційного моделювання та об'єктивного контролю ведення бойових дій, а саме використання системи HOME STATION INSTRUMENTATION TRAINING SYSTEM (HITS) із забезпеченням безпечної передачі даних до віддалених командних точок [80]. HITS -це мобільна система, яка здатна покращити колективну підготовку підрозділів в режимі реального часу на стаціонарних станціях. HITS надає можливість командирам підрозділів та призначеним спостерігачам-контролерам-тренерам (ОС-Т) для надання зворотного зв'язку з навчальними підрозділами за допомогою автоматизованих систем. HITS - це інтегрована система обчислювальних

пристроїв, цифрових дисплеїв карт, радіоприймачів на основі GPS, лазерних модельованих засобів залучення та реле бездротового зв'язку, які виробляють, записують та подають дані, голосові та відео файли (Рис.2.11).

Дані щодо результатів підготовки необхідно використовувати під час проведення підсумків. Система HITS повністю інтегрована з реальною, віртуальною та конструктивною системою бойового середовища типу JCATS, VBS-3, MILES, LAZERTAG, бойової системи управління тактичної ланки «КРОПИВА», системи відображення повітряної обстановки АРМ «ВІРАЖ-ПЛАНШЕТ». Система HITS надасть змогу проводити підготовку в Інтегрованому тренувальному середовищі LVC (Live, Virtual, Constructive) (Рис. 2.12).

Live (реальне середовище) - підрозділи займаються на штатному ОВТ:

- ТН з залученням підрозділу позначення противника, MILES, LASERTAG)

- ТН з бойовою стрільбою.

Virtual (віртуальне середовище) підрозділи (штаби) займаються у віртуальному середовищі:

- VBS-3 та аналоічні системи;

- динамічні тренажери, які діють в одній мережі (просторі).

Constructive (конструктивне середовище) командири підрозділів (штаби) керують віртуальними підрозділами відповідно ОШС**:**

- система імітаційного моделювання JCATS;

- бойова система управління тактичної ланки «КРОПИВА»;

- система відображення повітряної обстановки АРМ «ВІРАЖ-ПЛАНШЕТ»;

- WARSIM (США).

Рис. 2.11 Структурна схема інтегрованого тренувального середовища

При такому поєднанні компонентів в інтегрованому тренувальному середовищі виникає ряд проблем.

Одна з них – наявність інформаційних конфліктів між компонентами системи. Підходи до визначення інформаційного конфлікту були досліджені у роботі [82]. Ми згодні з вченими [83-88], які пропонують в поняття інформаційний конфлікт (кіберконфлікт) вкладати процес зіткнення сторін на етапах збору, формування, передачі, зберігання, обробки, подання та інтерпретації інформації про стан, наміри та дії.

Інформаційні конфлікти як конфлікти в інформаційних системах між впровадженими програмами або у телекомунікаційних системах між радіоелектронними засобами та системами безпеки лежать в основі системи інтегрованого тренувального середовища. Важливо розділи конфлікти процесів, внутрішньомережні конфлікти, конфлікти між програмним забезпеченням та програмами, що здійснюють захист інформації та соціальні конфлікти.

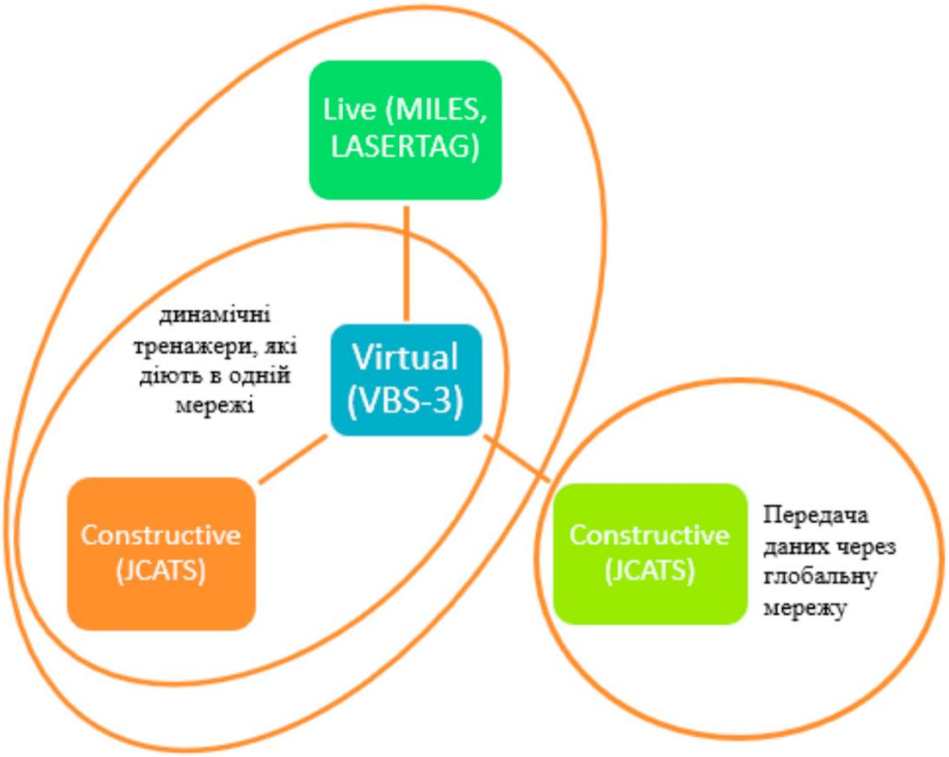


Рис. 2.12 Інтегроване тренувальне середовище LVC

При побудові системи інтегрованого тренувального середовища необхідно враховувати наступні чинники:

- вивчення динаміки кожного із конфліктів;

- визначення впливу кожного конфлікту та впливу сумарної взаємодії даних конфліктів на розвиток системи;

- створення математичної моделі функціювання системи в умовах конфлікту (або конфліктів);

- управління конфліктами у даній системі.

Якщо конфлікт переростає в активну стадію, коли виникають різкі зміни та стрибкоподібні процеси, що пов’язані з інцидентами у інформаційній та кібернетичній безпеці, є логічним застосувати положення теорії катастроф [58].

2.2.2. Кіберконфлікт як складна нелінійна динамічна система

У сучасних військових інформаційних системах кібербезпека є цілісною керованою системою, яка відповідає за реагування на загрози, які в свою чергу провокують кіберконфлікти. Тому кіберконфлікт доцільно розглядати як динамічний процес, який впливає на систему управління інформаційною безпекою під дією зовнішніх факторів впливу [80,81].

Основними елементами системи управління інформаційною безпекою (СУІБ) виступають засоби прогнозування, реагування та виявлення кіберінцидентів (IDS/IPS, SIEM, SOC), протоколи безпеки та відновлення, а також оператори та аналітики. Дана система є складною динамічною системою керування, в якій кіберінциденти відіграють роль зовнішніх збурень, засоби прогнозування, реагування та виявлення кіберінцидентів є підсистемою спостережень і керувань, а поточний рівень безпеки визначає стан системи в момент реагування на кіберзагрози [82,83].

В роботах [84,85] дані системи розглядаються зі сторони кіберстійкості стану даних систем, а саме важливими є переходи між станами (нормальний, деградації, адаптації та відновлення), під час реагування на кіберінциденти, що змінюють стан всієї інформаційної системи.

Стан системи управління інформаційною безпекою позначають через змінну $x(t)$, яка описує рівень захисту, доступ до сервісів, цілісність даних та функціонування критичних функцій.

Зміна стану системи під впливом кіберконфліктів задається рівнянням

$$\frac{dx}{dt} = f(x(t), u_A(t), u_D(t), \xi(t)) \qquad (2.15)$$

де вектор керування атакою

$$u_A(t) = \begin{bmatrix} \lambda(t) \\ \alpha(t) \\ \upsilon(t) \end{bmatrix}$$

задає активність кіберінцидентів, де $\lambda(t) \geq 0$ відповідає за інтенсивність атак (частота подій), $\alpha(t) \in [0,1]$ – за міру складності технік, а $\upsilon(t) \in \{1, \ldots, V\}$ вибирає вектор атаки серед можливих типів. Дані типи атак використовують при побудові стохастичних та ігрових моделях [86,87].

До складу рівняння (2.15) входить вектор захисту системи

$$u_D(t) = \begin{bmatrix} m(t) \\ r(t) \\ p(t) \end{bmatrix},$$

який визначає, як реагує система управління інформаційною безпекою на кіберінциденти, та визначається $m(t) \in [0,1]$, який показує інтенсивність виявлення змін (SIEM кореляція), $r(t) \in [0,1]$ – інтенсивність реагування, а $p(t)$ визначає рівень захисту (ізоляція та блокування критичних зон). Всі зазначені параметри дозволяють системи тривалий час боротися з тривалими кібератаками [88,58].

За стохастичний вплив на систему у рівнянні (2.15) відповідає параметр $\xi(t)$, який показує помилки спостереження та прийняття рішень, що виникають при виявлені помилки кореляції подій чи затримці в аналізі кіберінцидентів і, звичайно, вплив людського фактору. Саме тому при побудові моделей кібербезпеки враховують всі зазначені стохастичні параметри [58].

Важливо відмітити, що всі процеси реагування на кіберінциденти в системі управління інформаційною безпекою поділяють на процеси, які виявляють інциденти, а саме збирають телеметрії з хостів, мереж чи додатків, формують події в IDS/IPS чи SIEM, виправлення подій чи відкидання хибних дій. Також виділяють процеси, що аналізують та здійснюють класифікацію інцидентів через аналіз

журналів подій, тип атак, їх джерел виникнення, а також надають рівні реагування в підсистемі SOC (Security Operations Center) системи управління інформаційною безпекою, який відповідає за моніторинг, виявлення, аналіз і реагування на кіберінциденти. Важливими є процеси прийняття рішень, які відповідають за вибір сценарію реагування, а саме за ізоляцію вузла чи блокування трафіку. На останок доцільно відмітити процеси, що відповідають за захист всієї системи і реалізуються через відключення облікових записів або відновлення даних з резервних копій. Всі зазначені процеси в сукупності описують повну затримку реагування системи на інциденти, яка задається

$$\tau = \tau_1 + \tau_2 + \tau_3, \qquad (2.16)$$

де τ_1 – час виявлення інциденту, τ_2 – час аналізу та прийняття рішення, τ_3 – час створення захисної дії.

Враховуючи (2.16) рівняння (2.15) набуває вигляду

$$\frac{dx}{dt} = f(x(t), u_A(t), u_D(t-\tau), \xi(t),$$

де τ – час затримки. В роботах [69]-[70] показано, що незначна затримка τ призводить до порушення стійкості системи.

Всі зазначені особливості дозволяють поняття кіберконфлікту в системах управління інформаційною безпекою досліджувати як складну нелінійну динамічну систему, яка залежить від впливу часових параметрів та стохастичних збурень, і вимагає подальшого вивчення стійкості станів системи, виявлення критичних областей переходу даних станів, а також побудови моделей та методів для забезпечення стійкості системи управління інформаційною безпекою.

2.2.3. Математичні моделі взаємодії сторін у кіберконфліктах

У сучасних військових інформаційних системах кіберконфлікт розглядають як нелінійну динамічну систему (2.15), яка залежить від впливу зовнішніх та внутрішніх факторів, випадкових збурень, а також реального стану системи у відповідний момент часу. Саме тому важливо розглядати не поточний стан системи, а особливу увагу приділити тому, як система реагує на дії двох сторін, а саме сторони атаки та відповідно захисту.

Для дослідження даних кіберконфліктів існує ряд математичних підходів, які дозволяють описати взаємодію даних сторін за певних умов під впливом кіберінцидентів.

В роботі [71], [72] запропоновано теорію диференціальних ігор, за допомогою якої зміни в стані системи можна представити за допомогою нелінійного диференціального рівняння (2.15). При погіршені стану системи під дією кіберінцидентів сторона захисту має зменшити інтеграл ризику, який задано формулою

$$J_d(u_d, u_a) = \int_0^T L(x(t), u_d(t))dt + \Phi(x(t)),$$

де $L(x, u_d)$ – функція ризику, яка зростає при зміні стану системи, $\Phi(x(t))$ – функція, що вказує на наявність критичного стану системи.

Сторона атаки навпаки має збільшити даних інтеграл, тобто

$$J_d(u_d, u_a) = -J_d(u_d, u_a).$$

Таким чином мінімізація ризиків за умов кіберконфліктів досягається за умови знаходження

$$\min_{u_d} \max_{u_a} J_d(u_d, u_a),$$

при цьому функція зміни стану системи, що задається рівнянням Гамільтона-Якобі

$$-\frac{\partial \mathrm{V}}{\partial \mathrm{t}} = \min_{\mathrm{u_d}} \max_{\mathrm{u_a}} [\mathrm{L}(\mathrm{x}, \mathrm{u_d}) + \nabla \mathrm{V}^{\mathrm{T}} \mathrm{f}(\mathrm{x}, \mathrm{u_d}, \mathrm{u_a}, \mathrm{t})], \qquad \mathrm{V}(\mathrm{x}, \mathrm{T}) = \Phi(\mathrm{x}),$$

де $\nabla V(x,t)$ – градієнт функції зміни стану і вказує на залежність рівня ризику від зміни стану системи, а саме втрати стійкості досліджуваної системи, спостереження біфуркацій при інтенсивності впливу кіберінцидентів або появи різких переходів між станами системи, що є важливим для аналізу критичних станів.

В роботах [62], [68], [74] для побудови системи підтримки прийняття рішень, які дозволяють автоматизувати процеси виявлення чи прогнозування кіберінцидентів, запропоновано підхід, що базується на стохастичних процесах та марковських іграх. При цьому інформаційна система задається множиною станів

$$s_k \in S, \;\; t = 0,1,2,\ldots,$$

де зміни в стані системи в момент часу $t+1$ задається ймовірністю

$$P(s_{t+1} | \, s_t, u_d, u_a)$$

та функцією зміни стану системи

$$r(s_t, u_d, u_a),$$

яка кількісно показує зміни в стані s_t, а саме рівень змін в стані системи.

При всіх перевагах, даний підхід відображає окремі кроки зміни в системі, але не зміни системи в цілому, зокрема втрати стійкості, виявлення критичних станів, що не дозволяє здійснювати прогнози критичних станів.

В роботах [71]-[74] для прогнозування та виявлення кіберконфліктів в системах управління інформаційною безпекою запропоновано використовувати байєсівські моделі, стохастичні ігри та методи машинного навчання, які в свою чергу мають недоліки, а саме не вивчають питання стійкості систем та наявності критичних переходів між станами при реагуванні на кібератаки (Таб.2.1).

Таблиця 2.1

Математичні підходи для моделювання кіберконфліктів в СУІБ

Математична модель	*Основний підхід*	*Недоліки*
Диференціально-ігрові моделі	Динаміка системи розглядається через нелінійні диференціальні рівняння та оптимізацію взаємодії сторін системи	Складність знаходження розв'язків; не розглядаються умови втрати стійкості системи
Стохастичні моделі	Динаміка системи розглядається через випадкові процеси	Статистичні методи для аналізу змін в динаміці системи
Марковські ігри	Дискретні описи станів системи	Досліджуються локальні переходи, в цілому стан системи не розглядається
Байєсівські моделі	Стан системи досліджується в окремих точках за інформаційної невизначеності	Складність в обчисленнях, проводиться лише оцінка системи, але не розглядаються зміни в станах системи
Методи машинного навчання	Використовують навчання на даних для прогнозування кіберінцидентів	Відсутня аналітична модель
Мережеві моделі	Досліджуються загрози в складних мережах	Висока залежність від параметрів, що не завжди дозволяє оцінити переходи в станах системи

Проведений аналіз зазначених підходів показав, що всі вони не враховують внутрішню структуру нелінійної динаміки системи, а саме не виявляють втрату стійкості системи, виявлення біфуркаційних явищ, а також не виявляють переходи між станами функціонування систем під впливом кіберінцидентів.

2.3. Математичні засади кластеризації загроз та уразливостей в інформаційних системах

Сучасні системи управління інформаційною безпекою фіксують велике зростання кількості та різновидів кіберзагроз, які змінюють свою внутрішню структуру, а також умови впливу їх на інформаційні системи. Для розробки та удосконалення систем інформаційної та кібернетичної безпеки доцільно використовувати математичні моделі з використанням інформаційних технологій [89]. Математичні методи та технології є підґрунтям для створення та покращення показників у сфері захисту інформації [90-95]. Сучасний стан потребує такі методи, які б дозволили прораховувати та прогнозувати можливі ризики використання загрозами уразливостей інформаційних активів з метою забезпечення конфіденційності, цілісності та доступності інформації. Обробка ризиків буде результативною, якщо ефективним буде процес аналізу, ідентифікації та оцінки ризиків. Для інформаційних та кібернетичних систем властива якісна оцінка ризиків, яка здійснюється на основі експертних оцінок фахівців. І хоча ця процедура містить математичну обробку цих оцінок, обчислюється узгодженість експертів, проте існує висока ймовірність отримати даний результат суб'єктивним. Для усунення даних похибок доцільно використовувати процес кластеризації загроз та уразливостей, ймовірностей настання ризиків інформаційної безпеки та ідентифікації методів захисту активів. Кластерний аналіз використовують для розбиття множини на підмножини, щоб елементи кожної підмножини були схожі між собою, а елементи різних підмножин були найбільш відмінними, в результаті чого маємо можливість працювати з більш зв'язними, вузькими і конкретними даними. Таким чином, виділення окремих кластерів кіберзагроз дозволить класифікувати об'єкти безпеки для подальшого формування бібліотек типових класів кіберінцидентів. Кожен клас даних загроз описує характерні ознаки кіберінцидентів, їх інтенсивність впливу на інформаційну систему, а також можливі наслідки для критичних станів. Збір та аналіз

кіберінцидентів у окремі кластери дозволяє швидко реагувати на нові та модифіковані загрози, що в свою чергу забезпечує використання даних знань для автоматизованих систем підтримки прийняття рішень, SIEM-системах, а також для прогнозування зміни станів кіберстійкості та виникнення критичних переходів в інформаційних системах.

2.3.1. Формування множини ознак загроз та уразливостей у військових інформаційних систем

Розглянемо множину категорій кіберінцидентів [89], яка задається

$$\mathrm{C} = \{\mathrm{C}_1, C_{2,}\ldots, C_{10}\},$$

C_k – категорії кіберінцидентів містять множину підкатегорій C_j^k. При цьому E_i – зафіксовані кіберінциденти, які відносять до відповідних категорій та підкатегорій, тобто

$$E_i \in C_j^k,\ i = 1,\ldots n,$$

де n – кількість інцидентів за час t_i.

Відповідно кіберзагроза розглядається як сукупність кіберінцидентів відповідної категорії зі спільними властивостями та умовами впливу на інформаційну систему.

Відповідно множина кіберзагроз, що діють на військову інформаційну систему задається рівнянням

$$Z = \{Z_1, Z_2, \ldots, Z_m\},$$

де m – кількість зафіксованих кіберінцидентів на інтервалі часу $[t_0, t_1]$, Z_i – кіберзагроза, що визначається формулою

$$Z_i = \bigcup_{n \in L_j} E_{n,}\ L_j \subseteq \{1, \ldots, K\}.$$

Відповідно до сучасних моделей опису кіберзагроз [96], [97] Z_i доцільно представити у вигляді сукупності відповідних параметрів впливу, а саме

$$Z_i = \{c_i, \alpha_i, v_i, t_i\}, \quad (2.17)$$

де $c_i \in \{0,1\} -$ належність до відповідної категорії [89], α_i $-$ параметри активності кіберзагрози, а саме частоти

$$f_i^k = \frac{|\{E_i \in Z_i : E_i \in C^k\}|}{N_i}, k = 1, \dots, 10,$$

де C^k- категорія кіберінцидентів [89]. Частота f_i^k показує періодичність повторення кіберзагрози та використовується з показником інтенсивності кіберзагрози λ_i, який задається як

$$\lambda_i^w = \frac{1}{t_1 - t_0} \sum_{l \in L_j} w_c(l),$$

де $w_c(l)$ $-$ваговий коефіцієнт, який вказує на відповідну категорію інциденту E_l [89, 49]. Характеристики уразливостей і конфігураційних помилок v_i, відповідно до стандарту управління ризиками [49] надають інформацію про кількість та тип експлуатованих уразливостей, а також про рівень критичності потенційного впливу на систему. Ще одним важливим параметром, що характеризує кіберзагрозу Z_i відповідно до [49] множина t_i, що включає час інтенсивності, тривалості, регулярності та пікових стрибків, можна задати формулою

$$t_i = (t_i^s, t_i^p, \Delta t_i, f_i, \beta_i, k_i) \in R^6,$$

де t_i^s $-$ початковий час виявлення кіберзагрози, $t_i^p -$ час завершення кіберзагрози, $, \Delta t_i = t_i^p - t_i^s$ вказує на тривалість кіберзагрози, $f_i -$ частота появи кіберінцидентів, $\beta_i -$ інтенсивність дії кіберзагрози у момент часу Δt_i, та k_i, що показує кількість кіберінцидентів у момент часу Δt_i та задається формулою

$$k_i = \frac{max_{1 \le r \le N}(n_{i,r})}{\frac{1}{N}\sum_{r=1}^{N} n_{i,r} + \varepsilon},$$

$n_{i,r} -$ кількість кіберінцидентів Z_i у $r -$ му вікні, де $r = 1, \ldots, N$. При цьому за умови $k_i > 1$ показує атаку кіберзагрози на інформаційну систему. Параметр t_i показує часову дію кіберзагрози та дозволяє фіксувати різницю між кіберзагрозами, які мають однакову кількість кіберінцидентів, але відрізняються параметрами інтенсивності β_i та частотою їх появи k_i. Важливість часових параметрів, що визначають кіберзагрози Z_i, розкриваються в подальшому при визначенні метрик подібності, визначення множини ознак та побудови кластерів кіберзагроз для задач моделювання кіберстійкості військових інформаційних систем.

У сучасних наукових дослідженнях [98], [99] для кількісного аналізу кіберзагроз вводять відображення

$$\varphi\colon Z \to X \subseteq R^n, \qquad x_i = \varphi(Z_i),$$

де $x_i = (x_{i1,} x_{i2}, \ldots, x_{in})$- вектор ознак. При цьому

$$x_{i,k} = \left|\{E_i \in Z_i \colon E_i \in C^k\}\right|, k = 1, \ldots, 10$$

описує кількість кіберінцидентів кожної категорії щодо відповідної кіберзагрози, а також включає параметри інтенсивності, частоти та величину впливу. Всі виявлені характеристики дозволяють формувати параметри впливу

$$\lambda(t) = \Phi(\{x_i(t)\}_{i=1}^{m}),$$

які визначають параметри керування динамічної системи управління інформаційною безпекою.

2.3.2. Метрики подібності кіберзагроз і уразливостей у військових інформаційних системах як основа кластерного аналізу

Векторне представлення множин ознак загроз та уразливостей (2.17) у військових інформаційних систем не дають можливість визначати сценарії реагування на них. Тому доцільно ввести метрики подібності кіберзагроз і уразливостей, щоб кількісно оцінювати їх подібність і відносити до одного класу ознаку.

Нехай кіберзагроза Z_i задається множиною характеристик

$$x_i(t) = (c_i, \alpha_i, v_i, t_i) \in X \subseteq R^n,$$

де c_i – визначає відповідну категорію кіберінциденту [89], α_i – інтенсивність і частота дії кіберзагрози в системі, v_i – параметри уразливостей і конфігураційних помилок системи, t_i – проміжок часу дії кіберзагрози. Саме залежність x_i від часу вказує, що кіберзагрози постійно змінюються в реальних умовах функціонування військових інформаційних систем.

Для того, щоб порівняти кількісні характеристики виявлених кіберзагроз, потрібно побудувати функцію відстані

$$d: X \times X \to R_+,$$

де X – множина ознак загроз і уразливостей, $d(x_i, x_j)$ дозволяє групувати кіберзагрози відповідно до їх спільник ознак і виступає метрикою, тобто для $\forall\, x, y, z \in X$ виконуються умови

1. $d(x, y) \geq 0$,
2. $d(x, y) = 0 \leftrightarrow x = y$,
3. $d(x, y) = d(y, x)$,
4. $d(x, z) \leq d(x, y) + d(y, z)$,

виконання яких дозволяє виділити кластери близьких за ознаками кіберзагроз [99]. Відповідно метрика дозволяє ввести $\varepsilon -$ окіл кіберзагрози $x_i \in X$ за допомогою множини

$$B_\varepsilon(x_i) = \{x \in X: d(x, x_i) \leq \varepsilon\},$$

яка визначає кластер подібних кіберзагроз, що дозволяє провести аналіз даних кластерів, які впливають на військову інформаційну систему. Для визначення радіусу кластера, відстані та меж між кластерами важливою є умова (4), яка вказує на те, що кластери утворюють групи загроз зі спільними сценаріями впливу. Симетричність метрики відповідно до умови (3) дозволяє не враховувати порядок при оцінці подібності загроз, а умова (2) забезпечує єдине представлення загрози у просторі ознак.

Для визначення відстаней доцільно нормувати ознаки для компонентів x_i, які мають різну розмірність, за законом

$$\tilde{x}_{ik} = \frac{x_{ik} - \mu_k}{\sigma_k}, k = 1, \dots, n,$$

де μ_k, σ_k $-$ оцінки математичного сподівання та стандартного відхилення певної ознаки. Нормування дозволяє відхилити перевагу окремих параметрів для визначення окремої метрики подібності [99].

Для опису кіберзагроз в стандартах [96,97] простір ознак загроз та уразливостей представлено за допомогою декартового добутку підмножин

$$X = X_c \times X_\alpha \times X_v \times X_t,$$

де X_c $-$ відповідність категоріям [89], X_α - показники активності загроз, X_v $-$ параметри уразливостей і конфігураційних помилок системи, X_t $-$ параметри часу дії кіберзагрози.

В цьому випадку застосовують композиційну метрику подібності

$$D(x_i, x_j) = \left(\sum_r \alpha_r d_r(x_i^r, x_j^r)^p \right)^{\frac{1}{p}}, \quad \alpha_r > 0,$$

де d_r – метрики на підмножинах, α_r – коефіцієнт впливу кожної групи ознак.

Потрібно також враховувати, що для військових інформаційних систем категорії кіберінцидентів мають різну критичність, тому важливо ввести систему ваг для категорій

$$\omega = (\omega_1, \omega_2, \ldots, \omega_{10}), \quad \omega_j > 0,$$

де ω_j визначає важливість однієї з категорій кіберінцидентів [89]. Важливість ваг категорій впливає на визначення критичних кіберінцидентів (втручання, порушення доступності системи), що мають найбільший вплив на метрику подібності при групуванні загроз.

Наступним кроком проводиться групування загроз за допомогою кластерного аналізу

$$\{x_i(t)\}_{i=1}^m \rightarrow \{C_1(t), C_2(t), \ldots, C_k(t)\}, \qquad k \ll m,$$

де кластер $C_k(t)$ відображає загрози, які мають спільні характеристики впливу на інформаційну систему. При цьому для кожного кластера визначається центроїд

$$\bar{x}_k(t) = \frac{1}{|C_k(t)|} \sum_{x_i(t) \in C_k(t)} x_i(t),$$

який є узагальненим вектором ознак.

В роботі [100] відзначено, що предметно-орієнтовані метрики розкривають практичну цінність результатів кластеризації, а в роботі [49] для моделювання кіберстійкості систем, вводиться поняття функціоналу пливу

$$I: X \to R_+,$$

який дозволяє оцінити ризики, які виникають у даних системах. При цьому має виконуватись умова

$$\left|\mathrm{I}(\mathrm{x_i}) - \mathrm{I}\left(\mathrm{x_j}\right)\right| \leq \mathrm{LD}(\mathrm{x_i}, \mathrm{x_j}), \mathrm{L} > 0,$$

яка забезпечує системний вплив загроз, що належать одному кластеру.

Метрики подібності кіберзагроз і уразливостей дозволяє групувати окремі загрози у кластери з подібними параметрами впливу на інформаційну систему та становлять математичну основу для удосконалення методу кластеризації загроз та уразливостей для побудови моделей кіберстійкості та прогнозування критичних переходів у військових інформаційних системах.

Висновки до розділу 2

1. Проведено аналіз математичної основи стійкості динамічних інформаційних систем на основі теорії катастроф. Встановлено, що інформаційні системи кіберзахисту мають складну нелінійну динамічну структуру, стан яких змінюється під впливом кібератак, внутрішніх збурень чи людських факторів.
2. Проведено моделювання сценаріїв втрати стійкості системи, наявності станів рівноваги та різких переходів між станами системи на основі елементарних типів катастроф, які дозволяють встановлювати критичні області, показують переходи в станах системи від нормального до порушення стійкості, що призводить до руйнування системи кіберзахисту.
3. Встановлено, що наявність біфуркаційних точок у нелінійних динамічних системах кіберзахисту визначають параметри, які показують інтенсивність атак, затримки в реагуванні чи рівень захисту та дозволяють прогнозувати появу катастрофічних змін в системі.

4. Проведено аналіз сучасних інформаційних технологій, які дозволяють проводити командно-штабні навчання у форматі, де динаміка бойових дій моделюється і відображається в масштабі реального часу на робочих стаціях системи імітаційного моделювання відповідно до прийнятих рішень. Запровадження даної моделі, що поєднує реальні, віртуальні та конструктивні системи бойового середовища для проведення командно-штабного навчання з залученням військ надасть можливість зменшити у декілька разів залучення озброєння та військової техніки, що, в свою чергу, скоротить кількість використання палива, боєприпасів та зменшить моторесурс техніки. Встановлено, що небезпечним для даного середовища є наявність конфлікту, що переростає в активну стадію, коли виникають різкі зміни та стрибкоподібні процеси, пов’язані з інцидентами у інформаційній та кібербезпеці. На даному етапі доцільно застосувати теорію катастроф забезпечення стійкості інформаційної системи.
5. Проведено аналіз математичних моделей кіберконфліктів, який показав доцільність поєднання теорії катастроф, теорії біфуркацій та кіберконфліктів для побудови нових методів та моделей забезпечення стійкості військових інформаційних систем, а також для виявлення та прогнозування кіберінцидентів.

РОЗДІЛ 3. РОЗРОБКА МОДЕЛЕЙ ТА МЕТОДІВ ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ ВІЙСЬКОВИХ ІНФОРМАЦІЙНИХ СИСТЕМ

3.1. Розробка математичної моделі на основі катастрофи типу «Метелик» для прогнозування критичних станів інформаційної системи

У сучасних умовах інформаційна безпека систем має вирішальне значення для ефективності та безпеки військових операцій. Однією зважливих завдань Збройних Сил України (ЗСУ) є здатність ефективно управляти інформаційною безпекою та забезпечувати безперервність дій, конфіденційність інформації та загальну оперативну ефективність як на полі бою, так і при здійсненні підготовки штабів (підрозділів). Система управління інформаційною безпекою (СУІБ) є важливим елементом захисту від можливих загроз і збоїв, яка піддається впливу різних внутрішніх і зовнішніх факторів, які можуть призвести до незворотних наслідків [101].

Можливі шляхи виявлення та попередження даних кіберзагроз пропонують науковці через удосконалення та пошук ефективних математичних методів та технологій, а також розробкою математичних моделей та їх застосування в інформаційних системах безпеки [59], [82], [90], [91], [95], [102]-[105]. Для дослідження даних наслідків доцільно розглянути математичну теорію катастроф, яка дозволяє аналізувати зміни стану системи через незначні флуктуації вхідних параметрів. За допомогою теорії катастроф здійснюється моделювання кризових ситуацій, проводиться оцінка рівня стійкості системи та фіксуються критичні точки, в яких система стає особливо уразливою до зовнішніх або внутрішніх впливів. Математичну основу теорії катастроф детально представлено в Розділі 2. Використання цього підходу при аналізі СУІБ для ЗСУ дозволяє краще зрозуміти, як система реагуватиме на різні сценарії атак і як уникнути можливих переходів у критичний стан [58].

3.1.1. Вхідні параметри математичної моделі впливу кіберінцидентів на стійкість систем на основі теорії катастроф

Теорію катастроф, як програму прогнозування нестійкості різних систем, використовують в задачах забезпечення захисту інформації [105]. В роботі [105] наведено історичний розвиток теорії катастроф, як розділу прикладної математики, що вивчає різні теорії для опису та аналізу складних систем, що залежать від зміни параметрів, які безпосередньо впливають на дані системи. Також зазначено, що математичний апарат теорії катастроф базується на теорії особливостей гладких відображень Х. Уітні, теорії стійкості та біфуркацій динамічних систем А. Пуанкаре, А. Ляпунова, А. Андронова, а також в дослідженнях Р. Тома, який у 1960-х роках описав дану теорію у дослідженні «Структурна стабільність і морфогенез». Наведено основні визначення, що використовуються для моделювання складних систем, типи елементарних катастроф, а також доцільність застосування даної теорії до систем, які можуть реагувати на зміни параметрів і переходити від стану рівноваги до іншого стану. Теорію катастроф, яка дозволяє виявляти зміни в поведінці складних систем через невеликі збурення, доцільно застосовувати для аналізу кіберінцидентів, які впливають на кіберстійкість системи управління безпекою [106]. Перелік категорій кіберінцидентів [89], який постійно оновлюється з урахуванням появи нових видів та типів, включає також опис даних інцидентів і їх вплив на інформаційну систему.

Відповідно до переліку категорій кіберінцидентів [89] розрізняють наступні типи:

1. Шкідливий (образливий) вміст (Abusive content):
    1.01. Спам (Spam).
2. Шкідливий програмний код (Malicious Code):
    2.01. Зараження шкідливим програмним забезпечення (Malware infection).
    2.02. Розповсюдження ШПЗ (Malware distribution).

2.03. Командно-контрольний центр (C2) (Command & Control (C2)).

2.04. Шкідливе підключення (Malicious connection).

3. Збір інформації зловмисником (Information Gathering):

3.01. Сканування (Scanning).

3.02. Сніфінг (Sniffing).

3.03. Фішинг (Phishing).

4. Спроби втручання (Intrusion Attempts):

4.01. Спроба експлуатації уразливості (Vulnerability exploitation attempt).

4.02. Спроби авторизації/входу в систему (Login attempts).

5. Втручання (Intrusion):

5.01. Компрометація облікового запису (Account compromise).

5.02. Компрометація системи (System compromise).

6. Порушення доступності (Availability):

6.01. Атака на відмову в обслуговуванні (DoS/DDoS).

6.02. Саботаж шкідливі дії (Sabotage).

6.03. Збій (Outage, no malice).

7. Порушення властивостей інформації (Information Content Security):

7.01. Несанкціонований доступ до інформації (Unauthorised access toinformation).

7.02. Несанкціонована модифікація (Unauthorised modification of info).

8. Шахрайство (Fraud):

8.01. Шахрайський сайт (Fraudulent site).

9. Відома вразливість (Vulnerable):

9.01. Вразливість (Vulnerability).

9.02. Некоректна конфігурація (Misconfiguration).

10. Інше (Other):

10.01. Невизначений інцидент (Undetermined incident).

Збір та аналіз кіберінцидентів дозволяє розробити профілі загроз, щоб протидіяти їм у майбутньому, а також виявляти аномалії, які вказують на інцидент у реальному часі та вжити заходів для протидії атакам до їх початку. Важливо проводити оцінку вразливих місць інформаційної системи та підвищити її рівень кіберстійкості з урахуванням частоти, інтенсивності і типу атак, а також оцінити ризики, а саме розробити та протестувати плани реагування на інциденти, які швидко змінюються та адаптуються до нових умов. У свою чергу, використання даних інцидентів у поєднанні з теорією катастроф дозволяють дослідити раптові зміни в поведінці інформаційної системи, виявити точки, в яких система переходить з нормального до критичного стану, а також встановити пороги критичних змін, які можуть призвести до збоїв в даній системі [58].

Всі зазначені типи кіберінцидентів складають множину вхідних параметрів для побудови математичної моделі, оскільки вони визначають основні параметри впливу на інформаційну систему. Доцільно виділити саме ті типи, які мають найбільший вплив на стійкість системи.

Так в в річному звіті [1] за 2024 рік Державний центр кіберзахисту Держспецзв’язку виділив найпоширеніші типи інформаційної безпеки. При цьому було опрацьовано 3 мільйона подій, серед яких 28 тисяч були критичними та вимагали швидкого втручання. В результаті аналізу системою опрацьовано 1042 кіберінциденти і визначено відсоткове відношення кількості виявлених типів категорій кіберінцидентів, які мали найбільший вплив на систему (Рис.3.1).

Як зазначено у даному звіті, складність кіберзагроз щороку зростає, що вимагає постійного вдосконалення систем захисту. Також зловмисники все частіше використовують легітимні сервіси та інструменти, що ускладнює їх виявлення і запобігання [1].

Саме тому важливо розробляти нові підходи та рішення щодо прогнозування, виявлення та реагування системи на кіберзагрози для забезпечення стійкості всієї системи.

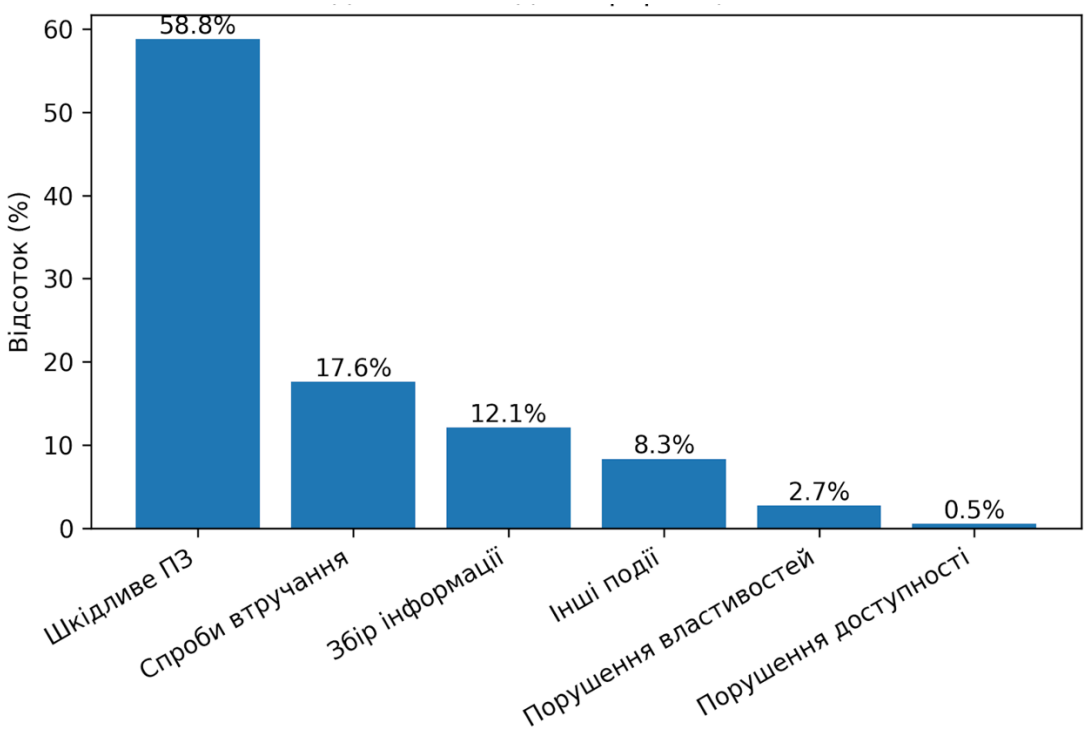


Рис.3.1. Розподіл типів подій інформаційної безпеки за 2024 рік

3.1.2. Математична модель впливу кіберінцидентів на стійкість систем управління інформаційною безпекою

До складу системи виявлення і реагування на кіберінциденти входять підсистеми, що відповідають за збір даних, прогнозування, аналіз та блокування кіберінцидентів. Щороку відділом Кібербезпеки ЗСУ складається звіт про виявлені кібератаки на різні системи. Виявлені кіберінциденти у період 2022–2024 дозволили сформувати вхідні параметрів керування для побудови математичної моделі впливу кіберінцидентів на стійкість систем управління інформаційною безпекою.

Для побудови математичної моделі впливу кіберінцидентів на стійкість систем управління інформаційною безпекою запропоновано алгоритм, який складається з наступних кроків.

Крок 1. Вибір параметрів керування, які відтворюють вплив кіберінцидентів на інформаційну систему. Виділено 5 основних кіберінцидентів. А саме шкідливий вміст, шкідливий програмний код, збір інформації зловмисником, порушення доступності та відома уразливість.

Крок 2. Найбільш наближена модель до типу катастрофи, дозволяє визначити перехід від стабільного стану до стану зі змінами під впливом 5 параметрів керування. Серед можливих типів катастроф виділено метелик, який опису швидку зміну стану системи під впливом п'яти параметрів управління. Хвіст ластівки описує систему, що залежить від чотирьох параметрів, та складка, що залежить від двох параметрів керування, що можливо при моделюванні впливу доступності та властивостей інформації.

Крок 3. Для побудови математичної моделі використано загальне рівняння для катастрофи «Метелик», яке має вигляд

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

де x — змінна, що визначає стан системи; a, b, c, d — параметри управління, які відповідають категоріям кіберінцидентів [106].

Крок 4. Для опису зміну стану системи використано метод градієнтного спуску, який застосовують для пошуку мінімального значення функції, а саме зменшення потенціалу і досягнення стабільного стану системи [107].

Формула для градієнтного спуску має вигляд:

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

де x_1 — нове значення змінної x; η — крок зміни; $\nabla f(x_2)$ — градієнт функції$f(x)$ в точці x_2.

Враховуючи метод градієнтного спуску, диференціальне рівняння, що описує мінімізацію потенціалу та показує градієнт системи, має вигляд:

$$\frac{dx}{dt} = -\frac{dV(x)}{dx} = -(6x^5 + 4ax^3 + 3bx^2 + 2cx + d) \qquad (3.1)$$

Також потрібно відмітити, що точки, де $\frac{dx}{dt} = 0$, відповідають станам рівноваги і залежать від значень параметрів a, b, c, d.

У свою чергу при зміні даних параметрів система може перейти в стан «катастрофи», тобто досягти точок біфуркації [108], [109]. Даний стан можливий при моделюванні ситуації, коли кількість кіберінцидентів стрибне до критичних значень, що призведе до збоїв системи.

Крок 5. Проведено аналіз точок рівноваги, які залежать від параметрів керування, що дозволило визначити критичні точки та виникнення біфуркацій, а також критичні режими функціонування системи.

На Рис. 3.2 наведено схему математичної моделі впливу кіберінцидентів на стійкість систем управління інформаційною безпекою на основі теорії катастроф.

Визначено основні модулі, які відповідають за збір та обробку даних, математичне моделювання для подальшого аналізу стійкості системи та підтримки прийняття управлінських рішень.

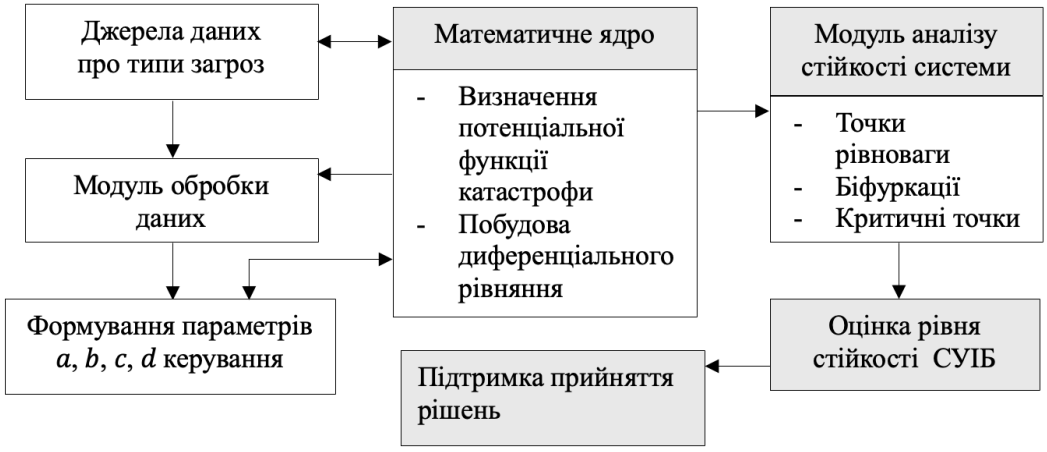


Рис. 3.2 Схема математичної моделі впливу кіберінцидентів на стійкість систем управління інформаційною безпекою

Математична модель впливу кіберінцидентів на стійкість систем управління інформаційною безпекою відкриває нові шляхи для аналізу стану системи за рахунок виявлення точок рівноваги, критичних точок і біфуркацій, що дозволяє оцінити рівень стійкості системи та прийняти вірне рішення щодо реагування на кожну окрему кіберзагрозу.

3.2. Удосконалення методу кластеризації загроз та вразливостей військових інформаційних систем

Сучасні виклики кіберпростору вимагають нових підходів щодо прогнозу та попередження ризиків виникнення загроз та їх впливу на стійкість інформаційної системи, що забезпечує конфіденційність, цілісність та доступність інформації. Методи кластерного аналізу дозволяють ефективно проводити аналіз, ідентифікацію та оцінку даних ризиків в умовах постійного зростання обсягу гетерогенних даних, а також застосовуються для виявлення аномалій у логах безпеки, аналізу складних сценаріїв кібератак, кореляції та узагальнення подій, які надходять із систем управління інформаційною безпекою.

Проведений аналіз наукових джерел показав, що методи кластерного аналізу широко використовують у сфері кібербезпеки [110]-[123]. Так в роботі [124] систематизовано підходи, щодо аналізу логів безпеки із застосуванням ML-техніки для виявлення патернів. Дані підходи не враховують часової динаміки, а також кластерний аналіз використовують лише для опису патернів без оцінки станів системи. Запропоновані в роботі [125]-[127] різні підходи штучного інтелекту та машинного навчання, які використовують методи кластерного аналізу та застосовуються для виявлення та аналізу кіберзагроз з великим масивом подій у інформаційній системі. Всі зазначені методи дозволяють автоматизовано виявляти закономірності та аномальні патерни без попередньої розмітки даних. Але також дані підходи орієнтовані на аналіз окремих подій і не дозволяють сформувати загальну оцінку стану інформаційної системи та її динаміку в часі. Тому доцільно при удосконаленні методу кластеризації загроз та уразливостей у військових

інформаційних системах врахувати часову динаміку розвитку загроз та використовувати інтегральні показники ризику для оцінки стану інформаційної системи.

3.2.1. Постановка задачі кластеризації загроз та уразливостей військових інформаційних систем

В розділі 3.1 розроблено математичну модель прогнозування критичних станів інформаційної системи на основі теорії катастроф, яка дозволяє визначати умови втрати стійкості та фіксувати критичні переходи. Для практичного застосування даної моделі доцільно перейти від неперервного опису до дискретного представлення станів системи на основі даних моніторингу виявлених загроз та уразливостей, які представлені у звіті про фіксовані кіберінциденти за 2022-2024 роки.

Нехай вхідні дані представлено у вигляді часового ряду

$$X = [x_{t,j}] \in R^{N \times m}, \tag{3.2}$$

де N – кількість днів спостережень у період 2022 – 2024 р., m – кількість категорій загроз та уразливостей, які зафіксовані в певний період часу, тобто $x_{t,j}$ показує кількість виявлених кіберінцидентів j – ого класу в час t. Таким чином, рядок матриці X описує події за певний проміжок часу. Важливо також проставити $x_{t,j} = 0$, якщо в момент часу t не зафіксовано кіберінцидент. На основі даних матриці X потрібно сформувати множину агрегованих станів системи, для обробки якої застосовується методи кластерного аналізу.

Аналіз окремих подій не дозволяє оцінити стан інформаційної системи, оскільки вони не враховують те, що загрози та уразливості можуть мати накопичувальний характер у певний період часу. При об’єднанні кількох

послідовних часових зрізів на певному інтервалі часі формується агрегований стан інформаційної системи.

Агрегований стан системи для часового вікна, що задається формулою

$$W_k = \{(k-1)\Delta + 1, (k-1)\Delta + 2, \ldots, k\Delta\}, \qquad k = 1,2,\ldots,K,$$

де $K = \left[\frac{N}{\Delta}\right]$ – кількість часових вікон, Δ – інтервал днів спостережень, задається вектором

$$S_k = \left(S_{k,1}, S_{k,2}, \ldots, S_{k,p}\right),$$

де

$$S_{k,i} = \sum_{t \in W_k} f_i(x_t), \;\; i = 1,2,..,p,$$

де $f_i(x_t)$ – функції агрегування, що групують категорії загроз і уразливостей, тобто задають параметри керування, які мають вплив на функціонування інформаційної системи. Для кількісної оцінки кожного агрегованого стану застосовується інтегральний показник критичного стану, який задається формулою

$$K_k = \Phi(S_k),$$

де $\Phi(S_k)$ – оцінює рівень ризику на певному інтервалі часу. Таким чином кожен стан інформаційної системи задається вектором

$$Z_k = (S_k, K_k).$$

Для оцінки подібності між станами Z_k та Z_l доцільно використати метрику відстані між агрегованими станами системи у просторі ознак

$$d(Z_k, Z_l) = \sqrt{\sum_{i=1}^{p} \alpha_i (S_{k,i} - S_{l,i})^2 + \beta (K_k - K_l)^2},$$

де $S_{k,i}, S_{l,i}$ – агреговані стани для вікон k та l; K_k, K_l – інтегральні показники критичного стану; α_i – вагові показники для параметрів загроз та уразливостей; β – коефіцієнт ваги для інтегрального показника ризику.

Задача кластеризації загроз та уразливостей військових інформаційних систем має на меті розбити множину

$$Z = \{Z_1, Z_2, \ldots, Z_k\}$$

на підмножини $\mathrm{C}_1, \mathrm{C}_2, \ldots, \mathrm{C}_L$ так, щоб вектори одного кластеру були максимально наближені до режимів функціонування інформаційної системи і виконувались умови

$$\mathrm{C}_i \cap C_j = \emptyset, \qquad \bigcup_{i=1}^{L} C_i = Z,$$

де L – кількість кластерів, які показують кількість режимів функціонування інформаційної системи. Перехід між кластерами показує зміну в режимах функціонування системи та фіксує переходи в системі, які надалі використовують для прогнозування критичних переходів в стані системи.

3.2.2. Алгоритм кластеризації станів військових інформаційних систем на основі аналізу загроз та уразливостей

В роботі [100] проведено аналіз найбільш поширених методів кластерного аналізу як алгоритм k-means, fuzzy c-means, DBSCSN та їх застосування в системах інформаційної та кібербезпеки. Встановлено, що ієрархічні методи кластеризації дозволяють виявити зв’язки між кластерами даних, але мають суттєві недоліки, серед яких перебудова кластерної структури при оновленні даних, а також висока

математична складність реалізації. Метод DBSCSN ((Density-Based Spatial Clustering of Applications with Noise) застосовують для виявлення аномалій, але неефективний для визначення режимів функціонування системи, оскільки зміна параметрів алгоритму сильно впливає на зміну структури кластерів. Також встановлено, що метод k-means має ряд переваг, серед яких низька математична складність, а також кожен кластер відповідає конкретному режиму функціонування системи. Таким чином, найбільш ефективним є використання метод k-means для задачі кластеризації станів військових інформаційних систем.

Проведений аналіз показав, попри те, що метод k-means відіграє важливо роль в задачі кластерного аналізу, але не дозволяє враховувати часової агрегації подій, накопичення загроз та уразливостей, а також інтерпретувати результати у вигляді режимів функціонування системи. Тому постало завдання удосконалити метод кластеризації на основі методу k-means, який дозволить враховувати часову агрегацію подій, сформувати інтегральний оцінку переходу системи до критичних станів, а також описувати кластери як режими функціонування системи.

Наведемо основі кроки алгоритму кластеризації загрози та уразливості для виділення станів військових інформаційних систем, який представлено в Додатку А.

Нехай підсистема моніторингу безпеки військової інформаційної системи збирає загрози та уразливості, в режимі реального часу, які на далі фіксує як кіберінциденти.

Крок 1. Потік кіберінцидентів задають множино подій

$$Y = \{y_1, y_2, \dots, y_m\},$$

де кожному кіберінциденту $y \in Y$ ставлять у відповідність часову мітку $\tau(y_i) \in R_+$ та категорії загрози або уразливості $j(y_i)$, $i = 1 \ \in N$.

Крок 2. Задається множина функцій

$$F = \{f_i, f_2, \ldots, f_p\}, f_i: R^m \to R,$$

де f_i відповідають за параметри керування, які мають вплив на стійкість системи.

Крок 3. Задані основні параметри для визначення ковзного часового вікна, а саме $\Delta \in R_+$ – довжина вікна, $\delta \in R_+, \delta$ – крок зсуву вікна та $\Delta = n\delta, n \in N$.

Крок 4. Перевіряється умова

$$\delta > 0, \Delta > 0, \delta < \Delta,$$

де не виконання хоча б однієї з умов повертає до повторного задання параметрів ковзного вікна на кроці 1.

Крок 5. За умови виконання циклу, що оновлює $\tau_k = \tau_0 + k\delta$, де $k \in N$ при зміні $k = \overline{0, k+1}$ виконуються наступні дії.

Крок 5.1 Сформовано ковзане вікно

$$W_k = (\tau_k - \Delta, \tau_k]$$

Крок 5.2 Відібрані підмножини кіберінцидентів Y_k таким чином, що часові мітки вказують на ковзане вікно. При цьому підмножини інцидентів задаються рівнянням

$$Y_k = \{y \in Y | \tau(y) \in W_k\}.$$

Крок 5.3 Для кожної категорії визначено кількість інцидентів

$$x_{k,j} = \{y \in Y_k | \, j(y) = j\}, \qquad j = 1, .., m,$$

а далі формується вектор частот

$$x_k = (x_{k,1} \ldots, x_{k,m}) \in R^m,$$

де кожна $x_{k,j}$ вказує на кількість інцидентів j − ої категорії у вікні W_k.

Крок 5.4 На даному кроці вектор частот кіберінцидентів x_k переведено у вектор агрегованих параметрів стану

$$S_k = \left(S_{k,1}, \ldots, S_{k,p}\right) \in R^p,$$

який сформовано на основі параметрів керування f_i, тобто

$$S_{k,i} = f_i(x_k), i = 1, .., p,$$

які дозволяють оцінити критичні переходи та режими функціонування інформаційної системи.

Крок 5.5 Визначено інтегральний показник критичності

$$K_k = \Phi(S_k),$$

де Φ: $R^p \to R_+$, яка перетворює параметри керування у скалярний показник ризику. При цьому функція Φ враховує вагові коефіцієнти параметрів стану системи. Значення K_k кількісно показують рівень ризику переходу системи до критичного стану в кожному часовому вікні W_k.

Крок 5.6 Визначено вектор стану для аналізу режимів функціонування системи

$$Z_k = (S_k, K_k).$$

Даний крок задає вхідні дані для подальшої кластеризації на основі удосконаленого метода кластеризації для виявлення стабільних та критичних режимів функціонування військової інформаційної системи.

Крок 5.7 Завершальний етап збирання всіх векторів станів в множину агрегованих станів для подальшої кластеризації. Здійснено перевірку умови

$$|Z_{k-1}| < M_w, \tag{3.3}$$

де $M_w = n$ – кількість часових вікон. При виконанні умови, Z_{k-1} додається до множини Z_k

$$Z_k = Z_{k-1} \cup \{Z_k\}$$

та збільшується індекс часового вікна

$$k := k + 1,$$

після чого алгоритм формує новий стан. При не виконанні умови (3.3) множина станів Z сформована і відбувається перехід до етапу кластеризація (блок А алгоритму Додадок А).

Крок 6. Сформовано множина станів системи

$$Z = \{Z_1, Z_2, \ldots, Z_{M_w}\},$$

де M_w – кількість часових вікон. Також задано кількість кластерів $\mathrm{C} = 1,2,3$, які відповідають режимам функціонування системи.

Крок 7. Проведено нормалізацію вектора $\tilde{Z}_k$ для встановлення номера кластера за правило мінімальної евклідової відстані

$$c_k^t = argmin_i \left\| \tilde{Z}_k - \mu_i^t \right\|,$$

що дозволило сформувати множину кластерів C_i^t.

Крок 8. Оновлено центри кластерів за правилом середнього значення

$$\mu_i^{t+1} = \frac{1}{|c_i^t|} \sum_{\tilde{Z}_k \in c_i^t} \tilde{Z}_k, \;\; i = 1, \ldots, C.$$

Крок 9. Встановлено умову збіжності для завершення задачі кластеризації, а саме алгоритм завершується за умови

$$\max_i \left\| \mu_i^{t+1} - \mu_i^t \right\| < \varepsilon,$$

при стабілізації положення центрів в кластерах.

Крок 10. Процес кластеризації завершено і сформовано множину агрегованих станів

$$Z = \bigcup_{i=1}^{c} C_i,$$

де C_i – кластери, що сформовані удосконаленим метод кластеризації на основі k-means.

Крок 11. Проведено оцінку критичності станів для відповідних кластерів шляхом обчислення середнього значення інтегрального показника критичності

$$\widetilde{K}_i = \frac{1}{|C_i|} \sum_{Z_k \in C_i} K_k \,, \qquad i = 1, \ldots, C.$$

Крок 12. Впорядковано кластери за зростанням $\widetilde{K}_i$

$$(\mathrm{C}_1, \mathrm{C}_2, \mathrm{C}_3) = sort_{\uparrow \widetilde{K}_i}(C_i)$$

та поставлено у відповідність режими функціонування військових інформаційних систем, які відповідають стабільному, деградації та критичному стану.

Таким чином, запропоновано удосконалений метод кластеризації загроз та вразливостей для визначення станів військових інформаційних систем. За допомогою даного алгоритму кластеризації станів показано новий підхід, який забезпечує перехід від неперервного визначення станів досліджуваної системи до дискретної моделі, яка застосовується для аналізу та прогнозування втрати кіберстійкості інформаційних систем.

3.3. Розробка моделі прогнозування критичних переходів на основі інтеграції теорії катастроф у SIEM-системи

В сучасному світі ризики кібербезпеки мають вагомий вплив на військові системи управління інформаційної безпеки, що, в свою чергу, відіграє важливу роль при підготовці військових підрозділів в тренувальних центрах. Реалії війни показують, що кібератаки здійснюються в усіх напрямках, щоб забезпечити витік інформації, починаючи зетапів підготовки підрозділів. Зловмисники стали більш досвідченими та небезпечними, а їх належне та своєчасне виявлення стало справжнім викликом. Виділяють основні кіберінциденти, що можуть впливати на інтеграційні системи навчання, серед яких шкідливий програмний код, збір інформації зловмисником, спроби втручання та інші [58].

Для запобігання даних кібератак необхідно забезпечити виявлення поведінкових аномалій у реальному часі, що дозволить управляти інцидентами. Системи безпеки інформації та управління подіями (SIEM) розглядають вищезазначені можливості як вбудовані функції. Загалом, SIEM системи мають здатність збирати, агрегувати, зберігати та корелювати події, створені керованою інфраструктурою [128]. При всіх перевагах дана система має значні недоліки, а саме фальшиві спрацювання, що перешкоджає виявленню важливих загроз, не

здійснюється прогнозування розвитку подій, що не дозволяє оцінити майбутні ризики [129].

Дані недоліки обумовлюють актуальність запровадження нових рішень, що дозволять підсилити систем безпеки інформації та управління подіями (SIEM), що, в свою чергу, відіграє важливу роль при захисті даних на початковому етапі протистоянні кіберзагроз.

3.3.1. Переваги та недоліки використання SIEM-системи для прогнозування, виявлення та попередження кіберінцидентів

Проведений аналіз наукових досліджень показав, що SIEM – системи становлять центральну платформу сучасних операційних центрів безпеки, оскільки вони збирають події із системи виявлення вторгнень, антивірусів, брандмауерів, а також корелюють ці події та надають синтетичні представлення сповіщень для обробки загроз і звітування про безпеку [129]. В роботах [130, 131] запропоновано методи машинного навчання для послідовного визначення аномалій у мережах, а саме навчання без учителя, для обробки логів із різних джерел для обходу правил без генерації хибних сповіщень. Однак в даних роботах основний фокус направлено на статистичні показники виявлення аномалій, але при цьому не приділяється увага динамічним змінам у системі. Також не досліджено вплив кібератак на стійкість системи в цілому. В роботі [132] наведено архітектуру SIEM – системи у базах даних інформаційно-комунікаційних систем військового призначення, яка враховує багаторівневий захист на основі теорії нечітких множин. Проте даний підхід не розглядає поведінку системи в часі, що призводить до ручного налаштування та не виявлення прихованих атак, де вже порушується стійкість всієї системи.

В роботі [133] використано мовну модель (Large Language Model, LLM), а саме глибоке навчання для представлення та обробки кіберзагроз, що дозволяє автоматизувати реагування та визначення точності класифікації інцидентів у SIEM -системах. Проте дані моделі фокусуються на інтерфейсі та не дають системного

аналізу стану даної системи, а також не враховують наявність накопичення кібератак та мають високу залежність від навчальних даних. Аналіз робіт українських та іноземних науковців показує, що велика увага приділена виявленню кіберінцидентів за допомогою методів машинного навчання, які мають свої переваги, але також виявлено важливі недоліки. В роботах не розглядаються питання стійкості системи та прогнозу критичних переходів станів безпеки даною системи

На основі аналізу наукових джерел постало завдання розробити алгоритм виявлення критичних станів у SIEM-системі на основі теорії катастроф для швидкого реагування на кіберінциденти в інтегрованій системі навчання військового призначення. Для досягнення поставленої мети необхідно проаналізувати технічні можливості SIEM-системи для прогнозування, виявлення та попередження кіберінцидентів, а також побудувати модель виявлення нестабільних станів системи під час кіберінцидентів із використанням SIEM-системи та теорії катастроф.

Сучасні SIEM - системи мають потужні функції з точки зору кореляції, зберігання, візуалізації та продуктивності, а також здатність автоматизувати процес реагування шляхом вибору та розгортання контрзаходів. Проте дані системи реагування дуже обмежені, а контрзаходи вибираються та розгортаються без виконання комплексного аналізу впливу атак і сценаріїв реагування [128] на стійкість системи управління інформаційної безпеки.

В роботах [82, 101] запропоновано використовувати теорію катастроф для виявлення змін в поведінці системи управління інформаційної безпеки. Побудовано модель впливу кіберінцидентів на стійкість СУІБ військового призначення на основі набору даних, який включав розділені по категоріях виявлені кіберінциденти різного характеру у період 2022 – 2024 років.

Отримані результати дозволили математично показати доцільність використання теорії катастроф для дослідження швидких змін в поведінці системи, виявляти точки, в яких система переходить до критичного стану, а також визначати

пороги критичних зм ін, які призводять до порушення стійкості всієї системи управління інформаційної безпеки [101]. Звичайно, що математичне і практичне дослідження має місце в подальшому інтегруватися в сучасні системи управління інформаційної безпеки, які набули використовують і додають нові способи максимально прогнозувати, виявляти та попереджувати кібератаки у військових інформаційних системах.

На основі отриманих результатів, а також аналізу наукових джерел сформовано основні недоліки, які виявлені в SIEM - системі, а також шляхи вирішення із використанням теорії катастроф (Таб.3.1).

Таблиця 3.1

Переваги застосування теорії катастроф у SIEM-системі

Основні недоліки SIEM-системи	**Характеристика**	**Шляхи вирішення із застосуванням теорієї катастроф**
Реагування	SIEM реагує після того, як подія вже сталася	Теорія катастроф дозволяє прогнозувати критичні точки переходу (нестабільність → збій)
Недостатня адаптивність	Системи працюють по встановлених правилах (rule-based)	Системи описують динамічні стани, які не працюють по правилам
Фальшиві спрацювання (false positives)	Система перевантажена подіями, важко знайти справжню загрозу	Теорія катастроф виявляє критичні стани, а не окремі події
Не працює з динамікою подій	SIEM не фіксує накопичення подій	Теорія катастроф аналізує динамічні зміни стану системи у часі
Не враховує взаємозалежності між інцидентами	Атаки часто складні (APT, ланцюжки), а SIEM не бачить повної картини	Модель катастроф описує системну поведінку, а не окремі компоненти
Обмежена аналітика	Стандартна кореляція слабка при нетипових атаках	Різні типи моделі теорії катастроф дозволяють аналізувати критичні точки
Неможливість оцінки майбутнього ризику	SIEM не прогнозує розвиток подій	Теорія катастроф використовується для прогнозування критих станів в ситемі

3.3.2. Алгоритм побудови моделі прогнозування критичних переходів на основі інтеграції теорії катастроф у SIEM-системи

В роботі [105] проведено аналіз сучасних систем імітаційного моделювання динаміки бойових дій у форматі командно -штабних навчань в режимі реального часу, а також детальний опис даної системи наведено в розділі 2. Структура інтегрованої системи навчання складається з основних логічних блоків, які доцільно об’єднати за допомогою SIEM в один ланцюг подій. Основні компоненти інтегрованої системи навчання [105], їх призначення та роль SIEM-системи наведено в Таб.3.2.

Таблиця 3.2

Структура інтегрованої системи навчання із застосуванням SIEM-системи

Компонент	**Призначення**	**Роль SIEM-системи**
Засоби зв’язку	Передача даних	Виявлення логів мережі, затримки, втрата пакетів
Сервери JTLS / JCATS	Навчальні сервери	Доступність, навантаження, визначення помилок
Клієнти	Користувачі (оператори)	Активація, логіни, час сеансу
Інтернет (50 мбіт/с)	Канал зв'язку	Моніторинг пропускної здатності
Підрозділи (бн, бр, ок)	Навчальні вузли	Стан, взаємодія, зв’язок

Впровадження SIEM-системи з блоком виявлення критичних переходів, які включають втрату каналу або відключення підроздів, які ідентифікуються за допомогою моделювання критичних станів на основі теорії катастроф, забезпечує інтелектуальне реагування на структуру поведінки всієї інтегрованої системи навчання у режимі реального часу. В плив кіберінцидентів, що детально досліджено в роботі [101], призводить до критичного стану всієї системи.

Математичне застосування теорії катастроф описує перехід системи із нормального функціонування в стан збоїв, що в свою чергу загрожує втратою важливої інформації про стан військової операції. Інтеграція SIEM-системи у поєднанні із моделями теорії катастроф дозволяє виявляти вплив кіберінцидентів,

а також прогнозувати критичні зміни у інтегрованій системинавчання, що забезпечує вчасне виявлення, попередження і усунення витоку військової інформації. Математична складова теорії катастроф, а також практичне дослідження за допомогою Python на основі реального звіту кіберінцидентів за 2020–2024 роки наведено в розділі 3.1 та буде представлено в розділі 4. Доцільно навести алгоритм побудови моделі виявлення нестабільних станів системи під час кіберінцидентів із використанням SIEM-системи та теорії катастроф в інтегрованій системі навчання, що дозволить показати комплексне дослідження, щодо побудови системи управління інформаційною безпекою у процесі підготовки військових підрозділів. Розглянемо основні кроки даного алгоритму.

Крок 1. Виділення джерела даних:

- сервери JTLS та JCATS, які виконують роль симуляторів, які генерують лог-файли з інформацією про події та мережеві підключення;
- засоби, які відповідають за процес збору, моніторингу та передачі даних між командними рівнями (підрозділи, бригади, головне управління) в центральну систему, які стосуються мережевого трафіку, поведінки системи та подій безпеки;
- мережевий сегмент із виходом в інтернет (канал 50 Мбіт/с), що потенційно є точкою входу зовнішніх загроз або витоку даних;
- підрозділи (HICON, PTA, SPA), які відіграють роль спостереження та реагування.

Крок 2**.** Інтеграція з SIEM реалізується декількома способами:

- отримання логів від серверів JTLS та JCATS, телеметрію засобів зв’язку та подій з елементів системи імітації бойових дій (VBS, MILES/LAZERTAG).

Крок 3. Встановлення модуля на основі теорії катастроф (окремий аналізатор), який виконує ряд завдань:

- нормалізація кіберінцидентів, які досліджено в роботі [101] і виділення найбільш впливових;

- побудова функції на основі виділених контрольних параметрів, яка моделює асимптотичну поведінку системи, а також дозволяє аналізувати стійкість складних систем та має вигляд [58], як приклад “ катастрофа метелик” [101]:

$$V(x) = 6x^5 + 4ax^3 + 3bx^2 + 2cx + d + ex^6 + fx^4 \quad (3.4)$$

де $a, b -$ контрольні параметри, c – Спам (Spam), d – Шкідливий програмний код (Malware), e – Атака на відмову в обслуговуванні (DoS/Ddos), f – Уразливість (Vulnerability);

- аналізує критичні токи та стабільність системи, де

$$\frac{dx}{dt} = -\frac{dV(x)}{dx}) = 0; \quad (3.5)$$

- визначає нестійкість системи, а саме виявлення точок біфуракції [59], [103], які показують збурення системи і є тригером реагування на вплив кіберінцидентів у момент часу t, при умові

$$R_t = \{x \in R | V'(x) = 0\},$$

де R_t – множина дійсних коренів, $n_t = |R_t|$ - дійсні корені. При порівнянні кількісті дійсних коренів у моменти часу t та $t-1$. За умови $n_t \neq n_{t-1}$ виникає нестабільний стан;

- побудова 3D графік для наочного представлення точок біфуркації і подальшого аналізу.

Крок 4. Розміщення блоку прийняття рішень, який відповідає за:

- ідентифікацію інциденту;

- автоматичне реагування за допомогою зміни маршрутизації, блокування трафіку і обов'язково оповіщенням і фіксацією в журналі, для подальшого дослідження і попередження в майбутньому;
- повернення інформації до блоку Головного управління.

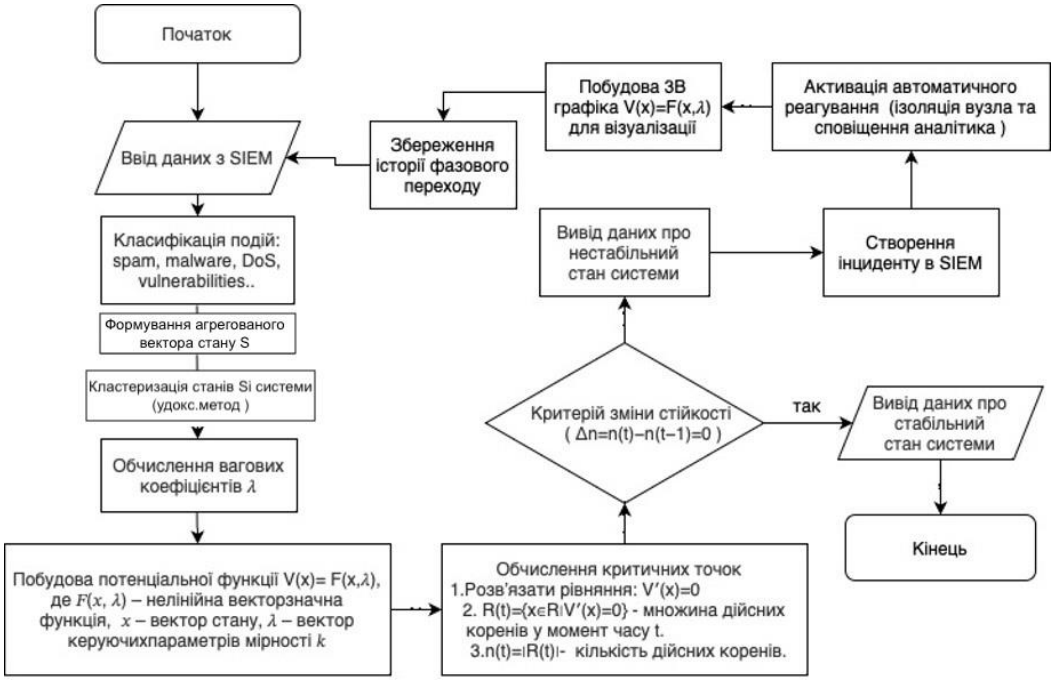


Рис.3.3 Схема алгоритму виявлення нестабільних станів системи із SIEM та теорії катастроф

Запропоновано алгоритм (Рис.3.3) виявлення нестабільних станів системи під час дії кіберінцидентів із використанням SIEM-системи та теорії катастроф в інтегрованій системі навчання, яка дозволяє прогнозувати і виявляти нестійкі стани системи, а також своєчасно реагувати на витік інформації в реальному часі, що забезпечує підвищення рівня кіберстійкості військової системи.

3.4. Удосконалення методу підтримки прийняття рішень щодо забезпечення кіберстійкості військових інформаційних систем

Захист систем військового призначення набуває все більшої актуальності в час реальної війни, яка змінює свої правила гри на арені безпеки інформаційно-комунікаційних систем і вимагає нових технічних рішень для підвищення даної безпеки. У сучасному кіберпросторі існує велика кількість різноманітних кібератак, які негативно впливають на військові інформаційно-комунікаційні системи та порушують їх здатність адаптуватися і відновлюватися після кожної атаки в цілому [134]. Але вагомим в даному контексті залишається здатність системи продовжувати безперервно працювати завдяки надійності каналів зв'язку та сталим інформаційним потокам [135].

3.4.1. Вибір рішень щодо побудови інтелектуальної системи прийняття рішень для забезпечення кіберстійкості інформаційних систем

Всі сучасні військові операції залежать від сучасних розробок кіберзахисту, які можуть протидіяти реальним загрозам та гарантувати стійкість інформаційно-комунікаційних систем до інтенсивних кібератак [136]. Використання системи управління інформаційною безпекою дозволяє зберігати конфіденційність даних, забезпечує безперервність дій та підтримує загальну оперативну ефективність на всіх етапах військових операцій. Також системи управління інформаційною безпекою є контрольним блоком для виявлення, попередження і блокування всіх можливих загроз і збоїв під час планування та реалізації бойових завдань [101].

В роботі [101] запропоновано математичну теорію катастроф для забезпечення стійкості системи управління інформаційною безпекою. Виявлено, що різні типи кіберінцидентів мають свій вплив на стійкість і рівновагу системи в цілому. Встановлено наявність зон ризику на площині точок рівноваги системи, які критично важливі при різких змінах станів системи під впливом кіберінцидентів. Дані результати дозволяють застосовувати математичну теорії катастроф для

підвищення стійкості системи управління інформаційною безпекою, що дозволяє прогнозувати дестабілізаційні процеси в системі.

Важливими також є результати роботи [137], в якій наведено переваги і недоліки використання SIEM-системи з використанням математичної теорії катастроф для прогнозування, виявлення та попередження кіберінцидентів в інтегрованих системах навчань військового призначення.

Важливим блоком для системи управління інформаційною безпекою є етап прийняття рішень, щодо виявлених загроз. В роботі [100] запропоновано метод кластерного аналізу для зменшення суб'єктивності експертних оцінок у процесі виявлення кіберзагроз.

Нажаль, традиційні методи, які використовують у системах управління інформаційною безпекою, не завжди швидко та точно приймають рішення у критичних ситуаціях в реальному часі, тому постає актуальне завдання про створення інтелектуальної системи підтримки прийняття рішень (ІСППР) для забезпечення кіберстійкості військових інформаційних систем. Дані інтелектуальні системи мають на меті покращити якість і швидкість прогнозування, виявлення і попередження динамічних та складних кіберзагроз, використовуючи сучасні штучні інтелектуальні технології [138]. Технології штучного інтелекту та машинного навчання використовують автоматизований аналіз великих обсягів даних та прогнозують загрози на основі виявлення аномалій у реальному часі [139]. Не потрібно також відкидати інтеграцію людино-машинної взаємодії, оскільки оператори військових інформаційно-комунікаційних систем мають брати участь у прийняті критичних рішень, що дозволить знизити ризик помилок, які виникають при автоматизованій роботі ІСПР [140].

Огляд сучасних наукових джерел показав зростання зацікавленості до використання штучного інтелекту в системах управління інформаційною безпекою, який дозволяє аналізувати великі обсяги даних, виявляти вразливі місця, а також прогнозувати можливі кіберзагрози [141]. В роботі [138] велику увагу приділено моделям глибинного навчання для підвищення надійності систем,

ефективності обробляти багаторівневі дані з різноманітних джерел. При цьому основна вимога покладена на систематичне навчання на основі отриманих даних в режимі реального часу, що сприяє постійному підвищенню якості підтримки прийняття рішень і реагування до нових кіберзагроз. В роботі [142] досліджується семантичні технології та технології великих даних у кіберзахисті, які дозволяють підвищити показники безпеки інформаційних систем. Також не потрібно забувати про поєднання хмарних технологій та оперативності периферійних систем, що дозволяє створити гібридні архітектури, які забезпечують перехід до створення масштабованих, надійних та інтелектуальних систем, які мають важливі для виконання складних операцій [139].

Для швидкого реагування на кібератаки, оцінки ризиків та створення протидій в реальному часі в [12] запропоновано поєднувати онтологічну модель знань, когнітивну архітектуру та аналіз даних. Важливою складовою інтелектуальної системи управління інформаційною безпекою є система прийняття рішень, яка часто не сприймає скоординовану дію кількох кіберагентів, які використовують різні шляхи проникнення до системи. Щоб дана система реагувала на складні атаки в режимі реального часу в [143] запропонували за основу системи вибрати ієрархічне моделювання та байєсівський аналіз для динамічного оновлення моделей і формування рекомендацій для забезпечення ефективності та стійкості у реальних сценаріях кіберзагроз.

Дослідники нідерландського аерокосмічного центру [131] пропонують комбінований підхід, який об’єднав інтеграцію штучного інтелекту та моделювання з симуляцією (M&S) для створення інтелектуальної системи підтримки прийняття рішень для систем військового призначення. Дане поєднання дозволяє підвищити точність прогнозів і якість рішень за рахунок попередніх результатів дій, які важливі для командирів під час планування операцій. Також даний метод дозволяє зменшити когнітивне навантаження на військових аналітиків та швидке реагування на зміни в бойових ситуаціях за рахунок створення нових сценаріїв в реальному часі.

Підходи до побудови інтелектуальних систем прийняття рішень для забезпечення кіберстійкості військових інформаційних систем, які запропоновані в роботах [12], [131], [138] – [143] мають звичайно переваги, але в свою чергу також мають ряд негативних показників таких, як надмірну складність моделювання когнітивних процесів і масштабування і реальному часі, складність взаємодії агентів і ризики некоректного автономного реагування без врахування єдиного контексту, велика залежність від якості даних, а також висока складність розрахунків при розширені функціонування системи, а також обмежена реалістичність симуляції в поєднанні з великими витратами ресурсів та залежності від точності моделей, які використовуються. Всі зазначені підходи (когнітивні, байєсівські, стимуляційні, мультиагентні) забезпечують аналіз і реагування на кібератаки, але не враховують динамічні процеси, що призводять до втрати стійкості системи. У даному досліджені пропонується використання теорії катастроф і кластерного аналізу як аналітичного центру DSS, що забезпечить перехід від реактивного до попереджувального управління кіберстійкості військових інформаційних систем.

Доцільно навести порівняльну характеристику використання різних підходів до побудови інтелектуальної системи прийняття рішень для забезпечення кіберстійкості інформаційних систем військового призначення.

Класичні системи підтримки прийняття рішень (DSS) мають ряд переваг, а саме структурований аналіз даних, відсутність повної автоматизації, простота реалізації, використовується для планування, оцінки ризиків і логістичних завдань. Але при цьому і недліки, серед яких низька швидкість реагування на кібератаки в динамічних системах, низька ефективність виявляти складні аномалії та реагувати в режимі реального часу та високі вимоги до вмінь і навичок операторів.

Наступними для порівняння є інтелектуальні системи підтримки прийняття рішень (AI+DSS), які також мають перваги і недоліки у своєму підході. До переваги відносять можливість обробки великих даних, ефективність роботи в режимі реального часу, використання машинного навчання для прогнозування

атак, висока точність і швидке ухвалення рішення, можливість навчання на нових інцидентах та формування ситуаційних знань у командних центрах. Основними недоліками можна виділити: високі вимоги до якісних даних, оновлення моделей, залежать від adversarial attacks, AI black box та Automation bais.

Цікавими є також автономні агентські системи забезпечення кіберстійкості (MAS, Autonomous Cyber Defense Agents), основними перевагами в яких виділяють виявлення, аналіз і реагування на кібератаки автономно, response and recovery та самостійне здійснення прогнозування кіберзагроз та відновлення після кібератак. Але існують також і недоліки, серед яких потреба високого рівня контролю даних, складність сертифікації в бойових умовах, складність в обчисленні та кіберзахисту агентіва та висока ймовірність втрати «людського контролю» в критичних умовах.

3.4.2. Побудова моделі підтримки прийняття рішень щодо забезпечення кіберстійкості військових інформаційних систем

Для розробки моделі інтелектуальної системи підтримки прийняття рішень (ІСППР) для забезпечення кіберстійкості військових інформаційних систем запропоновано класичні та інтелектуальні підходи забезпечення швидкого реагування та прийняття рішень щодо виявлених кібератак. Запропонований підхід, який ґрунтується на виявленні динамічних змін станів системи та відрізняється від традиційних, які фіксують події та реакції на вже виявлені кіберінциденти, бере за основу положення теорії катастроф. Теорію катастроф доцільно застосовувати для опису поведінки складних систем у точках біфуркації, які виникають при зміні параметрів і призводять до різкої втрати стійкості. Такий підхід передбачає не лише виявлення кіберінцидентів, а й дозволяє прогнозувати їх наслідки за рахунок аналізу змін станів в системі [101], [137], [131]. Для побудови цілісної аналітичної архітектури, де всі модулі взаємодіють у режимі реального часу, застосовано поетапний підхід, який складається зі збору та нормалізації

даних, моделювання, кластеризації, синтезу рішень і в заключенні – контроль якості прийняття рішень, у контурі якого залишається людина (Human in the loop).

Для побудови даної моделі система формально представлена як гібридна динамічна система з неперервними та дискретними блоками, які моделюють стан стійкості, переходи режимів та прийняття рішень.

Отримані результати наукових досліджень в роботах [101]-[137], [131] показали доцільність використання нелінійної динаміки та математичної теорії катастроф для побудови моделі інтелектуальної системи підтримки прийняття рішень (ІСППР) для забезпечення кіберстійкості військових інформаційних систем. Даний підхід забезпечує математично передбачити критичні переходи під впливом зростаючих кібератак, навантаження чи конфлікту систем.

Нелінійні системи залежать від початкових умов, а також від впливу зовнішніх чинників, що призводить до різких стрибків або катастроф у стійкості системи [144].

Стан нелінійних систем задається формулою:

$$\frac{dx}{dt} = f(x; a, b) + \xi(t), \tag{3.6}$$

де $x(t)$ – інтегральна змінна, яка показує стан системи (рівень кіберстійкості), a, b – параметри системи, які відповідають за інтенсивність подій, рівень кіберінцидентів, $\xi(t)$ – показує шум або флуктації даних.

Використовується також тип катастрофи «Метелик», який показує перехід від стабільного до змінного стану під впливом 5 параметрів.

Загальне рівняння для катастрофи «Метелик», має вигляд

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

де x — змінна, що визначає стан системи; a, b, c, d — параметри управління, які відповідають категоріям кіберінцидентів [101].

Для визначення диференціального рівняння, що описує зміну стану системи, використано метод градієнтного спуску, який використовується для пошуку мінімального значення функції, а саме зменшення потенціалу і досягнення стабільного стану системи. Нагадаємо, що формула для кроку градієнтного спуску має вигляд:

$$Vx_1 = x_2 - \eta \nabla f(x_2)$$

де x_1 — нове значення змінної x; η — крок зміни; $\nabla f(x_2)$ — градієнт функції $f(x)$ в точці x_2.

Точки, де

$$\frac{dx}{dt} = 0,$$

відповідають станам рівноваги і залежать від значень параметрів a, b, c, d. В свою чергу при зміні даних параметрів система може перейти в стан «катастрофи», тобто досягти точок біфуркації. Даний стан можливий при моделюванні ситуації, коли кількість кіберінцидентів стрибне до критичних значень, що призведе до збоїв системи.

Критичний стан системи можна також визначити за допомогою метрики:

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

яка показує, що система втрачає рівновагу, настає етап активації підсистеми реагування.

Математична теорія катастроф надає можливість виявити складні взаємозалежності між різними кіберінцидентами і вчасно виявити катастрофічні зміни в стані системи. В свою чергу метод градієнтного спуску, а саме аналіз потенціалу

$$V(x_t; a_t, b_t, c_t, d_t)$$

дозволяє вчасно виявляти зони ризику та запобігати змінам стану системи.

В реальних умовах процес зміни станів у військових інформаційних системах здійснюється дискретно, тому для моделювання даних переходів використано метод кластеризації на основі ознак поведінки системи.

Для опису поведінкового профілю системи у момент часу t використовують багатовимірний вектор, який описує всі ознаки, що реалізують відповідні зібрані дані SIEM-системи, журналів подій, телеметрії військових підсистем, та задається формулою:

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

де λ_t – кількість кібератак за одиницю часу; σ_t^2 – дисперсія подій у ковзному вікні; $\rho_{1,t}$ – автокореляція; Sw_t – асиметрія розподілу; Kt_t – аксцес розподілу; H_t – ентропія стану системи; δ_t – відстань до стану катастрофи; p_t – нормований ризик; q_t – рівень довіри.

Множину векторів $\{\phi_1, \phi_2, \ldots, \phi_t\}$, яка описує динамічну поведінку системи в певний момент часу побудовано га основі удосконаленого методу кластеризації загроз та уразливостей, який запропоновано у розділі 3.2. Основна перевага даного методу, що процес кластеризації відбувається з урахуванням часової агрегації кіберінцидентів та з використанням інтегрального показника, що задає критичній стани системи. За допомогою удосконаленого методу кластеризації множину векторів розділяють на класи зі спільними властивості, тобто кластери

$$S = \{Stable, Degraded, Critical\}.$$

Далі мінімізують відстані між елементами одного кластера та максимізують відстані між елементами різних кластерів, тобто мінімізують функціонал середньоквадратичних відстаней:

$$D = \sum_{k=1}^{K} \sum_{\phi_i \in C_k} \|\phi_i - \mu_k\|^2$$

де K – кількість кластерів, C_k – множина точок у кластері k, μ_k- центр кластера. Таким чином всі вектори множини $\{\phi_1, \phi_2, \ldots, \phi_t\}$ отримають мітку кластера після навчання алгоритму, яка визначає стан системи $s_t \in S$ з відповідними ознаками, а саме стан Stable включає низьку дисперсію, низьку автокореляцію та малу етропію; стан $Degraded$ описує середнє значення автокореляції, зростання варіаційності та підвищення нормованого ризику; стан Critical описує високі H_t, σ_t^2, p_t та зменшення довіри q_t.

Запропонований удосконалений метод кластеризації використовує агреговані стани системи, які утворилися на основі виявлених кіберінцидентів у ковзних часових вікнах. Даний підхід враховує динаміку утворення загроз та підвищує точність встановлення режимів реагування системи. Таким чином, удосконалений методу кластеризації займає місце аналітичного ядра інтелектуальної системи підтримки прийняття рішень для забезпечення стійкості військової інформаційної системи.

Потрібно також враховувати, що на систему можу діють нові кіберінциденти, які впливають на зміну стану системи. Нехай система у деякий момент часу перебуває у стані $s_t \in S$, тоді ймовірність переходу системи до стану s_{t+1} визначається формулою:

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

де елементи p_{ij} оцінюють статистично враховуючі історичні дані:

$$p_{ij} = \frac{N_{ij}}{\sum N_{ij}},$$

де N_{ij} – кількість спостережень при переході станів $s_i \to s_j$.

На Рис.3.4. представлено State Diagram, яка описує стани системи в залежності від елементи p_{ij}, які визначають швидкі реагування підсистеми на виявлені кібератаки.

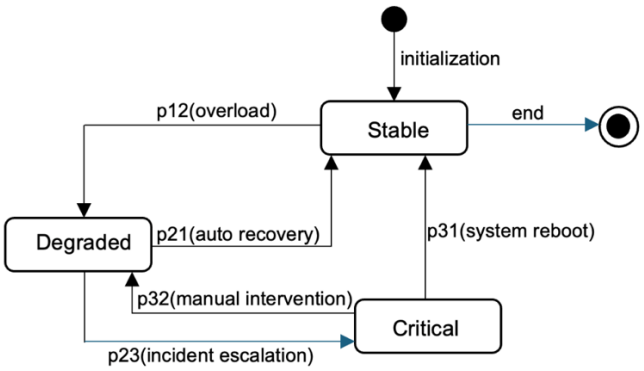


Рис.3.4 State Diagram моделі переходу станів системи

Проведена кластеризація за допомогою удосконаленого методу кластеризації станів здійснює поділ всіх наявних даних SIEM системи на поведінкові характеристики, кожен з яких відіграє свою роль в інформаційній системі. Як зазначалось раніше, кожен кластер має свій центр μ_k, який показує стан системи та відстань $\|\phi_t - \mu_k\|$, яка є мірою зміни стану системи [128].

Існує прямий зв'язок між кластерами та показниками, які застосовуються в катастрофі виду «Метелик». Так стан Stable можна отримати при локальному мінімумі потенціалу $V(x)$, тобто у точці x_s при

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

При даних показниках система перебуває у стійкому стані, де параметри катастрофи метелик a, b, c, d піддаються не значним коливанням, що не вливає на втрату рівноваги системи в цілому.

При виявленні стану Degraded, система піддається впливу кібератак і її стійкість порушується, але вона все ще функціонує в межах своїх можливостей. В даній області градієнт потенціалу слабкий, що провокує сповільнення системи повернутися до стану рівноваги після виявлення кібератаки. Дані зміни супроводжуються змінами в параметрах a, b, c, d, переходом до нового мінімуму або появи точок біфуркації, тобто система стає чутливою до випадкових флуктацій.

Третій стан Critical визначає перехід системи в катастрофічну область, що призведе до катастрофічного стану, а саме порушення стійкості кіберсистеми, що характеризується відмовою або втратою контролю з боку системи керування. Даний стан математично показує зміна знаку другої похідної $V''(x)$ та нестійкістю потенціалу енергії

$$\frac{d^2V(x)}{dx^2} \to 0.$$

В цей момент система перебуває у точці біфуркації, що позбавляє систему змінити поточний стан. Поєднання кластерного аналізу та теорії катастроф дозволяє оцінити стійкість системи у визначений момент часу, а також за рахунок відстаней до виявлених точок біфуркації, які дають можливість прогнозувати потенційні точки переходу між станами системи.

Запропонована модель інтелектуальної системи підтримки прийняття рішень поєднує взаємодію аналітика та автоматизованих модулів для реагування на кіберінциденти. На Рис.3.5. представлено Sequence diagram, яка показує логіку реагування всієї системи [129].

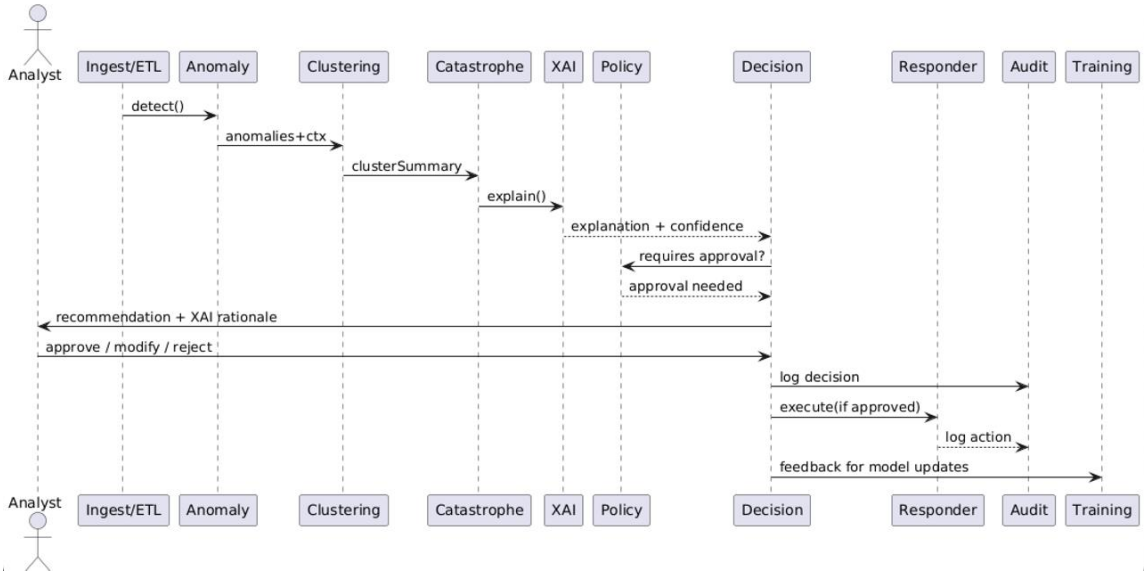


Рис.3.5. Діаграма послідовності «Людина в циклі»
(реалізована в середовищі PlantUML)

Запропонована взаємодія людини та штучного інтелекта дозволяє вивести існуючі системи на новий інтелектуальний рівень, а також підвищити показники виявлення, прогнозування кібератак, що, в свою чергу, підвищить точність і стійкість системи при прийнятті рішень у складних операціях.

3.4.3. Алгоритм реагування системи підтримки прийняття рішень з урахуванням динаміки кіберінцидентів

Інтеграція СУІБ з платформою SIEM (security Information and Event Management) та системою виявлення вторгнень (IDS**)**, дозволить виявити та реагувати на кібератаки у реальному часі [145]. В свою чергу SIEM-система здійснює моніторинг, кореляцію подій та автоматизоване реагування на кіберінциденти. В роботі [146] наведено функціональну модель SIEM-системи, яка забезпечує нормалізацію, фільтрацію, класифікацію, агрегацію, кореляцію, пріоритезацію та аналіз подій, а також генерацію різноманітних звітів, повідомлень і візуального представлення даних для оперативного та обґрунтованого прийняття рішень. В роботі [132] представлено модель ідентифікації кіберінцидентів SIEM-системою, які виявлено в інформаційно-комунікаційних системах (ІКС), і враховує

багаторівневий захист на основі теорії нечітких множин. Проте даний підхід не розглядає поведінку системи в часі, що призводить до ручного налаштування та не виявлення прихованих атак, де вже порушується стійкість всієї системи.

Також мають місце методи машинного навчання в функціональному забезпеченні даних систем, а саме застосовуються для визначення аномалій у мережах [130,131]. Основним недоліком запропонованих підходів є направленість на статистичні показники виявлення аномалій, але відсутні дії при динамічній зміні у системі, що не дозволяє оцінити вплив кібератак на стійкість систему в цілому.

В свою чергу, IDS системи фіксують події низького рівня, які показують ранні дії кібератак і дозволяє швидко реагувати на них. Визначають головні показниками IDS системи: стабільність, яка забезпечує послідовно і надійно виявляти загрози без хибних сигналів у часі, та точність виявлення, а саме відношення true тривог до всіх виявлених. Дані показники відображають якісне функціонування IDS системи, як елемента СУІБ, оскільки від них залежить швидкість та коректне реагування системи на кіберзагрози в цілому Для покращення ефективності роботи IDS – систем та систем запобігання вторгнень (IPS) в роботі [147] використовують методи машинного навчання.

Проведений аналіз наукових розробок показав, що в багатьох роботах розглядаються дані системи для прогнозування, виявлення та попередження кіберінцидентів, але не приділено уваги стійкості системи та прогнозу критичних переходів станів безпеки даною системи. В роботі [82], [101] запропоновано теорію катастроф для виявлення змін в поведінці системи управління інформаційної безпеки. Побудовано модель впливу кіберінцидентів на стійкість СУІБ військового призначення на основі набору даних, які розділені по категоріях виявлення кіберінцидентів різного характеру.

Завданням даного дослідження є інтеграція теорії катастроф у моделі прийняття рішень для систем управління інформаційною безпекою, які використовують платформу SIEM, IDS та IPS системи. Даний підхід дозволить моделювати різкі переходи системи від стабільного до критичного стану, а також

визначати пороги критичних змін, які призводять до порушення стійкості всієї системи управління інформаційною безпекою.

У сучасних умовах час реагування на кіберінциденти у системах управління інформаційною безпекою вимірюється у секундах, тому відсутність автоматизованого прийняття рішення призведе до критичних наслідків. Модуль прийняття рішень чітко визначає, коли ізолювати вузол, повідомити про дану загрозу чи заблокувати доступ, тоді як SIEM, IDS та IPS системи лише надають інформацію про кіберінциденти та аномалії. В Таблиці 3.3 наведено основні компоненти систем і їх функції для реалізації СУІБ.

Модуль прийняття рішень повинен враховувати вид загрози, попередній досвід, динаміку зміни стану системи та прогнозувати майбутні наслідки. Включаючи всі наведені властивості, модуль прийняття рішень дозволяє СУІБ швидко адаптуватися до впливу кіберінцидентів у режимі реального часу [132, 133]. Тому для створення даного модуля використовують сучасні математичні підходи: машинне навчання, байєсівські мережі, теорію ігор та теорії катастроф, яка дозволяє виявляти точки біфуркації та раптові переходи стану від стабільного до критичного [101].

В роботі [132], [133] запропоновано архітектуру інтелектуальної SIEM-системи для виявлення кіберінцидентів у базах даних інформаційно-комунікаційних систем військового призначення та використання штучного інтелекту для ефективного реагування на інциденти у SIEM системі.

Проведений аналіз дозволив виявити ряд недоліків в стратегічному функціонуванні SIEM – системи. Основний недолік в тому, SIEM реагує після того, як подія вже сталася та не фіксує їх накопичення. Система працює по встановлених правилах (rule-based), а також вона перевантажена подіями, тому важко знайти справжню загрозу. Атаки часто складні (APT, ланцюжки), а SIEM не бачить повної картини, також стандартна кореляція слабка при нетипових атаках.

Table 3.3

Ролі ключових компонентів СУІБ

Компонент	**Роль у системі**	**Ключові функції**
SIEM (Управління інформацією та подіями безпеки)	Централізований збір, обробка та кореляція подій безпеки	Агрегація журналів Аналітика Генерація інцидентів Зберігання подій
IDS (Система виявлення вторгнень)	Виявлення підозрілої або аномальної активності (пасивне)	Аналіз мережевого трафіку Виявлення аномалій/шаблонів Сповіщення
IPS (Система запобігання вторгненням)	Реагування на загрози в режимі реального часу (активне)	Блокування атак Ізоляція вузлів Фільтрація трафіку
Система прийняття рішень	Аналізує моделі ризиків та інциденти для вибору відповідної відповіді	Оцінка стабільності стану Вибір дії (MONITOR / IPS / ALERT) Автоматизація
Аналітик безпеки / SOC (Центр операцій безпеки)	Людський нагляд, перевірка та ручне керування відповідями	Огляд інциденту Ручне втручання Аналіз першопричини
База знань / Політики	Основа для прийняття рішень, реагування та дотримання вимог	Визначення правила Оцінка відповідності Аудит
Користувачі та активи	Об'єкти захисту та джерела ризику	Джерела подій Системи, служби, файли Мережева активність

Також визначено Порівняльна характеристика основних метрик ефективності математичних підходів, які визначені на основі проведеного аналізу наукових джерел [58], [128], [148], [149], [150] та усереднених оцінок, наведено в Таблиці 3.5.

Доцільно відмітити основні метрики, які використанні при порівнянні даних підходів, а саме: Response Time (сек) - час між інцидентом і рішенням; Adaptability - датність пристосуватись до нових атак без перенавчання; Instability Detection - виявлення критичних переходів/біфуркацій; Interpretability – можливість пояснити аналітику рішення; Data Requirement – кількість історичних подій для точності; CPU Efficiency - споживання обчислювальних ресурсів.

Таблиці 3.4

Порівняння методів прийняття рішень в СУІБ

Критерій	**Машинне навчання (ML)**	**Баєсівські мережі**	**Теорія ігор**	**Теорія катастроф**
Тип обробки	Статистичний / на основі навчання	Ймовірнісна логіка	Стратегічне моделювання	Аналітична динаміка
Середній час прийняття рішення	1,2 – 3,5 сек	2,5 – 10 сек	4 – 12 сек	0,5 – 1,0 сек
Вимога до навчання	Так (перед тренуванням)	Так (структура + CPT)	Формалізація стратегії	Ні (параметризована модель)
Обсяг історичних даних	>10 000 подій	1000–5000 записів	Сценарії, матриця стратегії	5–20 параметрів (інцидентів/особливостей)
Залежність від контексту	Висока	Середня	Висока	Низька (зосередження на критичних точках)
Адаптивність до нових інцидентів	Низька	Обмежена	Статична	Висока (чутлива до стану)
Точність (виявлення нестабільності)	70–90% на навчальних даних	65–85%	60–80%	95–99% (за умови правильної конфігурації)
Інтерпретованість рішень	Низька (чорний ящик)	Висока (на основі графіків)	Середня	Висока (карта біфуркації)
Прогнозування катастрофічних змін	Частково можливе	Не реалізовано	За допомогою моделювання	Основна функціональність

Проведено візуалізацію Таблиці 3.4 у вигляді Radar Chart (Рис.3.6.) за допомогою Python та бібліотек Matplotlib та Numpy.

На графіку видно чітке домінування теорії катастроф за ключовими параметрами: швидкість реагування, виявлення нестабільності, інтерпретованість, адаптивність та ефективність, що підкреслює доцільність її використання при будові удосконалених СУІБ.

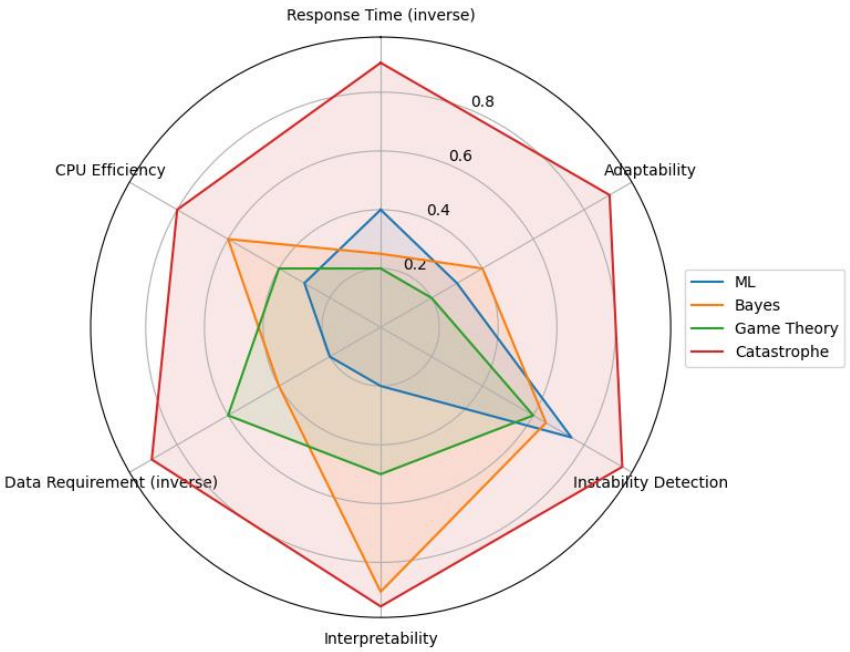


Рис. 3.6. Radar Chart: Порівняльний аналіз методів прийняття рішень у СУІБ

Наведемо кроки реалізації алгоритму прийняття рішень в системі, яка реагує на кіберінциденти.

Крок 1. Ініціалізація системи підтримки прийняття рішень (DSS) з відповідними початковими параметрами, а саме встановлення часу $t = 0,$ порогові значення $\tau_m, \tau_i, \tau_f,$ які відповідають критичним рівням інтегрального показника ризику $\rho(t)$ та визначають режими функціонування системи.

Крок 2. Введення вхідних даних, які отримані із SIEM в DSS (Рис. із схеми SIEM)

$$S(t) = [x(t), x(t+1), n(t), \Delta n, z(t)],$$

де $x(t), x(t+1)$ – поточний та прогнозований стани систем, $n(t)$- стійкість системи, Δn – виникнення біфуракційних точок, а також $z(t)$ – параметри керування.

Крок 3. Перевірка на існування біфуракційних точок, при яких система переходить у критичний стан

$$C(t) = \begin{cases} 1, & \Delta n \neq 0, \\ 0, & \Delta n = 0, \end{cases}$$

при $C(t) = 1$.

Крок 4. Оцінка показників, що відповідають за стійкість функціонування системи на основі інтегрального показника ризику

$$\rho(t) = \Psi(x(t+1), n(t), \Delta n),$$

який за умови монотонності

$$\frac{\partial \rho(t)}{\partial x(t+1)} > 0, \Delta n \neq 0 \text{ та } \rho(t) > \rho(t+1) \text{ при } \Delta n = 0$$

вказує на зростання ризику появи критичних точок, тобто появи біфуркаційних точок.

Крок 5. Фіксація кіберінцидентів в SIEM-системі на основі виявлених критичних переходів при $\Delta n \neq 0$ та значення ризику $\rho(t)$.

Крок 6. Здійснюється аналіз стратегій атак S_A та стратегій реагування системи захисту S_D на основі теорії конфліктів, тобто задається конфлікт двох сторін

$$G = \langle S_A, S_D, U \rangle,$$

$S_A = \{a_1, a_2, \ldots, a_k\}$ – множина стратегій атак, $S_D = \{d_1, d_2, \ldots, d_k\}$ – множина стратегій реагування системи захисту, $U(a_j, d_j)$ – функція реагування системи.

Стратегія реагування системи DSS визначається, як

$$d = arg \max_{d_j \in S_D} U(a_j, d_j).$$

На основі поточного стану системи та значення ризику $\rho(t)$ формується множина $R(t)$ стратегій реагування на кіберінцидентів, яка задається рівнянням

$$R(t) = \{d_j \in S_D : U(a_j, d_j, \rho(t), n(t), \Delta n)\},$$

або

$$R(t) = \Phi(\rho(t), n(t), \Delta n, z(t)),$$

де $\rho(t)$ – інтегральний показник ризику, $n(t)$ – параметр стійкості системи, Δn – показник виникнення біфуркаційних точок, $z(t)$ – параметр керування системою.

Крок 7. Визначення режиму реагування системи у відповідності зі змінами її стану

$$D(t) = Decision(\rho(t), n(t), \Delta n) = \\ = \begin{cases} monitor, & \rho(t) \le \tau_m \text{ або } \Delta n = 0, \\ activate\_IPS, & \tau_m < \rho(t) \le \tau_i \text{ і } \Delta n \ne 0, \\ system\_failure, & \rho(t) > \tau_f \text{ і } n(t) = 0. \end{cases}$$

Крок 8. Активація сценарію реагування системи та виконання відповідних дій відповідно до функції стану $D(t)$.

Крок 9. Візуалізація та архівація історії реагування системи на кіберінциденти

$$H(t) = [x(t), x(t+1), n(t), \Delta n, \rho(t), D(t), z(t)]$$

та перехід до початкового кроку за умови

$$t \to t + 1.$$

Даний удосконалений метод реагування системи прийняття рішень на основі теорії катастроф та теорії конфліктів виступає аналітичною оболонкою над потоком SIEM -даних і дозволяє виявляти критичні зміни стану (біфуркаційні переходи), адаптуватись системі до динаміки кіберзагроз, а також поєднувати автоматичне та експертне реагування на виявлені кіберінциденти Рис.3.7 .

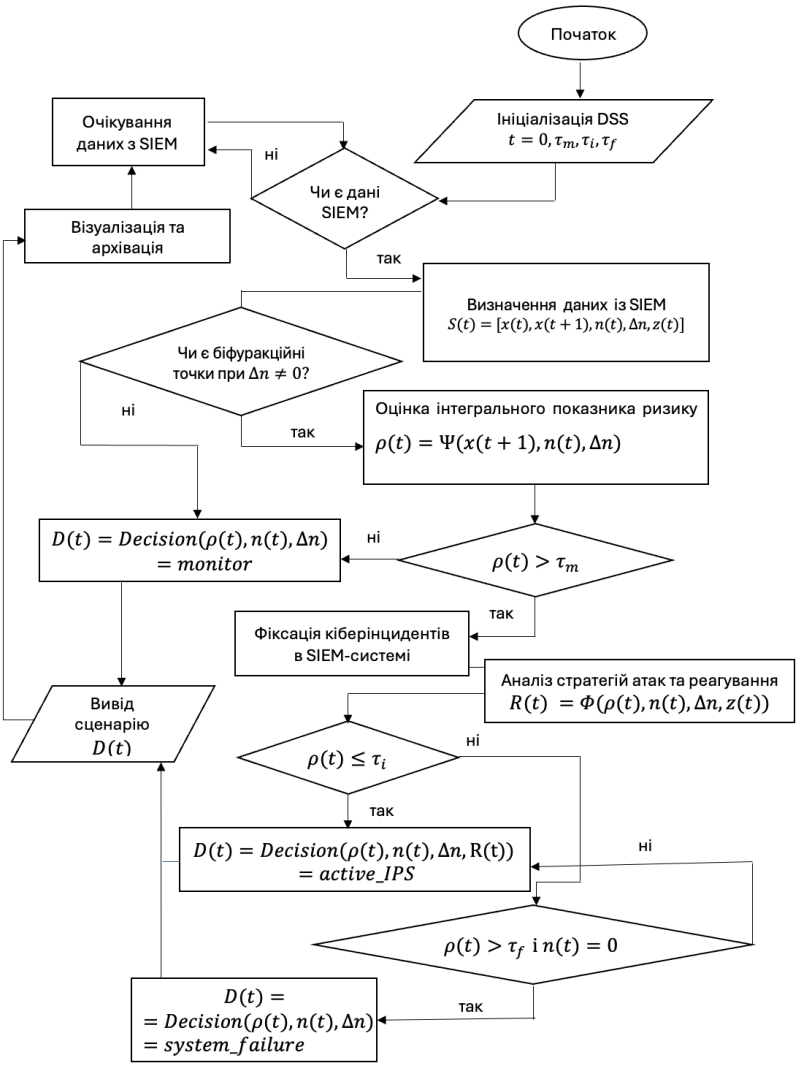


Рис. 3.7. Алгоритм реагування системи підтримки прийняття рішень з урахуванням динаміки кіберінцидентів

Висновки до розділу 3

1. Розроблено математичну модель прогнозування критичних станів систем управління інформаційною безпекою військового призначення на основі теорії катастроф. Проведено аналіз ключових параметрів керування та виділено п’ять основних параметрів, які відповідають категоріям кіберінцидентів, що мають найбільший вплив на інформаційну систему та задають катастрофу типу «Метелик», яка дозволяє описати нелінійну динаміку кіберінцидентів. Встановлено, що дана математична модель дозволяє визначити точки рівноваги, критичні пороги стійкості та біфуркації станів, що відповідає фіксації переходів системи від стійкого до нестабільного або критичного стану інформаційної системи.
2. Удосконалено метод кластеризації загроз та уразливостей військових інформаційних систем для встановлення режимів функціонування системи та переходу між ними. Розроблений алгоритм базується на основі k-means із врахуванням часових вікон та інтегральних показників критичності стану системи. Дискретне подання динамічної поведінки інформаційної системи дає основу для прогнозування втрати стійкості її станів та аналізу переходів між режимами функціонування системи, що підвищує ефективність управління інформаційною безпекою.
3. Проведено аналіз переваг та недоліків використання SIEM-системи для прогнозування, виявлення та попередження кіберінцидентів, а також доцільність її використання в системах військового призначення. На основі проведених досідженнь побудувано математичну модель для обробки та захисту передачі інформації в інтегрованій системі навчання військового призначення на основі реальних даних про кіберінциденти за 2020 - 2024 роки, математичного застосування теорії катастроф та покрокового алгоритму його реалізації в SIEM системі.

4. Удосконалено метод підтримки прийняття рішень для забезпечення кіберстійкості військових інформаційних систем на основі теорії катастроф, теорії конфліктів та кластерного аналізу для прогнозування критичних переходів станів військових інформаційних систем під дією кіберзагроз та кіберзагроз.

РОЗДІЛ 4. ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ ЗАПРОПОНОВАНИХ МОДЕЛЕЙ І МЕТОДІВ

4.1. Комп'ютерне моделювання та оцінка ефективності математичної моделі катастрофи типу «Метелик»

Система управління інформаційною безпекою є важливим елементом захисту від можливих загроз і збоїв, яка піддається впливу різних внутрішніх і зовнішніх факторів, які можуть призвести до незворотних наслідків. Саме тому прогнозування впливу різних типів інцидентів дозволяє забезпечити стабільність та рівновагу складних динамічних систем, їх конфіденційність, цілісність та доступність. В розділі 3 побудовано математичну модель впливу кіберінцидентів на стійкість системи управління інформаційною безпекою на основі теорії катастроф типу «Метелик». Для оцінки практичної ефективності даної моделі доцільно провести комп'ютерне моделювання на основі реальних статистичних даних кіберінцидентів та порівняти отримані результати з існуючими підходами, які використовуються для оцінки критичних станів інформаційних систем.

4.1.1. Реалізація моделі катастрофи типу «Метелик» для прогнозування критичних станів інформаційної системи

В роботі [100] для комп'ютерного моделювання математичної моделі катастрофи типу «Метелик» запропоновано використовувати Python з бібліотекою Pandas для обробки даних, математичних обчислень та чисельного моделювання, а також набір кіберінцидентів за 2022 – 2024 роки, які надані відділом Кібербезпеки ЗСУ, які збиралися для аналізу поточної поведінки загроз та уразливостей на військову інформаційну систему.

Проведено початковий аналіз вхідних даних показав наявність 934 спостережень в часовому діапазоні від 01.04.2022 до 20.10.2024 року з результатами дослідження кожного дня з 21 категорією кіберзагрози відповідно до переліку категорій кіберзагроз, який розроблений на основі Переліку категорій

кіберінцидентів, схваленого Національним координаційним центром кібербезпеки при Раді національної безпеки та оборони України (Протокол № 18 засідання Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України від 25.10.2021 (від 28.10.2021 № 16/320/21дск)) [89]. Початкову оцінку впливу кожного інциденту встановлено шляхом обчислення кількості інцидентів по кожній категорії, а також визначено частоту інцидентів, яка характерна для кожної категорії за період 2022–2024 років (Табл.4.1). Чим вищий середній рівень інцидентів, тим більше даний вид загрози впливає на систему.

Таблиця 4.1

Кількісна оцінка інцидентів відповідно до переліку категорій

(не включені категорії з нульовим показником)

№ типу категорії	**1.01**	**2.01**	**2.02**	**2.04**	**3.01**	**3.03**	**4.01**	**4.02**	**5.01**	**5.02**	**6.01**	**9.01**	**9.02**
Кількість	26873	2077131	43944	3971	281	1852	17	89	165	15	170	7983	4240
Середній рівень	29.7	2461.05	104.4	5.36	1.6	4.03	1.3	1.2	2.2	1.25	1.39	9.4	5.3

Проведений аналіз вхідних даних показав, що частина категорій регулярно активні за даний період (Таблиця 4.1), інша частина має тільки десятки подій за 2,5 роки, а в деяких значення відсутні. Таким чином, встановлено, що наданий реальний дата сет містить велику кількість пропусків в категоріях загроз, різну частоту появи кіберінцидентів, а також різні масштаби значень. Для візуалізації досліджених даних побудовано графіки розподілу інцидентів по категоріях за допомогою бібліотек Matplotlib та Seaborn (рис.4.1 та рис.4.2).

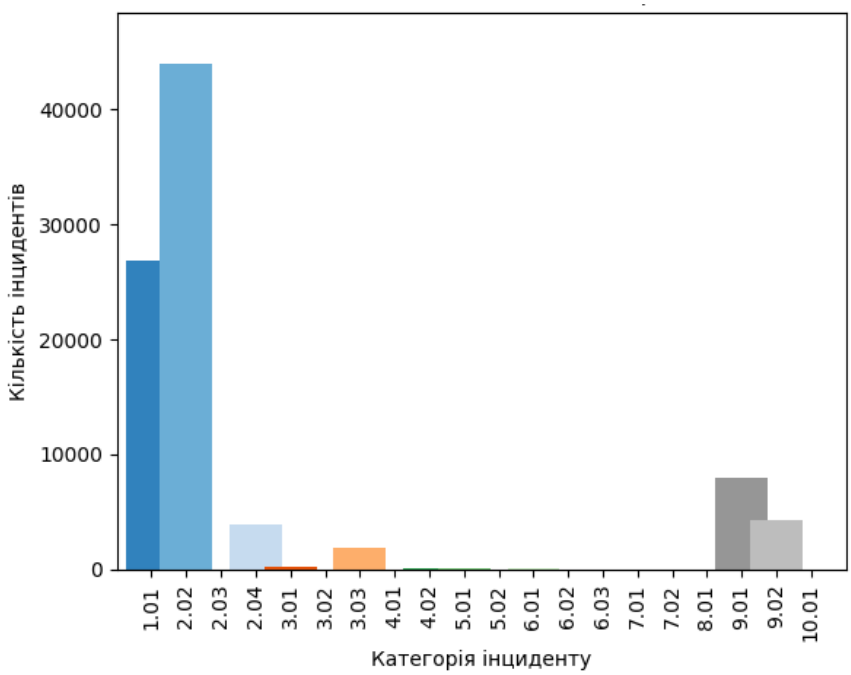


Рис 4.1. Кількість інцидентів розподілених по категоріях за 2022 – 2024 роки

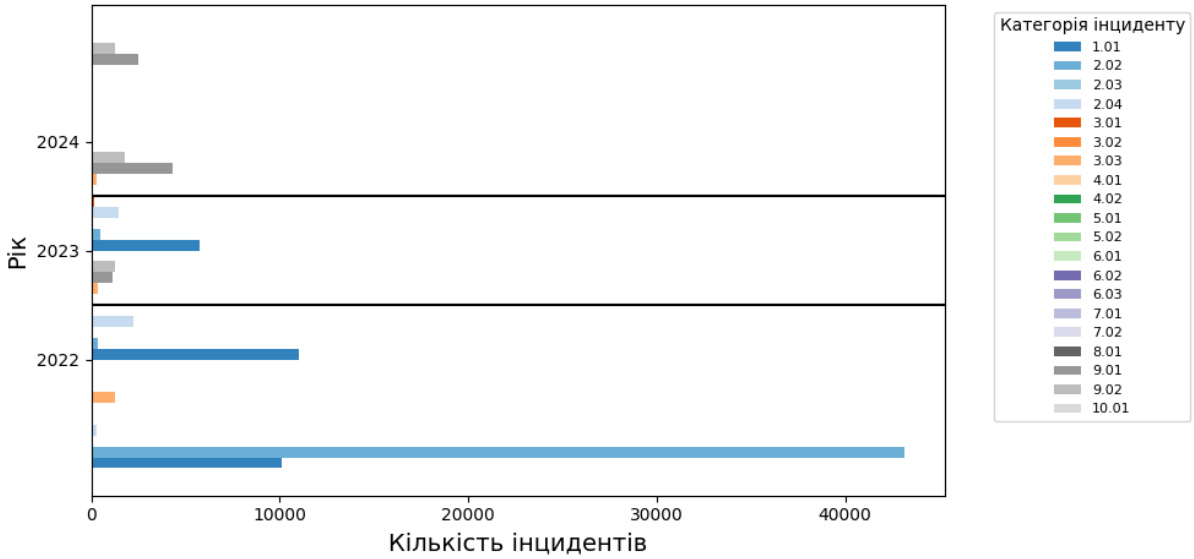


Рис 4.2. Кількість інцидентів по роках і категоріях за 2022 – 2024 роки

Структура даного дата сету описує реальні дані кібербезпеки та показує наявність розріджених часових рядів та подій різної інтенсивності. Все це

ускладнює застосовувати до них лінійні та порогові моделі оцінки ризиків, але дозволяють застосовувати нелінійні підходи, в тому числі теорію катастроф.

Для подальшого дослідження всі значення категорій приведено до числового значення, а також пропущені значення проставлено як нуль.

Проведений аналіз набору даних показав найбільш активні категорії інцидентів, які виявлені у період 2022 – 2024 років. Відповідно до переліку [89] виділено наступні активні загрози, серед яких Шкідливий вміст (1.01), Шкідливий програмний код (2.01, 2.02, 2.04), Збір інформації зловмисником (3.01, 3.03), Порушення доступності (6.01), Відома уразливість (9.01, 9.02). Тому дані категорії вибрані, як основні параметри для побудови моделі впливу інцидентів кібербезпеки на стійкість системи управління інформаційної безпеки в ЗСУ.

Інформація про кількість інцидентів кожної категорії, а також середній рівень (кількість) кожної категорії, дозволив розрахувати вагу для кожної категорії інцидентів за формулою:

$$W_i = \frac{n_i}{\sum_{i=1}^{m} n_i} \times \frac{k_i}{\sum_{i=1}^{m} k_i}, \tag{4.1}$$

де $n_i -$ кількість інцидентів у $i -$ категорії, $i = \overline{1, m}$, $k_i -$ середня кількість інцидентів у кожній $i -$ категорії.

Вагу для кожної з 5-ти категорій інцидентів знайдено за допомогою Python і наданої бази даних інцидентів. Для початку підсумували кількість інцидентів кожної вибраної категорії і використали формулу (4.1). Результати розрахунків наведено в Таблиці 4.2.

Таблиця 4.2

Ваги для категорій інцидентів

Назва категорії інцидентів	**Тип інциденту**	**Вага, w**
Шкідливий вміст	1.01 Спам	0.0124
Шкідливий програмний код	2.01 Зараження ШПЗ 2.02 Розповсюдження ШПЗ 2.04 Шкідливе підключення	0.9809
Збір інформації зловмисником	3.01. Сканування (Scanning) 3.02. Сніфінг (Sniffing) 3.03. Фішинг (Phishing)	0.0010
Порушення доступності	6.01 Атака на відмову в обслуговуванні DoS/DDoS	0.0011
Відома уразливість	9.01 Уразливість 9.02 Некоректна конфігурація	0.0056

Для побудови математичної моделі використано теорію катастроф, розрахунок і візуалізацію здійснено за допомогою Python, бібліотек Numpy та Plotly.graph_objects (Додаток Б). В рівняння катастрофи типу «Метелик» (1), що визначено в Розділі 3, закладено параметри (спам, шкідливий програмний код, атаки на відмову в обслуговуванні, вразливості) і їх вагу з Таблиці 4.2, що характеризує вплив інцидентів на систему, за основу якої взято модель катастрофа «Метелик», яка застосовується для аналізу стабільності і рівноваги системи піж впливом зовнішніх факторів.

Задається похідна потенціальної функції

$$\frac{dV}{dx} = 6x^5 + 4ax^3 + 3bx^2 + 2cx + d + ex^6 + fx^4 \qquad (4.2)$$

де a, b – контрольні параметри, c = 0.0124 – Спам (Spam), d = 0.9809 – Шкідливий програмний код (Malware), e = 0.0011 – Атака на відмову в обслуговуванні (DoS/Ddos), f = 0.0056 – Вразливість (Vulnerability).

Вміст рівняння (4.2) дозволив моделювати асимптотичну поведінку системи, особливо в умовах значень змінної x, які виходять за межі допустимого діапазону.

Також дана модель враховує додаткові локальні мінімуми та максимуми, які важливі при аналізі стійкості складних систем.

Встановлено точки рівноваги та критичні точки, які характеризують стійкіст та біфуркацію динамічної системи (Рис.4.3). Дана візуалізація показує, що параметри $e\ i\ f$, мають малі ваги і змінюють лише асимптотику потенціалу, що впливає на зображення моделі катастрофи.

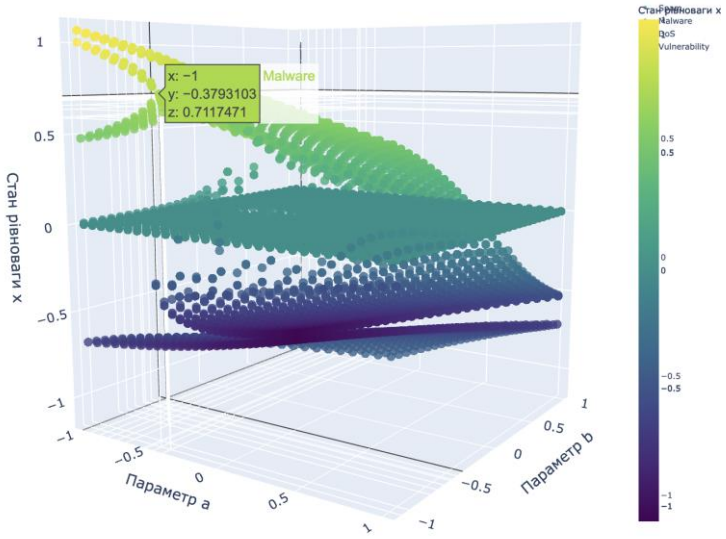


Рис.4.3 Множина рівноважних станів нелінійної моделі катастрофи типу «Метелик» у просторі параметрів

Проведений аналіз отриманих результатів показав, що Спам ($w = 0.0124$) створює локальні точки рівноваги при $x \in [-1,1]$, а саме

1. $a = -0.9, b = -0.7, x = -0.45$
2. $a = 0.1, b = 0.3, x = 0.42$
3. $a = 0.8, b = 0.6, x = 0.95,$

що вказує на незначний вплив на стабільність системи.

Інша ситуація із впливом інциденту Шкідливий програмний код ($w = 0.9809$), який провокує розгалуження у рівноважних станах, що характеризується тим, що для одних і тих самих значень параметрів a і b існують різні значення x (Рис.4.3), що також підсилюється візуально різкою зміною кольору (від темного до

світлого) і вказує на біфуркацію. Дані розгалуження показують нестабільність системи, а саме різкий перехід із одного в інший стан. Такі точки біфуркації призводять до каскадних збоїв у системі, оскільки невелика зміна параметрів a і b приводить до різкого переходу між станами.

Інцидент Атака на відмову в обслуговуванні ($w = 0.0011$) викликає нестабільність станів системи, де їх зони здебільшого обмежені, але при $a = 0.1, b = 0.3, x = -0.12$ або $x = 0.53$, що вказує на точку біфуркації.

Вплив інциденту Уразливість ($w = 0.0056$) створює потенційні точки входу для інших інцидентів, таких як Malware або DoS.

На графіку (Рис 4.4.) точки біфуркації можна побачити в областях, де розгалуження або різка зміна кольору від світлого до темного.

При деяких парах (a, b) потенціал системи не має локальних мінімумів або максимумів, що призводить до «дірки» в площині (Рис. 4.4), тобто рівноважні стані не можуть бути визначені.

Виявлений дефект показує критично важливу зону, де система не має рівноважного стану, чутлива до збурень, що відповідає небезпечним або хаотичним режимам роботи, особливо під впливом кіберінцидентів типу Malware та Vulnerability.

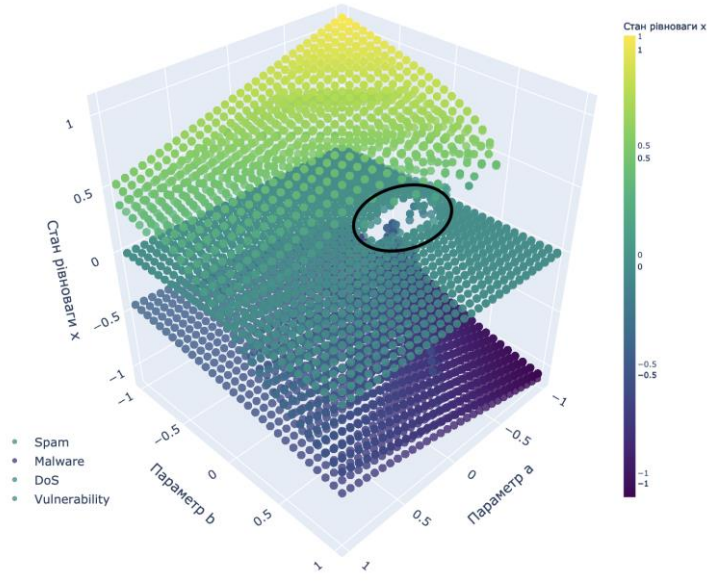


Рис.4.4 Наявність зони ризику «дірки» на площині точок рівноваги

Таким чином, використання динамічних моделей на основі теорії катастроф забезпечує ефективність математичних підходів для проведення аналізу та здійснення прогнозування безпеки складних інформаційних систем, а особливо те, як різні типи інцидентів (Спам, Шкідливий програмний код (Malware), Атаки на відмову в обслуговуванні (DoS) та Уразливості систем) впливають на стійкість і рівновагу інформаційної системи.

4.1.2. Порівняння та оцінка ефективності математичної моделі катастрофи типу «Метелик» для прогнозування критичних станів

Для оцінки ефективності математичної моделі катастрофи типу «Метелик» для прогнозування критичних станів доцільно обчислити кількісні показники і порівняти їх з відповідними показниками існуючих моделей, що дозволить встановити її переваги та визначити існуючі недоліки для подальшого вдосконалення. Порівняння та аналіз здійснено на основі лінійної моделі агрегованого ризику [151]-[153] та моделі ранніх попереджувальних сингалів CSD (Critical Slowing Down) [154]-[157]. За допомогою комп'ютерного моделювання в середовищі Python для трьох моделей знайдено чотири основні показники.

Перший показник визначає середній час раннього попередження $\overline{\Delta T}$ (WLT, warning lead time), який показує час між появою сигналу та виявленням критичного стану системи [158]-[160]. Математично середній час раннього попередження $\overline{\Delta T}$ задається математичним сподіванням

$$\overline{\Delta T} = M(\Delta T) = M(t_c - t_s),$$

де t_c – момент часу виявлення інциденту, t_s – момент часу, коли система зафіксувала попередження про інцидент.

Другий показник - це коефіцієнт покриття інцидентів K_{cov}, який визначає відношення кількості прогнозованих інцидентів до загальної кількості фактичних інцидентів за період часу t та обчислюється за формулою

$$K_{cov} = \frac{N_{cp}}{N_c},$$

де $N_c -$ кількості фактичних інцидентів за період часу t, $N_{cp} -$ кількість прогнозованих інцидентів [161-163].

Третій показник коефіцієнт хибних сигналів FAR (False Alarm Rate), який показує як часто система видає хибні попередження без фіксації інцидентів та обчислюється за формулою

$$FAR = \frac{FP}{FP+TN},$$

$$0 \leq FAR \leq 1,$$

де $FP -$ кількість хибних фіксацій (False Positive), $TN -$ кількість нормальних станів (True Negative), 0 – система не генерує хибну фіксацію, 1 – система генерує сигнал без інциденту [161-165].

Для комплексної оцінки якості функціонування кожної моделі, для яких визначено $\overline{\Delta T}$, K_{cov} та P_{f_a}, $P_{f_a} -$ ймовірність хибних інцидентів, використано інтегральний індекс ефективності кожної досліджуваної моделі, який задається

$$E = f(K_{cov}, P_{f_a}, \overline{\Delta T})$$

та обчислюється

$$I = \alpha K_{cov} + \beta(1 - P_{f_a}) + \gamma \Delta T,$$

де $\alpha, \beta, \gamma \geq 0$ і $\alpha + \beta + \gamma = 1$,

Для комп'ютерного моделювання заданих моделей, а також для обчислення та аналізу встановлених показників використано реальний набір фіксованих кіберінцидентів за 2022 - 2024 роки. За інтервали часу вибрано дані за місяць, а періоди встановлено кризовими, якщо вони відносяться до $D_{0,9}^{(\Delta T)}$.

Аналіз динаміки праматерів рівноважних станів системи за 2022-2024 роки моделі катастрофи типу «Метелик», які предсталені в Таблиці. 4.3 показав, що в періоди 2022-04, 2022-05, 2022-06,2023-02, 2023-04, 2023-06, 2024-03 та 2024-10 мають кілька стійких станів рівноваги (MultiStable =1), тобто можливі зміни в режимах функціонування системи під дією зовнішніх та внутрішніх впливів. Також збільшення показника розкиду рівноважних станів $Spread_{eq}$ та показника R_{but} вказують на наявність точок біфуркацій в даній період часу.

Таблиця 4.3

Динаміка параматерів рівноважних станів системи за 2022-2024 роки

Дата	N_eq	N_stable	MultiStable	Spread_eq	x_star	R_but	N_eq	N_stable
30.04.2022	5	3	1	1,792	-0,992	1	5	3
31.05.2022	3	2	1	1,694	-0,995	0,5	3	2
30.06.2022	3	2	1	1,757	-0,972	0,5	3	2
31.07.2022	1	1	0	0,000	-0,986	0	1	1
30.09.2022	3	2	1	1,674	-0,907	0,5	3	2
31.12.2022	1	1	0	0,000	-0,827	0	1	1
28.02.2023	3	2	1	1,439	-0,752	0,5	3	2
30.04.2023	3	2	1	1,413	-0,626	0,5	3	2
30.06.2023	3	2	1	1,482	-0,672	0,5	3	2
31.12.2023	1	1	0	0,000	-0,614	0	1	1
31.01.2024	1	1	0	0,000	-0,552	0	1	1
31.03.2024	3	2	1	1,098	-0,357	0,5	3	2
30.06.2024	1	1	0	0,000	-0,582	0	1	1
30.09.2024	1	1	0	0,000	-0,539	0	1	1
31.10.2024	3	2	1	1,229	-0,509	0,5	3	2

В таблиці Таблиця 4.3 вказані кількісні показники основних характеристик моделей, які розглядаються в порівнянні. Модель катастрофи типу «Метелик» показує найбільше значення середнього часу раннього попередження $\overline{\Delta T} \approx 7$ міс., при показниках для лінійної моделі $\overline{\Delta T} \approx 3$ міс., в також для моделі CSD він складає 1 міс. Модель типу «Метелик» формує сигнал критичний стан за 5-8 місяців, тоді як лінійна модель за 1-4 місяці, а моделі CSD в час настання критичного стану. Таким чином, нелінійна модель катастрофи типу «Метелик» надає більше часу для стратегічного реагування (Таб. 4.3).

Таблиця 4.4

Оцінка ефективності моделей на основі кількісних показників

Модель	**ΔT, міс**	**K_cov**	**FAR**	**I**
Лінійна модель агрегованого ризику	2.53	1.00	0.259	0.22
CSD	0.76	1.00	0.185	0.20
Катастрофа типу "Метелик"	**6.6**	1.00	**0.333**	**0.40**

Таблиця 4.5

Середній час раннього попередження ΔT в критичні періоди для моделей

Дата критичних станів	**ΔT, міс. / Моделі**		
	Linear	**CSD**	**Butterfly**
2023-11	1.0	0.0	5.1
2023-12	2.03	0.0	6.13
2024-01	3.07	1.03	7.17
2024-02	4.03	2.00	8.13

Аналіз показника K_{cov} вказує на те, що всі три моделі 100% покривають періоди, де настають критичні стани системи. В Таблиця 4.3 модель катастрофи типу «Метелик» має найбільший показник FAR, що вказує на те, що дана модель фіксує передкризові стани системи на етапі виявлення нестійкості стану. Тому дана модель не лише фіксує критичні стани системи, але і на ранніх етапах виявляє біфуркаційні точки, в яких відбувається перехід системи до нестабільного стану.

Для обчислення значення інтегрального індексу ефективності I надано вагу кожному показнику в залежності від його впливу на якість прогнозування. Таким чином, для $\alpha = \gamma = 0.4$, оскільки модель застосовують для раннього прогнозування критичних станів і важливо не пропускати інциденти в системі, а $\beta = 0.2$, що відповідає за хибне реагування системи на можливі порушення в системі. Аналіз отриманих результатів (Табл.4.4) показав, що найбільше значення інтегрального індексу ефективності $I = 0{,}4$ для моделі катастрофи типу «Метелик», що вказує на доцільність використання даної моделі для прогнозування критичних станів інформаційної системи.

Візуальне представлення отриманих значень показників для лінійної моделі агрегованого ризику, моделі ранніх попереджувальних сигналів CSD та модель катастрофи типу «Метелик», а також порівняння їх показників наведено на графіку (Рис.4.5).

Таким чином, проведено комп'ютерне моделювання для експериментального аналізу основних характеристик лінійної моделі ризику, моделі ранніх попереджувальних сингалів (CSD) та моделі катастрофи типу «Метелик» для прогнозування критичних станів військової інформаційної системи.

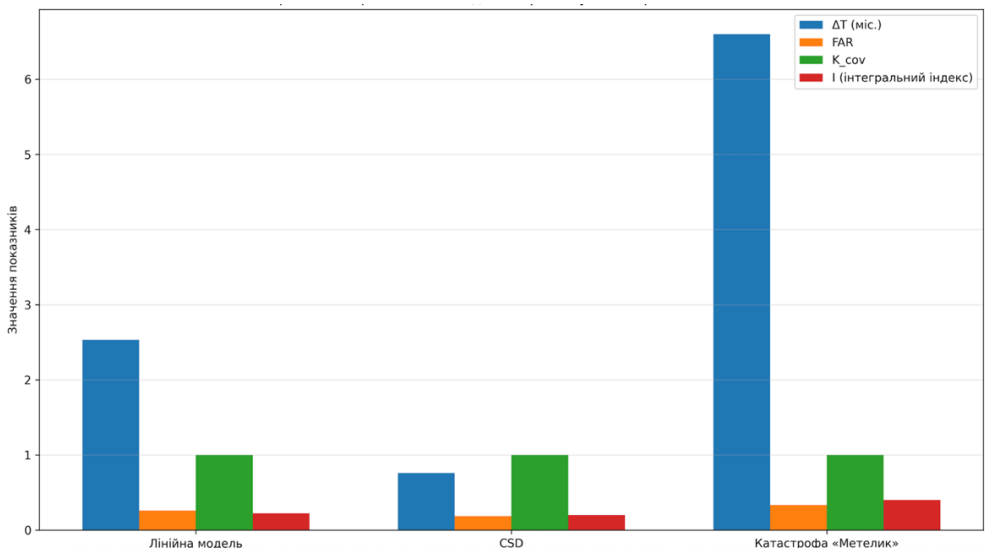


Рис. 4.5 Порівняння ефективності моделей прогнозування критичних станів системи на основі значень метрик

Проведений аналіз показав, що модель катастрофи типу «Метелик» має ряд переваг та дозволяє структурно та обґрунтовано прогнозувати моменти втрати стійкості системи та виявляти передкризові режими до моменту виявлення критичних станів системи. В свою чергу, лінійна модель ризику ефективна для моніторингу поточного рівня загроз без прогнозування та попередження, а модель CSD ефективна лише для статистичної оцінки настання критичних станів.

4.2. Імітаційне моделювання процесів та оцінка ефективності удосконаленого методу кластеризації загроз та уразливостей

Імітаційне моделювання процесів дозволило відтворити реальний процес кластеризації загроз та уразливостей, оцінити існуючі ризики та ефективність запропонованого підходу, який запропоновано в розділі 3.2, для подальшого застосування у системах управління інформаційною безпекою. За допомогою імітаційного моделювання відтворено динаміку накопичення загроз у часі, а також здатність удосконаленого методу кластеризації загроз та уразливостей виявляти переходи між стабільними, змінними та критичними станами інформаційної системи. Для імітаційного моделювання використано реальний набір даних фіксованих кіберінцидентів за 2022-2024 роки, що дозволило оцінити стійкість алгоритму до нерівномірності подій, сезонних коливань та шуму в даних, які характерні для військових інформаційних систем в умовах активного реагування на виявлені кіберзагрози [166]-[168].

4.2.1. Імітаційне моделювання процесу кластеризації загроз та вразливостей військових інформаційних систем

Імітаційне моделювання процесу кластеризації загроз та вразливостей військових інформаційних систем, яке реалізоване мовою Python із використанням бібліотек Pandas, NumPy, scikit-learn та Matplotlib, для кластеризації даних застосовано алгоритми k-means, для нормалізації використано StandardScaler та MinMaxScaler, проведено в декілька кроків.

Крок 1. Встановлення вхідних даних та визначення основних показників для задачі кластеразації. Вхідні дані подані матрицею спостережень $X = \{x_j(t)\}$, де $x_j(t)$ – кількість інцидентів категорії j в день t з використанням реального набору даних фіксованих кіберінцидентів за 2022-2024 роки (Рис.4.2).

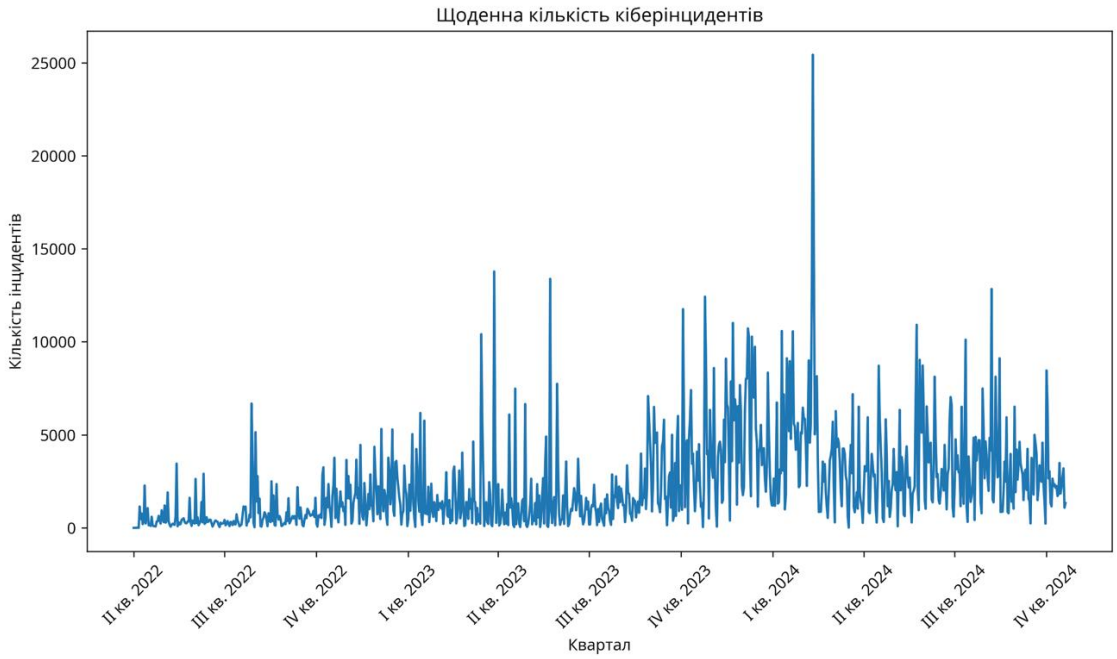


Рис.4.6 Вхідний часовий ряд кіберінцидентів для імітаційного моделювання

Крок 2. Проведено обробку вхідних даних. На даному кроці дані перетворено у формат datetime, заповнено пропуски даних $x_j(t) = 0$, а також виділено контрольну змінну Total, як суму по всіх категоріях за день.

На основі попереднього аналізу загальної кількості кіберінцидентів за добу (Таблиця 4.6) встановлено високу варіативність інтенсивності інцидентів за показником стандартного відхилення σ, наявність пікових навантажень, що відповідає масованим кібератакам в цей період часу, а також нерівність потоку інцидентів в часі вказує велика різниця між перцентилями.

Початковий аналіз основних показників обґрунтовує застосування удосконаленого методу кластеризації, який містить ковзні вікна, агрегування даних та кластеризацію станів.

Таблиця 4.6

Характеристика показника загальної кількості інцидентів за добу

Показник	**Значення**
Період спостереження	01.04.2022 – 20.10.2024
Кількість спостережень	934
Середнє значення	2319,84
Стандартне відхилення	2496,14
Мінімум	0
25-й перцентиль	565
Медіана	1451,5
75-й перцентиль	3284
Максимум	25431

Крок 3. Задано параметри імітаційного моделювання. Здійснено перехід від щоденних спостережень до станів системи за допомогою методу ковзного часового вікна, оскільки кіберінциденти мають накопичувальний характер.

Задано вектор кількості інцидентів $X(t) = (x_1(t), \ldots, x_m(t))$ за день t, довжину вікна L та крок зсуву s. У кожному вікні $W_k = [t_k, t_k + L - 1]$, де $t_k = t_1 + (k-1)s$, обчислено агреговану кількість інцидентів для кожної категорії інцидентів $f_{kj} = \sum_{t \in W_k} x_j(t),\ j = 1, \ldots, m$ та визначено матрицю агрегованих ознак $F = \{f_{kj}\} \in R^{n \times m}$, де n – кількість вікон, що відповідає станам системи. Всі задані параметри імітаційного моделювання задані в Таблиці 4.7.

Крок 4. Визначено параметри керування та інтегральний показник критичності для задачі кластеризації. На даному етапі проводилось групування категорій інцидентів у 5 параметрів керування відповідно до математичної основи удосконаленого методу в розділі 3.2. Встановлено множину параметрів керування $Z_k = (z_{k1}, \ldots, z_{k5})$, де $z_{k1} = \sum f_k(1.01)$, $z_{k2} = \sum f_k(2.01 - 2.04)$, $z_{k3} = \sum f_k(3.01 - 3.03)$, $z_{k4} = \sum f_k(6.01 - 6.03)$, $z_{k5} = \sum f_k(9.01 - 9.02)$.

Таблиці 4.7

Параметри імітаційного моделювання для задачі кластеризації на основі даних 2022 - 2024 років

Параметр	Значення	Визначення
L	14 днів	довжина ковзного вікна
s	7 днів	крок зсуву (перекриття 50%)
n	132	кількість сформованих вікон/станів
K	3	кількість кластерів (Stable/Degraded/Critical)

Також, визначено інтегральний показник критичності як нормована сума параметрів

$$R_k = \frac{\sum_{i=1}^{5} z_{ki} - min(\sum z)}{max(\sum z) - min(\sum z)},$$

де $R_k \in [0,1]$ і визначається як мінімальна інтенсивність загроз при $R_k \approx 0$ і максимальна інтенсивність загроз при $R_k \approx 1$ (Рис.4.7). Як приклад сформованих 5 параметрів та R_k для 10 вікон представлено в Таблиці.8.

Таблиця 4.8

Параметри керування та інтегральний показник критичності для $W_k = 10$

W_id	Start	End	z_k1	z_k2	z_k3	z_k4	z_k5	R_k
1	01.04.2022	14.04.2022	267.0	5789.0	68.0	16.0	2.0	0.02
2	08.04.2022	21.04.2022	539.0	6618.0	57.0	19.0	8.0	0.03
3	15.04.2022	28.04.2022	506.0	3814.0	84.0	16.0	21.0	0.01
4	22.04.2022	05.05.2022	495.0	6924.0	126.0	9.0	139.0	0.04
5	29.04.2022	12.05.2022	451.0	5991.0	260.0	1.0	132.0	0.03
6	06.05.2022	19.05.2022	445.0	5804.0	328.0	7.0	23.0	0.03
7	13.05.2022	26.05.2022	485.0	7102.0	137.0	7.0	27.0	0.04
8	20.05.2022	02.06.2022	526.0	7448.0	24.0	1.0	23.0	0.04
9	27.05.2022	09.06.2022	673.0	8068.0	92.0	1.0	24.0	0.05
10	03.06.2022	16.06.2022	789.0	7365.0	184.0	0.0	23.0	0.04

Як видно з графіка на Рис. 4.7 період 10.2023 по 01.2024 вказує на максимальне фіксування кіберінцидентів.

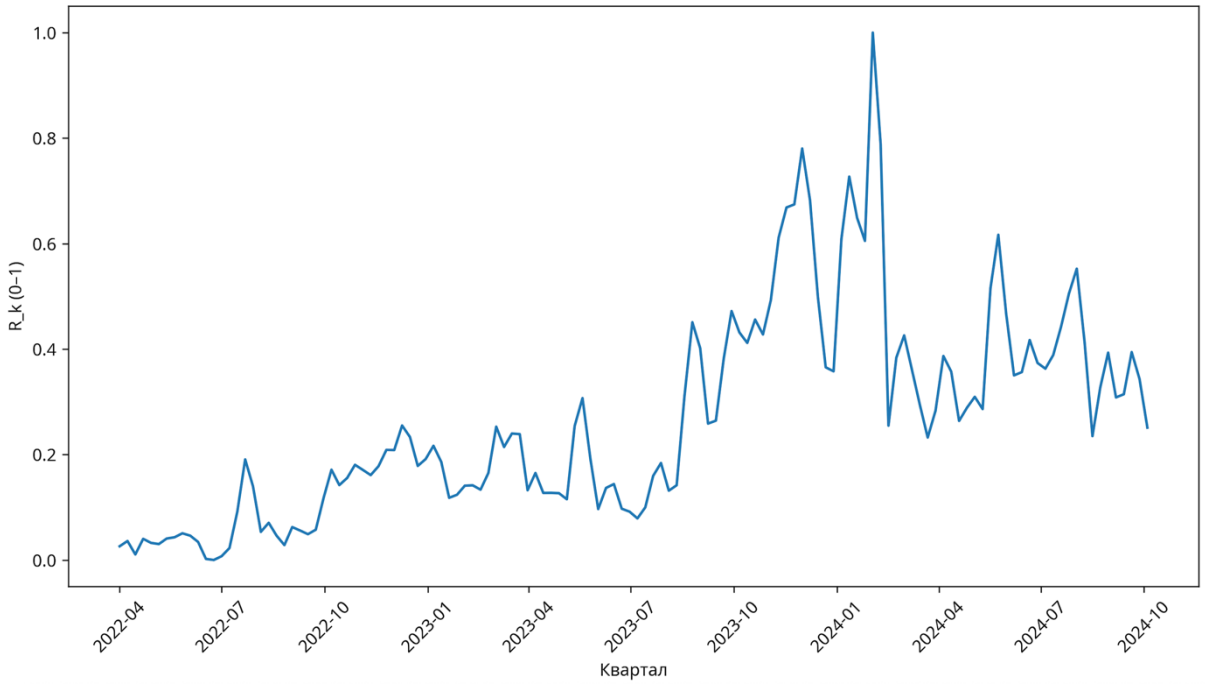


Рис. 4.7 Графік інтегрального показника критичності R_k відповідно кварталам 2022 - 2024 років

Крок 5. Здійснено кластеризацію агрегованих станів системи. Для початку сформовано простір ознак $S_k = (z_{k1}, \ldots, z_{k5}, R_k)$ та виконано метод $z - score$ стандартизація $S_k^* = \frac{S_k - \mu}{\sigma}$.

Надалі застосовано метод k-means з параметром $k = 3$ з мінімізацією функціоналу $J = \sum_{i=1}^{K} \sum_{S_k \in C_i} \|S_k - \mu_i\|^2$ та визначенням кластерів, які впорядковано за середнім значенням R_k: Stable, Degraded, Critical. Для візуалізації 6-вимірний простір переводять у 2-х вимірний, де PC1 та PC2 вказують напрямок найбільшої варіації даних (Рис. 4.8)

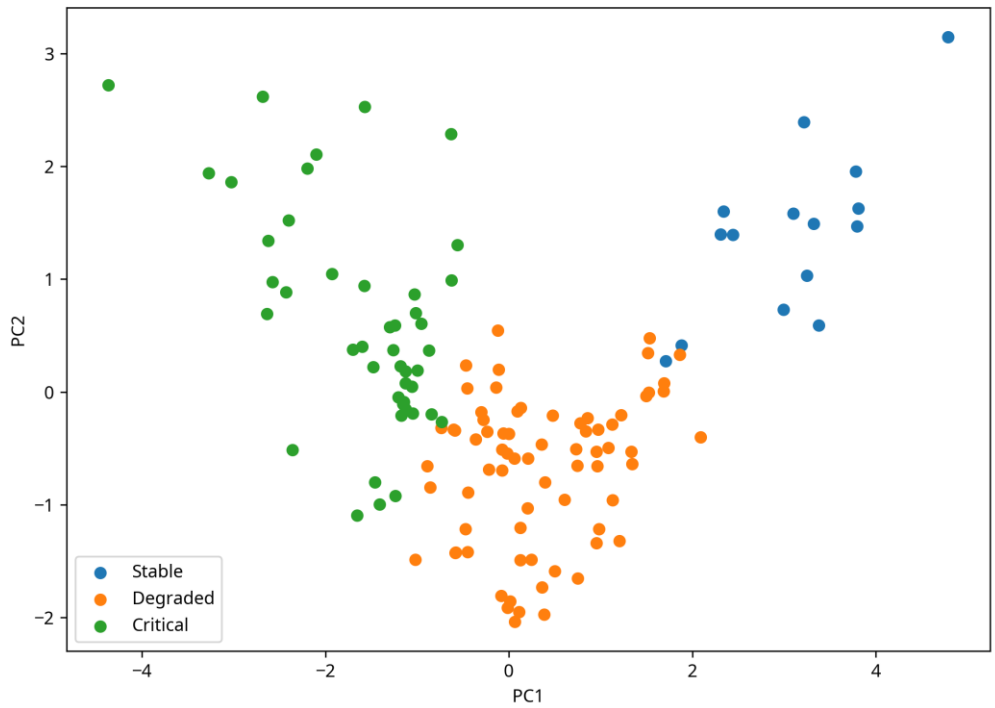


Рис. 4.8 Просторове розподілення режимів функціонування системи за допомогою 3-х кластерів

4.2.2. Порівняння та оцінка ефективності удосконаленого методу кластеризації загроз та вразливостей

В роботі [100] проведено аналіз найбільш поширених методів кластерного аналізу та їх застосування в системах інформаційної та кібербезпеки, що дозволило виділити два основних методи для оцінки ефективності удосконаленого методу кластеризації загроз та уразливостей. Для порівняння методів виділено метод k-means та DBSCAN (Density-Based Spatial Clustering of Applications with Noise), які виділено як базові алгоритми для кластеризації даних. Метод k-means застосовується для групування немаркованих точок даних у групи або кластери за допомогою центроїдів, які визначаються як середні значення або медіани всіх точок у кластері залежно від характеристик даних [169]-[173]. Метод DBSCAN працює на основі щільності, який групує точки даних, щільно упаковані одна з одною, та позначає викиди як шум на основі їхньої щільності в просторі ознак. Він ідентифікує кластери як щільні області в просторі даних, розділені областями з нижчою щільністю. На відміну від k-means або ієрархічної кластеризації, які

припускають, що кластери компактні та сферичні, DBSCAN добре справляється з обробкою реальних нерівномірностей даних [174]-[176].

Важливо для оцінки якості кластеризації даних методів застосувати набір внутрішніх метрик кластеризації, які дозволили оцінити компактність кластерів, точність класифікації, чутливість до викидів, стабільність у часовому вимірі. Для визначення ефективності удосконаленого методу кластеризації загроз та уразливостей та порівняння з існуючими методами, обчислено коефіцієнт силуету (Silhouette Score), який показує ступінь подібності даних до вказаного кластеру в порівнянні з сусідніми кластерами [177].

Математично коефіцієнт силуету (Silhouette Score) для елемента i задається

$$S(i) = \frac{b(i) - a(i)}{max(a(i), b(i))},$$

де $a(i) = \frac{1}{|\mathrm{C}_i|-1}\sum_{j\in C_i, j\neq i} d(i,j)$ – середня відстань між елемента i та іншими елементами даного кластеру, $b(i) = \min_{k\neq i}(\frac{1}{|\mathrm{C}_k|}\sum_{j\in C_k} d(i,j))$ – мінімальна середня відстань між елемента i та елементами інших кластерів, C_i – кластер з елементом i, C_k – сусідні кластери, $d(i,j)$ – відстань між i та j, $S(i) \in [-1,1]$, при цьому $S(i) \approx 1$ показує про найкраще відокремлення кластерів.

Для оцінки співвідношення між внутрішньою дисперсією кластерів та відстані між їх центрами обчислено індекс Девіса-Болдіна (DB), який математично задається формулою

$$DB = \frac{1}{K}\sum_{i=1}^{K} \max_{j\neq i}\left(\frac{\sigma_i+\sigma_j}{d(c_i,c_j)}\right),$$

де K – кількість кластерів, σ_i – дисперсія $i-$ ого кластера, $d(c_i, c_j)$ – відстань між центрами кластерів, і при цьому чим менше значення DB, тим більша відстань між кластерами [178].

Щоб оцінити компактність кластерів і чи вони відокремленні у багатовимірних даних використано індекс Данна (D), який задається математично

$$D = \min_i \left\{ \min_j \left(\frac{\min\limits_{x \in C_i, y \in C_j} d(x,y)}{\max_k \left\{ \max_{x,y \in C_k} d(x,y) \right\}} \right) \right\},$$

де $\max_{x,y \in C_k} d(x,y)$ – найбільша відстань між точками (x, y) одного кластера C_k, $\min\limits_{x \in C_i, y \in C_j} d(x,y)$ – найменша відстань між точками різних кластерів C_i та C_j. При $D \rightarrow$ велике маємо, що кластери далеко один від одного і вони компактні, в при $D \rightarrow$ мале значення маємо, що кластери перекриваються і вони розмиті [178].

Важливими метриками для оцінки здатності системи підтримувати стабільність в часі [179]-[180] при застосуванні даних методів визначено також показник кластерної стабільності (St), показник оцінки часової узгодженості (TCI) та показник зменшення шуму Noise Reduction (NR).

Таким чином, обчислено метрики для оцінки ефективності удосконаленого методу кластеризації загроз та уразливостей та проведено порівняння даних метрик для методі k-means та DBSCAN, з використанням реального набору даних фіксованих кіберінцидентів за 2022-2024 роки. Результати порівняння отриманих показників наведено в Таблиці 4.9.

Аналіз отриманих результатів показав, що удосконалений метод кластеризації загроз та уразливостей має найкращі показники. Інтерпретація даних результатів вказує на те, що класичні методи кластеризації показали обмежену ефективність при аналізі часових рядів заданих кіберінцидентів. Так, найменше значення показника якості кластеризації (S) та найбільше значення показника компактності кластерів (DB) вказують на те, що при метод k-means спостерігається

перекриття кластерів, а метод DBSCAN зменшує шум в даних, але має найменше значення показника стабільності кластерної структури (St).

Таблиці 4.9

Порівняння метрик для оцінки ефективності методів кластеризації загроз та уразливостей

Критерій	Показник	Методи кластеризації		
		K-Means	DBSCAN	Удоскон. метод
Якість кластеризації	S	0,138	0,189	**0,425**
Компактність кластерів	DB	1,773	1,439	**1,106**
Відокремленість кластерів	D	0,011	0,275	**0,31**
Стабільність кластерної структури	St	0,664	0,577	**0,985**
Часова узгодженість	TCI	0,664	0,577	**0,985**
Зменшення шуму	NR	0	0	**0,858**
Врахування часової динаміки	Temp. Aggr.	Ні	Ні	**Так**

Таким чином, удосконалений метод кластеризації загроз та уразливостей забезпечує високу часову узгодженість (0,985), використання ковзних часових рядів дозволяє зменшити шум в даних на 85,8%, також отримані результати вказують на високе розділення елементів між кластерами, внутрішню узгодженість кластерів та їх відокремленість. Для візуального представлення кластеризації даних здійснено графічне інтерпретацію даних методами k-means, DBSCAN та удосконаленим методом (Рис.4.9) за допомогою Python на наборі даних кіберінцидентів за 2022 -2024 роки.

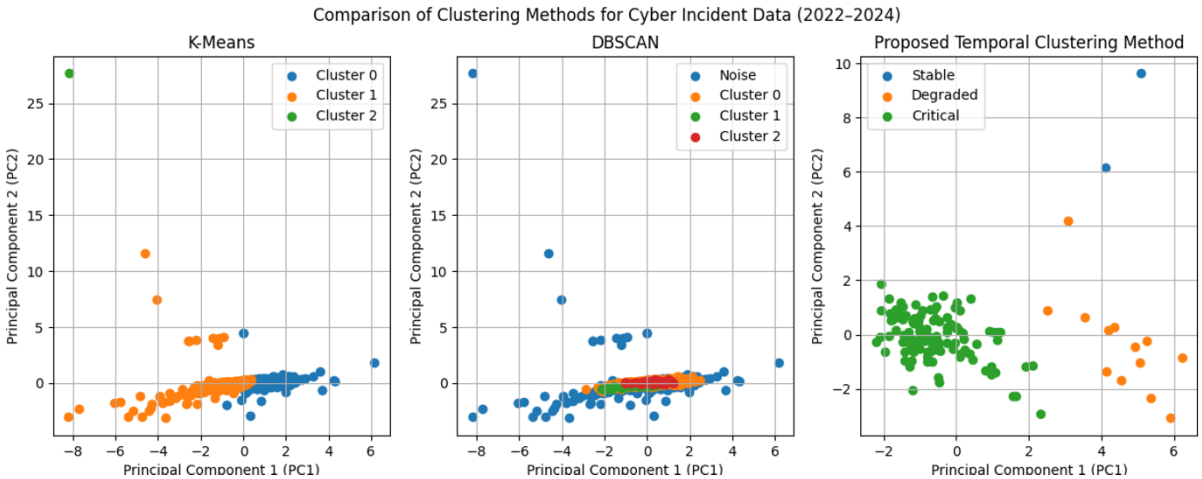


Рис. 4.9 Порівняння методів кластеризації даних про кіберінциденти за (2022-2024)

На даному графіку для візуалізації даних, що мають складну структуру типів кіберінцидентів, використано метод аналізу головних компонентів (PC1 та PC2), які дозволили зменшити розмірність даних та відобразити дані у 2-х вимірному просторі.

4.3. Експериментальна оцінка ефективності моделі прогнозування критичних переходів станів системи при інтеграції з SIEM-системою

Як відомо**,** система управління інформацією та подіями безпеки (SIEM) відповідає за агрегування та аналіз даних безпеки з різних джерел у військовій інформаційні системі для виявлення, аналізу та реагування на кіберзагрози в режимі реального часу. Системи SIEM збирають дані журналів з кінцевих точок, серверів, програм, рішень для ідентифікації, захисту електронної пошти та інших джерел, що дозволяє виявляти підозрілі події та блокувати потенційні загрози. Таким чином, системи SIEM проводять моніторинг загроз у режимі реального часу, тому забезпечують також попередження про критичну інформацію для усунення наслідків від виявлених інцидентів [181].

4.3.1. Постановка мети та завдання експериментального дослідження

В розділі 3.3 розроблено модель прогнозування критичних переходів на основі інтеграції теорії катастроф у SIEM-системи. Для оцінки ефективності даної моделі проведено експериментальне дослідження за допомогою середовища Python, бібліотек NumPy, Pandas, Scikit-learn, Matplotlib та SciPy, що дозволило перевірити всі можливості розробленої моделі щодо виявлення нестійких режимів функціонування інформаційної системи, а також прогнозування критичних переходів при інтеграції її у SIEM- систему. Використано набір щоденних кіберінцидентів за період 2022 -2024 років, які надані відділом кібербезпеки ЗСУ.

Початковий аналіз наданих даних показав 934 часових спостережень, які розподілені між 21 категоріями кіберінцидентів. Проведено очищення та нормалізацію даних, агрегацію інцидентів у часових вікнах, а також побудовано вектор стану інформаційної системи для подальшого застосовування удосконаленого методу кластеризації станів інформаційною системи, що дозволило визначити динаміку переходів між режимами функціонування інформаційної системи для проведення аналізу отриманих станів за допомогою моделі катастроф типу «Метелик», який розроблено в розділі 3.1.

Встановлено набір метрик, щоб оцінити основні характеристики розробленої моделі прогнозування критичних переходів на основі інтеграції теорії катастроф у SIEM-системи. До даних метрик відносять метрику точності (Precision), яка показує відсоток дійсних критичних станів у відношенні до хибних спрацювань системи, а саме

$$Prescision = \frac{TP}{TP + FP},$$

де TP $(True\ Positive)$ – кількість виявлених критичних станів, FP $(False\ Positive)$ – кількість хибних спрацювань системи. При цьому чим більше значення $Prescision$, тим менше система має хибних спрацювань [182].

Кількісне значення метрика повноти (Recall) показує, на скільки розроблена модель прогнозування критичних переходів виявляє всі можливі критичні стани системи. Для обчислення значення Recall використано формулу

$$Recall = \frac{TP}{TP + FN},$$

де $TP\ (True\ Positive)$ – кількість виявлених критичних станів, $FN\ (False\ Negative)$ – кількість критичних станів, які не виявлені. Також, більше значення показника $Recall$ вказує на те, що система пропускає менше кіберінцидентів [183].

Для оцінки балансу між точністю та повною виявлених кіберінцидентів використано метрику F1-score за допомогою формули

$$F1 = \frac{Precision \times Recall}{Precision + Recall},$$

яка при більшому значення F1 вказує на більш збалансовану модель [184].

Візуальне представлення матриці помилок (Confusion Matrix), яка задається Таблицею 4.10, допомагає провести оцінку структури вірних та хибних рішень системи.

Таблицею 4.10

Загальний вигляд матриці помилок (Confusion Matrix)

Стан системи	**Predicted Normal**	**Predicted Critical**
Actual Normal	TN	FP
Actual Critical	FN	TP

Основними показниками в матриці помилок (Confusion Matrix) визначено 4-х позиції, які визначають кількість спрацювань системи. Так, TN (Tru Negative) вказує на кількість нормальних станів, TP (Tru Positive) показує кількість

критичних станів, FP (False Positive) визначає кількість хибних спрацювань системою, FN (False Negative) показує кількість пропущених інцидентів [184].

Важливо також оцінити, як система прогнозує нестійкі стани. Саме тому використано метрику часу попередження (Early Warning Time), яку розраховано за формулою

$$EWT = t_m - t_{pr},$$

де t_{pr} – час прогнозу нестійкого стану, t_m – час фіксації критичного стану, а також для більшого значення показника EWT роблять висновок, що система раніше попереджає про настання критичного стану системи [185].

Для оцінки ефективності розробленої моделі прогнозування критичних переходів станів системи точно визначати критичні переходи станів інформаційної системи обчислюють частку критичних переходів (CTDR), які прогнозовані системою [186], а саме

$$CTDR = \frac{TP}{TP+FN},$$

де TP(Tru Positive) – кількість прогнозованих критичних переходів станів системи, FN (False Negative) – кількість критичних переходів станів системи, які не були прогнозовані. Таким чином, можна $CTDR$ вказує на ймовірність фіксування критичних переходів станів системи.

4.3.2. Результати та аналіз експериментальної оцінки ефективності розробленої моделі

Оцінка ефективності моделі прогнозування критичних переходів станів системи при інтеграції з SIEM-системою проведена на основі знайдених результатів метрик, які представлені в розділ 4.3.1 для SIEM систем з різними

режимами роботи (Таблиця 4.11), а саме стандартна SIEM та SIEM із інтегрованою моделлю прогнозування критичних станів системи [128], [187].

Таблиця 4.11

Порівняння основних характеристик стандартної SIEM – системи та SIEM – системи із інтегрованою моделлю прогнозування критичних станів

Функція	**Стандартна SIEM**	**SIEM із інтегрованою моделлю прогнозування критичних станів**
Збір даних	Збір журналів подій із мережевих пристроїв, серверів, IDS/IPS	Збір журналів подій із мережевих пристроїв, серверів, IDS/IPS
Нормалізація подій	Перетворення журналів подій у категорії інцидентів	Перетворення журналів подій у категорії інцидентів
Агрегація подій	Так (групування подій за часовими інтервалами)	Так (додатково застосовується **агрегація у ковзному часовому вікні** для аналізу динаміки інцидентів)
Кореляція подій	Так	Так (кореляція подій + **аналіз трендів** кіберінцидентів)
Аналіз інцидентів	Аналіз після виникнення інциденту	Аналіз із використанням **моделі прогнозування**
Класифікація станів системи	Ні	**Так** (на основі удосконаленого методу кластеризації станів системи)
Виявлення нестійких станів	Ні	**Так** (аналіз нестійких режимів функціонування системи)
Прогнозування критичних переходів	Ні	**Так** (на основі моделі катастрофи типу "Метелик")
Фіксація аномалій	Так (на основі правил)	Так (основі **динаміки зміни** станів системи)
Формування попереджень	Так (генерація сигналів після виявлення інциденту)	Так (генерація **попереджень** до настання критичного стану)
Підтримка прийняття рішень	Так	Так (управління **кіберстійкістю** системи)

Таким чином, розроблена модель прогнозування критичних станів системи, на відміну від класичної SIEM, дозволяє проводити аналіз динаміки кіберінцидентів, прогнозувати критичні переходи станів систем, а також виявляти нестійкі режими функціонування інформаційної системи до моменту фіксації критичних загроз та уразливостей.

Виявлені переваги функціональних можливостей SIEM-системи із інтегрованою моделлю прогнозування критичних станів підтверджені також кількісними значеннями основних метрик, які також обчислено для двох досліджуваних SIEM - систем. Результати знайдених оцінок наведено в Таблиці 4.12. та Рис. 4.10.

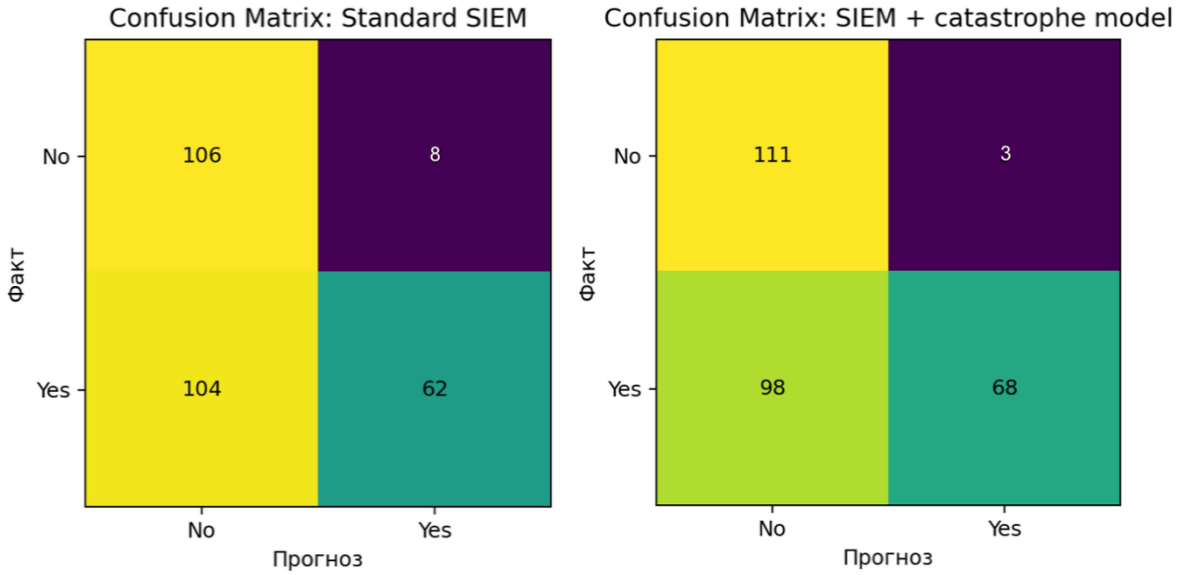


Рис.4.10 Матриці помилок (Confusion Matrix) для стандартної SIEM та SIEM із модулем прогнозування критичних станів системи

Проведений аналіз кількісних (Таб. 4.12, Рис.4.10) і якісних (Таб.4.11) значень показав, що SIEM – система з інтегрованою моделлю прогнозування критичних станів має вищу точність виявлення критичних станів системи на 7,2 % від стандартної SIEM відповідно до показника Precision (0.958).

Таблиці 4.12.

Оцінка ефективності підходів щодо виявлення критичних переходів станів системи

Модель	**Метрики для оцінки**				
	Precision	**Recall**	**F1**	**CTDR**	**EWT**
Стандартна SIEM	0.886	0.373	0.525	0.373	0 днів
SIEM + модель прогнозування критичних станів системи	**0.958**	**0.410**	**0.574**	**0.410**	**2–3 дні**

Отримані значення в матрицях помилок (Confusion Matrix) показали, що кількість FT для розробленої моделі становить 3, а для стандартної SIEM становить 8. Таким чином, показник False Positive підтверджує, що SIEM з інтегрованою розробленою моделлю на 62,5% менше спрацьовує на хибні сигнали.

Також, на основі отриманих значень показника Recall встановлено, що SIEM з інтегрованою розробленою моделлю на 3,7 % виявляє більше критичних станів інформаційної системи в порівняні зі стандартною SIEM.

Отримані значення інтегрального показника F1 вказує на те, що SIEM з інтегрованою розробленою моделлю працює ефективніше на 4,9% в порівняні зі стандартною SIEM.

Показник CTDR показав, що SIEM з інтегрованою розробленою моделлю на 3,7% точніше фіксує нестійкі режими функціонування інформаційної системи.

Важливо відмітити, що використання моделі прогнозування критичних станів дозволяє прогнозувати за 2-3 дні про критичні можливі переходи в станах інформаційної системи, що підтверджується метрикою EWT.

Таким чином, отримані результати експериментального дослідження підтверджують ефективність використання моделі прогнозування критичних станів з удосконаленим методом кластеризації загроз та уразливостей та моделі катастрофи типу «Метелик» у SIEM-систему для підвищення рівня кіберстійкості інформаційної системи.

4.4. Оцінка ефективності удосконаленого методу підтримки прийняття рішень для забезпечення кіберстійкості військових інформаційних систем

Для виявлення нестабільних станів СУІБ, що піддається впливу кіберінцидентами, доцільно застосувати удосконалений метод підтримки прийняття рішень для забезпечення кіберстійкості військових інформаційних систем, який базується на інтеграції математичних моделей, методів аналізу та прогнозування. Запропонований метод в розділі 3.4 забезпечує комплексне виявлення, класифікацію та прогнозування критичних станів, що дозволяє своєчасно попереджати розвиток небезпечних кіберінцидентів. Основою даного методу є математичний апарат теорії катастроф, який дозволяє описувати інформаційні системи, які мають ряд параметрів. Серед яких динамічність, тобто стан системи змінюється в часі, інерційність, система прагне зберегти свій поточний стан якомога довше, гістерезис (поточний стан залежить від шляху, яким система до нього дійшла), а також незворотність (зміна параметрів у зворотному напрямку не гарантує повернення системи до початкового стану). При моделюванні складних інформаційних системи дані властивості відіграють ключові ролі, оскільки рішення та ризики в інформаційній безпеці мають нерівноважну та асиметричну динаміку [148].

4.4.1. Умови та сценарії дослідження ефективності удосконаленого методу

Для побудови сценаріїв реагування системи прийняття рішень на основі теорії катастроф використано реальні статистичні дані кіберінцидентів за період 2022 – 2024 роки, а також запропоновану в розділі 3.1 катастрофу типу «метелик».

Набір даних включає 934 спостережень та 21 категорію кіберінцидентів, які класифіковані відповідно до переліку категорій кіберінцидентів [89]. В розділі 4.1 проведено аналіз даних та виділено 5 категорій кіберінцидентів (Рис.4.1), які мають найбільшу вагу впливу на стан інформаційної системи, а саме Спам (Spam),

Шкідливе програмне забезпечення (Malware), Збір інформації зловмисником (Information Gathering), Порушення доступності та відмови (DoS/DDos), Уразливості (Vulnerable).

Застосовано удосконалений метод кластеризації загроз та уразливостей, який розроблено в розділі 3.2 і підтверджено його ефективність в розділі 4.2, для визначення трьох кластерів, які відповідають нормальному стану системи (Stable), напруженому (Degraded) та критичному станів (Critical). Для формування даних кластерів використано параметри імітаційного моделювання для задачі кластеризації, які наведені в Таблиці 4.7., де визначено $n = 132$ ковзних вікна з 934 днів спостережень, $L = 14$ днів, що відповідає довжині ковзного вікна та $s = 7$ днів, що задає крок зсуву. На основі наданих параметрів сформовано центри кластерів C_1, C_2, C_3, наведено в Таблиці 4.13.

Таблиці 4.13.

Центри кластерів для визначення трьох станів системи
на 5 категорій кіберінцидентів

Кластер	**Spam**	**Malware**	**Information Gathering**	**DoS/DDoS**	**Vulnerable**	**Стан**
C1	142.80	5584.27	311.93	19.33	23.00	**Stable**
C2	28143.73	18.00	1037.24	221.27	51.76	**Degraded**
C3	38055.64	27.92	1568.85	98.26	76.20	**Critical**

Проведено аналіз переходів між станами системи, кількість яких вказано в Таблиці 4.14 за допомогою матриці переходів між станами системи. Встановлено, що існує перехід між станами Degraded та Critical, що вказує на нелінійну динаміку появи кіберзагроз, тому доцільно застосувати теорію катастроф для представлення даних змін станів інформаційної системи.

Таблиці 4.14

Показники матриці переходів між станами системи

Поточний стан	**Наступний стан**	**Кількість переходів**	**Ймовірність переходів**
Stable	Stable	41	0.62
Stable	Degraded	19	0.29
Stable	Critical	6	0.09
Degraded	Stable	15	0.27
Degraded	Degraded	28	0.51
Degraded	Critical	12	0.22
Critical	Stable	4	0.08
Critical	Degraded	18	0.35
Critical	Critical	29	0.57

Для візуального представлення побудовано траєкторію переходів станів системи для 132 ковзних вікон, які представлені на Рис. 4.11.

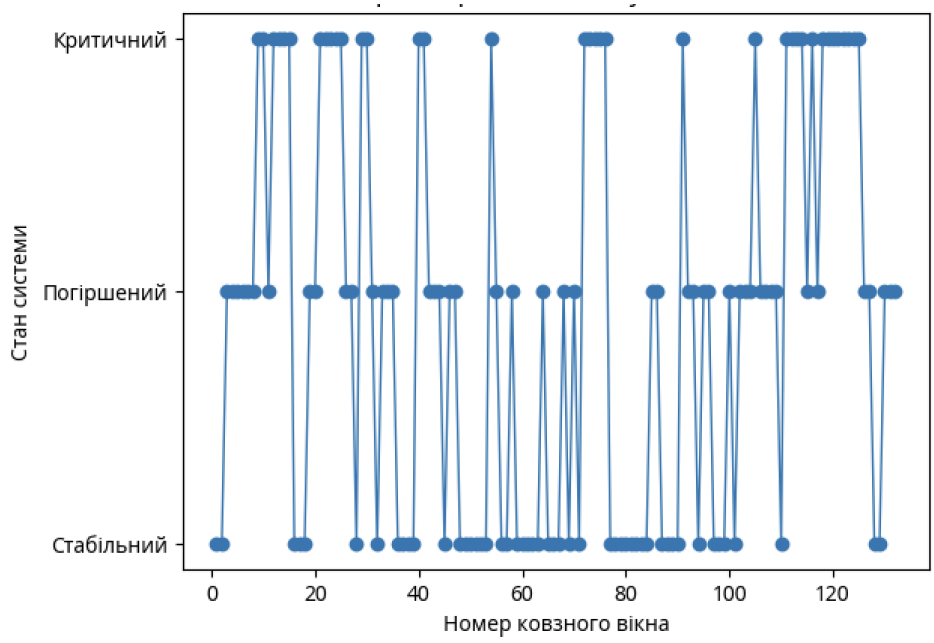


Рис. 4.11. Траєкторія переходів станів системи для 132 ковзних вікна

Наступним етап вводиться катастрофа типу «Метелик», що задається узагальненим рівнянням потенціалу

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

де $x \in R$ – поточний стан інформаційної системи,

$c, d \in R$ – змінні параметри, які показують вплив різних категорій кіберінцидентів на всю систему та визначаються за допомогою вагових значень коефіцієнтів.

Щоб показати всі можливі зміни стану системи x і реагування на них системи прийняття рішень, використано модифікований градієнтний спуск

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

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

де $\alpha, \alpha \in (0; 1)$ – крок зміни, $x_0 = 0{,}5$ – початковий стан системи.

Зміна стану системи при зміні параметрів призводить до переходів між станами і порушення стану рівноваги. Дані переходи фіксуються пороговими значеннями [58], [128], [150]:

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

де $\tau > 0$.

Враховано, що стан системи $x, x \in R$ в моделі катастрофи «Метелик» коливається в межах від 0 до 1, тобто при $|\tau| \in [0; 1]$ система перебуває в стані

рівноваги. При зміні $|\tau| > 1$ система переходить у фазу потенційної біфуркації, а при $|\tau| > 1{,}5$ наступає початок зони нестійкості системи. Математичним поясненням даних змін виступають точки інфлексії потенціалу, тобто визначення нульових похідних 2-го порядку. Практично важливим поясненням за захисту інформаційної системи є те, що при $|\tau| > 1{,}5$ наступає стан, коли загальна кількість кіберінцидентів перевищує інерційний опір системи, тобто система втратила здатність адаптуватися і виникає ймовірність настання критичного порушення всієї системи). Тому важливий баланс між чутливістю системи і її стабільністю, оскільки при $|\tau| < 1$, система видає часті хибні спрацювання, а при $|\tau| > 2$ система може не спрацювати вчасно на небезпечні зміни.

4.4.2. Аналіз результатів та оцінка ефективності удосконаленого методу

Проведено моделювання за допомогою інструментів та бібліотек Python, що дозволило визначити перший день реагування системи прийняття рішення з 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"
}

Для отримання всіх можливих станів реагування системи прийняття рішення реалізовано 4 сценарії симуляції з різними параметрами за допомогою Python, реального набору значень кіберінцидентів, які зафіксовано за 2022 – 2024 роки, а також допустимих змін параметрів при моделюванні. Зазначені сценарії наведено в Таблиці 4.15.

Таблиці 4.15.

Сценарії моделювання різних станів реагування системи прийняття рішення на виявлені кіберінциденти

Етап	**Конфігурація**	**Метрики**	**Реакція системи**	**Висновок**
1	Базові вагові коефіцієнти Malware = 0.9809; крок зміни стану $\alpha = 0.01$	Mean x ≈ 0.48 $\Delta x/day \approx 0.01$ PS = 0	Визначено у 100% випадків	Система перебуває у стабільному та контрольованому стані.
2	Підсилення інтенсивності загроз: Malware ×3, Spam ×2; крок $\alpha = 0.05$	Mean x ≈ 0.12 $\Delta x/day \approx 0.03$ IPS = 0	Визначено у 100% випадків	Зміна динаміки стану системи, проте система залишається в межах області стійкості.
3	Сценарій атаки: Malware > 500; підвищені вагові коефіцієнти; відсутність обмеження градієнта	x = NaN $\nabla F(x) \rightarrow \infty$	Режим функціонування падає, фіксується катастрофічний перехід стану системи	Фіксується нестійкість системи та реалізаціїя сценарію катастрофи
4	Помірна атака: Malware ≈ 300; gradient: ±1000	Mean x ≈ ±18 $\Delta x/day \approx 1.5$ PS = 6	Активація IPS при кожному переході через критичну область стану	Система переходить у нестійкий режим; модель фіксує нелінійну динаміку ризику; включається захист системи

На основі проведеного дослідження встановлено, що модель реагування системи прийняття рішень на основі теорії катастроф, який реалізується за допомогою удосконаленого методу прийняття рішень, виступає аналітичною оболонкою над потоком SIEM -даних і дозволяє виявляти критичні зміни стану

(біфуркаційні переходи), адаптуватись системі до динаміки кіберзагроз, а також поєднувати автоматичне та експертне реагування на виявлені кіберінциденти.

Для оцінки ефективності удосконаленого методу підтримки прийняття рішень вирішено здійснити порівняння основних кількісних метрик для методу машинного навчання, а саме алгоритму Support Vector Machine (SVM) та Random Forest, які застосовують для аналізу кіберінцидентів у SIEM-системах. Проте удосконалений метод підтримки прийняття рішень для забезпечення кіберстійкості військових інформаційних систем застосовується для фіксування критичних переходів станів інформаційної системи, тому потрібно порівнювати метрики, які вказують на точність виявлення критичних станів системи та оцінювати, чи метод може прогнозувати ранні переходи системи в критичний стан.

Сценарій 1. Порівняння метрик Precision, Recall, F1-score та ROC-AUC [188], математична основа яких описана в розділі 4.3, для критичного стану інформаційної системи Critical та поєднання станів Stable та Degraded. За допомогою такого підходу встановлено, чи методи можуть виявляти критичні стани системи. В середовищі Python з відповідними бібліотеками проведено обчислення відповідних метрик для зазначених методів підтримки прийняття рішень (Таб.4.16).

Сценарій 2. Порівняння метрик Precision, Recall, F1-score та Balanced Accuracy [189], для випадку реагування системи на перехід до стану Critical на кроці t+1. В даному випадку здійснюється можливість методу визначати стан системи, оцінювати ризики переходу системи в різні стани, а також приймати рішення, щодо реагування даної системи на виявлені критичні кіберзагрози. Результати обчислень наведено в Таблиці 4.17.

Проведено дослідження методів підтримки прийняття рішень для забезпечення кіберстійкості військових інформаційних систем за допомогою комп’ютерного моделювання в середовищі Python для оцінки їх реагування та прогнозування на переходи системи в критичні стани.

Таблиця 4.16

Порівняння методів підтримки прийняття рішень
для критичного стану Critical

Метод	**Precision (Critical)**	**Recall (Critical)**	**F1-score**	**ROC-AUC**
SVM	0.74	0.68	0.71	0.81
Random Forest	0.79	0.72	0.75	0.84
Удосок. метод	**0.83**	**0.88**	**0.85**	**0.87**

Таблиця 4.17

Порівняння методів підтримки прийняття рішень
для прогнозування критичного стану Critical

Метод	**Precision**	**Recall**	**F1-score**	**Balanced Accuracy**
SVM	0.70	0.64	0.67	0.73
Random Forest	0.75	0.69	0.72	0.77
Удосок. метод	**0.81**	**0.86**	**0.83**	**0.84**

Знайдені метрики показують, що удосконалений метод підтримки прийняття рішень має показник Recall для виявлення критичних станів вищий на 16%, а для сценарію прогнозування на 17%, відповідно F1 для сценарію 1 вищий на 10% та на 11% для сценарію 2. Збільшення ROC-AUX до 0,87 підтверджує те, що за допомогою удосконаленого методу можна розрізняти критичні стани системи. Таким чином, удосконалений метод підтримки прийняття рішень на основі удосконаленого методу кластеризації загроз та теорії катастроф має більшу ефективність виявляти критичні стани інформаційної системи та забезпечує прогнозування змін в станах системи для прийняття рішень щодо реагування на можливі кіберінциденти.

Висновки до розділу 4.

1. Проведено комп'ютерне моделювання математичної моделі катастрофи типу «Метелик» для прогнозування критичних станів системи за допомогою набору кіберінцидентів за 2022-2024 роки та середовища Python з бібліотекою Pandas для обробки даних, математичних обчислень та чисельного моделювання. Визначено показники $\Delta T, K_{cov}, FAR\ , I$ для лінійної моделі агрегованого ризику, моделі ранніх попереджувальних сигналів CSD та розробленої математичної моделі катастрофи типу «Метелик», щоб оцінити їх ефективность для прогнозування критичних станів системи при дії на неї загроз та уразливостей. Проведений аналіз показав, що модель катастрофи типу «Метелик» має ряд переваг та дозволяє структурно та обґрунтовано прогнозувати моменти втрати стійкості системи та виявляти передкризові режими до моменту виявлення критичних станів системи.
2. Проведено імітаційне моделювання удосконаленого методу кластеризації загроз та уразливостей для виявлення переходів між стабільними, змінними та критичними станами інформаційної системи. Здійснено порівняння методів k-means та DBSCAN, які виділено як базові алгоритми для кластеризації даних, з удосконаленим методом кластеризації загроз та уразливостей за допомогою метрик Silhouette Score, індекс Девіса-Болдіна, індекс Данна, стабільності кластерних структур, часової узгодженості, часової динаміки та зменшення шуму. Встановлено, що удосконалений метод кластеризації загроз та уразливостей має найкращі показники при аналізі часових рядів заданих кіберінцидентів в порівнянні з класичними методами кластеризації загроз та уразливостей.
3. Для оцінки ефективності моделі прогнозування критичних переходів станів системи при інтеграції з SIEM-системою проведено експериментальне дослідження за допомогою середовища Python, що дозволило перевірити всі можливості розробленої моделі щодо виявлення нестійких режимів

функціонування інформаційної системи, а також прогнозування критичних переходів при інтеграції її у SIEM- систему. За допомогою метрик Precision, Recall, F1-score, Confusion Matrix, $CTDR$ та EWT та порівняння двох SIEM систем з різними режимами роботи, встановлено ефективність використання моделі прогнозування критичних станів з удосконаленим методом кластеризації загроз та уразливостей та моделі катастрофи типу «Метелик» в SIEM-системі для підвищення рівня кіберстійкості інформаційної системи.

4. Побудовано сценарії реагування системи на кіберзагрози на основі удосконаленого методу підтримки прийняття рішень для забезпечення кіберстійкості військових інформаційних систем. Визначено перший день реагування системи прийняття рішення з Decision = «ACTIVATE_IPS» для набору досліджуваних фіксованих загроз за 2022-2024 роки., а також наведено 4 сценарії для можливих станів реагування системи прийняття рішень з відповідними параметрами. На основі метрик для методу машинного навчання здійснено порівняння удосконаленого методу з методом Support Vector Machine (SVM) та Random Forest, які застосовують для аналізу кіберінцидентів у SIEM-системах, та визначено переваги удосконаленого методу для виявлення критичних станів інформаційної системи та прогнозування змін в станах системи для прийняття рішень щодо реагування на можливі кіберінциденти.

ВИСНОВКИ

У ході проведеного дослідження були вирішені всі поставлені завдання і відповідно до мети отримані наступні **результати:**

- проаналізовано сучасні підходи забезпечення кібербезпеки військових інформаційних систем та визначено особливості нелінійної динаміки їх станів під впливом кіберінцидентів;
- обґрунтовано доцільність застосування математичної теорії катастроф та теорії конфліктів для моделювання динаміки станів інформаційних системи під впливом кіберінцидентів;
- розроблено математичну модель впливу кіберінцидентів на стійкість систем управління інформаційною безпекою з використанням катастрофи типу «Метелик» та проведено оцінку її ефективності;
- удосконалено метод кластеризації загроз та уразливостей інформаційних систем та проведено порівняльну оцінку його ефективності з класичними методами кластеризації;
- розроблено модель прогнозування критичних переходів станів інформаційної системи при інтеграції з SIEM-системою та проведено оцінку ефективності її застосування для раннього виявлення нестійких режимів функціонування системи;
- удосконалено метод підтримки прийняття рішень для забезпечення кіберстійкості військових інформаційних систем, особливістю якого є поєднання математичного апарату теорії конфліктів для симуляції відбиття атак та теорії катастроф для ідентифікації ризиків переходу системи у критичний стан;
- проведено оцінку ефективності удосконаленого методу підтримки прийняття рішень шляхом імітаційного моделювання сценаріїв реагування на кіберінциденти.

Одержані результати дають підстави зробити наступні **висновки**:

1. В умовах стрімкого збільшення інтенсивності кібератак та скорочення часу на їх реагування, проблема забезпечення інформаційної безпеки у військових ІТ-системах набуває статусу критично важливого завдання. Аналіз наукових джерел виявив деякі обмеження в існуючих технологіях захисту інформації, зокрема, не враховується або частково забезпечується динамічна та конфлікта взаємодія загроз та уразливостей у інформаційному середовищі та залишається без уваги нелінійність процесу у цьому середовищі, що призводить до непередбачуваних критичних станів і втрати кіберстійкості системи. У зв'язку з цим розробка моделей та методів забезпечення кібербезпеки військових ІТ-систем на основі математичних теорій конфліктів та катастроф є актуальною.

2. Вперше розроблено математичну модель впливу кіберінцидентів на стійкість систем управління інформаційною безпекою з використанням катастрофи типу «Метелик», що дозволяє прогнозувати перехід системи до небезпечного стану. Проведено комп'ютерне моделювання в середовищі Python для оцінки ефективності математичної моделі катастрофи типу «Метелик» та порівняння її показників якості з показниками лінійної моделі агрегованого ризику та моделі ранніх попереджувальних сингалів CSD. Встановлено, що запропонована модель показує найбільше значення середнього часу раннього попередження $\overline{\Delta T} \approx 7$ міс., формує сигнал про перехід системи до критичну стану за 5-8 місяців до його настання. Крім того, модель забезпечує 100% покриття періодів, де настають критичні стани системи та дозволяє виявляти на ранніх етапах біфуркаційні точки, в яких відбувається перехід системи до нестабільного стану. Використання запропонованої моделі збільшує в 2,5 рази час попередження про перехід стану системи до критичного. Таким чином, нелінійна модель катастрофи типу «Метелик» надає більше часу для стратегічного реагування.

3. Удосконалено метод кластеризації загроз та уразливостей, який враховує часову динаміку кіберінцидентів, що дозволяє зберігати 98,5% кластерної структури у часі (TCI = 0.985). Запропонований метод має вищу якість кластеризації (S=0.425), що на 24% більше ніж у K-means та DBSCAN, та кращу

компактність сформованих кластерів, на що вказує менше значення індексу Девіса-Болдіна (DB=1.106), що на 37.6 % нижчий ніж у методі K-means та 23%, ніж в DBSCAN. Обґрунтовано використання ковзних часових рядів у запропонованому методі, що дозволяє зменшити шум в даних приблизно на 85%. Отримані результати вказують на високе розділення елементів між кластерами, внутрішню узгодженість кластерів та їх відокремленість, що зменшує суб'єктивність експертних оцінок і підвищує об'єктивність управління ризиками у військових інформаційних системах.

4. Вперше запропоновано модель прогнозування критичних переходів, яка забезпечує підвищення рівня кіберстійкості військових інформаційних систем за рахунок інтеграції теорії катастроф у SIEM-системи. Проведено експериментальне дослідження за допомогою середовища Python, бібліотек NumPy, Pandas, Scikit-learn, Matplotlib та SciPy для стандартної SIEM та SIEM із інтегрованою моделлю прогнозування критичних станів системи. Встановлено, що

- дана модель демонструє вищу точність виявлення критичних станів системи на 7,2 % від стандартної SIEM відповідно до показника Precision (0.958);

- показник False Positive підтверджує, що SIEM з інтегрованою розробленою моделлю на 62,5% менше спрацьовує на хибні сигнали;

- показники Recall та CTDR доводять, що SIEM з інтегрованою розробленою моделлю на 3,7 % виявляє більше критичних станів інформаційної системи та точніше фіксує нестійкі режими функціонування інформаційної системи;

- отримані значення інтегрального показника F1 вказують на те, що SIEM з інтегрованою розробленою моделлю працює ефективніше на 4,9% в порівняні зі стандартною SIEM.

Таким чином, на відміну від традиційних підходів моніторингу кіберінцидентів, запропонована модель забезпечує виявлення нестійких режимів функціонування системи та формування сигналів про перехід системи до критичного стану. Використання даної моделі дозволяє SIEM-системі за 2-3 дні

сформувати попередження про перехід інформаційної системи до критичного стану.

5. Набув подальшого розвитку метод підтримки прийняття рішень у процесі забезпечення кіберстійкості військових інформаційних систем, який базується на інтеграції математичних моделей, методів аналізу та прогнозування на основі теорій конфліктів та катастроф. Проведено комп'ютерне моделювання в середовищі Python для оцінки методів машинного навчання (SVM, Random Forest) та удосконаленого методу для виявлення та прогнозування критичних станів. Виділено два сценарії для моделювання. У межах першого сценарію було проведено оцінку ефективності методу за метриками Precision, Recall, F1-score та ROC-AUC, де цільовим завданням була класифікація стану системи на «Critical» та об'єднаний клас «Stable/Degraded». Аналіз отриманих даних підтвердив вищу результативність удосконаленого методу: показник Precision зріс на 12,2 %, Recall — у середньому на 22 %, а значення ROC-AUC — на 7,4 % порівняно з аналогами, що свідчить про його підвищену здатність до ідентифікації критичних станів. Сценарій 2 був спрямований на перевірку точності прогнозування критичного стану системи на кроці t+1. Аналіз результатів моделювання показав, що удосконалений метод має вищу ефективність при прогнозуванні переходів системи до критичного стану, оскільки має значення Precision на 15.7 %, Recall в середньому на 24% та Balanced Accuracy на 9.1 % вищими в порівнянні з алгоритмами SVM та Random Forest.

Таким чином, мета дослідження щодо підвищення кіберстійкості військових інформаційних систем за рахунок розробки моделей та методів забезпечення кібербезпеки на основі застосування математичної теорії катастроф та теорії конфліктів для аналізу та моделювання складної нелінійної динаміки функціонування систем під впливом кіберзагроз і прогнозування критичних переходів їх станів досягнута.

Наукові та практичні результати можуть бути використані державними та військовими структурами при розробці та удосконаленні систем передавання інформації на об’єктах інформаційної діяльності критичної інфраструктури.

В якості пріоритетних напрямів подальших досліджень планується інтеграція запропонованих моделей у системи моніторингу кібербезпеки державних і військових структур.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Державна служба спеціального зв'язку та захисту інформації України. (2025). Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки: Річний звіт 2024. https://scpc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927c88006
2. Державна служба спеціального зв'язку та захисту інформації України. (2026). Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки: річний звіт 2025. https://scpc.gov.ua/uk/articles/402
3. Visiongain. (2024). Military cyber security market report 2024–2034. Research and Markets. https://surl.li/fabhmp
4. Міністерства оборони України. (2025). Галузевий профіль безпеки систем, де обробляється відкрита, конфіденційна або службова інформація. https://surl.li/ffcuzk
5. Levis, A., Wagenhals, L. (2000). C4ISR architectures: I. Developing a process for C4ISR architecture design. Systems Engineering, 3(4), 225–247. https://doi.org/10.1002/1520-6858(2000)3:4%3C225::AID-SYS4%3E3.0.CO;2-%23
6. Sowell, P. K. (2000). The C4ISR Architecture Framework: History, Status, and Plans for Evolution. The MITRE Corporation McLean, Virginia. https://www.mitre.org/sites/default/files/pdf/sowell_evolution.pdf
7. Плугова, О., Зінченко, М., Яковчук, О., Лазута, Р., Макарчук, В., Коваленко, І., Ткаченко, А., Атаманенко, М. (2024). Світові тенденції зі створення та розвитку автоматизованих систем управління збройними силами. *Національні інтереси України. Розділ «Воєнні науки, національна безпека, безпека державного кордону»*, 1(1), 103–115. https://doi.org/10.52058/3041-1572-2024-1(1)-103-115
8. Тимчук, В. (2024). Інформаційно-аналітичні основи мілітарних систем із систем на емерджентних і еволюційних властивостях. *Сучасні інформаційні технології у сфері безпеки та оборони*, 3(51), 108–119. https://doi.org/10.33099/2311-7249/2024-51-3-108-119

9. Office of the Deputy Under Secretary of Defense for Acquisition and Technology, Systems and Software Engineering. (2008). *Systems Engineering Guide for Systems of Systems. Version 1.0.* Washington, DC: ODUSD (A&T) SSE. https://surl.lu/uqzboe
10. National Institute of Standards and Technology. (2020). Security and Privacy Controls for Information Systems and Organizations: NIST Special Publication 800-53 Revision 5. Gaithersburg, MD: NIST. https://doi.org/10.6028/NIST.SP.800-53r5
11. Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., Mcquaid, R. (2019). Developing Cyber Resilient Systems: A Systems Security Engineering Approach. National Institute of Standards and Technology, NIST Special Publication 800-160, 2. https://doi.org/10.6028/NIST.SP.800-160v2
12. Blakely, B., Billings, H., Evans, N., Landry, A., Domingo, A. (2023). Evaluation of an autonomous intelligent cyberdefense agent at NATO cyber coalition exercise 2022. *Proceedings of SPIE: Disruptive Technologies in Information Sciences VII*, 12542. https://doi.org/10.1117/12.2662959
13. Живило, Є., Шевченко, Д., Черноног, О. (2021). Типологія систем кібербезпеки в інформаційно-телекомунікаційних системах військового (спеціального) призначення. *Сучасні інформаційні технології у сфері безпеки та оборони. Київ, Україна*, 42(3), 37–44. https://doi.org/10.33099/2311-7249/2021-42-3-37-44
14. Farooq, M. J., Zhu, Q. (2018). On the Secure and Reconfigurable Multi-Layer Network Design for Critical Information Dissemination in the Internet of Battlefield Things (IoBT). *In IEEE Transactions on Wireless Communications*, 17(4), 2618–2632. https://doi.org/10.1109/TWC.2018.2799860
15. NATO. (2024). Cyber defence. https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence
16. Jajodia, S., Cybenko, G., Subrahmanian, V. S., Swarup, V., Wang, C., & Wellman, M. (2020). *Adaptive autonomous secure cyber systems*. Springer, 290. https://doi.org/10.1007/978-3-030-35746-7
17. NATO. (2024). Interoperability: a Cornerstone Concept of NATO. https://www.act.nato.int/article/interoperability-cornerstone-concept/

18. Systematic. Multilateral Interoperability Programme: exchanging information with your coalition partners. https://surli.cc/jonqyz
19. Sahu, K., Kumar, R., Srivastava, R. K., Singh, A. K. (2025). Military Computing Security: Insights and Implications. Journal of The Institution of Engineers: Series B, 106, 1091–1115. https://doi.org/10.1007/s40031-024-01136-6
20. Franke, U., & Brynielsson, J. (2014). Cyber situational awareness – A systematic review of the literature. *Computers & Security, 46*, 18–31. https://doi.org/10.1016/j.cose.2014.06.008
21. Behzadan, V. (2017). Cyber-Physical Attacks on UAS Networks-Challenges and Open Research Problems. https://doi.org/10.48550/arXiv.1702.01251
22. Максимов І. О., Загоровець О. В. (2025). Аналіз методів приховування інформації в інформаційнокомунікаційних системах військового призначення. *Системи і технології зв'язку, інформатизації та кібербезпеки*, 8, 124–132. https://doi.org/10.58254/viti.8.2025.10.124
23. Levy, E., Maman, N., Shabtai, A., Elovici, Y. (2022). AnoMili: Spoofing Prevention and Explainable Anomaly Detection for the 1553 Military Avionic Bus. https://doi.org/10.48550/arXiv.2202.06870
24. Amanullazade, F. (2025). Ensuring cybersecurity in military communications through threat analysis and defense measures. V Міжнародна наукова конференція «Інтелектуальний ресурс сьогодення: наукові задачі, розвиток та запитання», 229–238. https://doi.org/10.62731/mcnd-29.08.2025.010
25. Крючкова, Л., Шандрук, М. (2025). Методи протидії в радіонавігаційних конфліктах. Кібербезпека: освіта, наука, техніка, 4(28), 766–780. https://doi.org/10.28925/2663-4023.2025.28.863
26. TajDini, M., Sokolov, V., Skladannyi, P. (2021). Performing sniffing and spoofing attack against ADS-B and Mode S using software defined radio. *Proceedings of the IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo)*, 7–11. https://doi.org/10.1109/UkrMiCo52950.2021.9716665

27. Ahmad, H., Dharmadasa, I., Ullah, F., Babar, M. A. (2021). A Review on C3I Systems' Security: Vulnerabilities, Attacks, and Countermeasures. https://doi.org/10.48550/arXiv.2104.11906

28. Машталір, В., Гук, О., Толмачов, І., Фараон, С. (2023). Прогнозування ступеню кібервпливу на гетерогенні інформаційні системи військового призначення з урахуванням його еволюції. *Сучасні інформаційні технології у сфері безпеки та оборони*, 48(3), 147–156. https://doi.org/10.33099/2311-7249/2023-48-3-147-156

29. Constantinescu, M. (2025). Building resilience against cybersecurity risks in military transportation networks. *International Conference Knowledge-Based Organization*, 31(1), 71–78. https://doi.org/10.2478/kbo-2025-0008

30. Stan, O., Elovici, Y., Shabtai, A., Shugol, G., Tikochinski, R., Kur, S. (2017). Protecting Military Avionics Platforms from Attacks on MIL-STD-1553 Communication Bus. https://doi.org/10.48550/arXiv.1707.05032

31. Unal, B. (2019). Cybersecurity of NATO's Space-based Strategic Assets. Chatham House. https://www.chathamhouse.org/2019/07/cybersecurity-natos-space-based-strategic-assets

32. Brannsten, M. R., Johnsen, F. T., Bloebaum, T. H., Lund, K. Toward (2015). Federated Mission Networking in the Tactical Domain. IEEE Communications Magazine, 53(10). https://doi.org/10.1109/MCOM.2015.7295463

33. Vollmer, B. (2021). NATO's Mission-Critical Space Capabilities under Threat: Cybersecurity Gaps in the Military Space Asset Supply Chain. https://doi.org/10.48550/arXiv.2102.09674

34. Radu, R. (2025). Building Cyber Resilience to Face the Challenges of Cognitive Warfare. *The Proceedings of the 24th European Conference on Cyber Warfare and Security (ECCWS)*, 803–810. https://doi.org/10.34190/eccws.24.1.3520

35. Горгуленко, В. (2024). Кіберборотьба у воєнних конфліктах сучасності: передовий досвід, тенденції та закономірності розвитку. Сучасні інформаційні технології у сфері безпеки та оборони, 2(50), 11–28. https://doi.org/10.33099/2311-7249/2024-50-2-11-28

36. Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G., Steinhardt, J., Flynn, C., hÉigeartaigh, S., Beard, S., Belfield, H., Farquhar, S., & Amodei, D. (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. Future of Humanity Institute, University of Oxford. https://arxiv.org/pdf/1802.07228.pdf

37. Boyens, J., Paulsen, C., Moorthy, R., & Bartol, N. (2015). Supply Chain Risk Management Practices for Federal Information Systems and Organizations. NIST Special Publication 800-161, National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-161

38. Гуцалюк, М.В. (2025). Кіберзагрози під час гібридної війни та протидія організованій кіберзлочинності. *Інформація і право*, 1(52), 123–131. https://doi.org/10.37750/2616-6798.2025.1(52).324708

39. S&P Global. (2024). What is Cyber Warfare? https://surl.li/hiiops

40. Chen, P., Desmet, L., & Huygens, C. (2014). A Study on Advanced Persistent Threats. Communications and Multimedia Security, Springer, 3–18. https://doi.org/10.1007/978-3-662-44885-4_1

41. Maathuis, C., Cools, K. (2025). Digital Sovereignty Control Framework for Military AI-based Cyber Security. https://doi.org/10.48550/arXiv.2509.13072

42. Sharma, V. (2025). Advanced Persistent Threat (APT) Detection Using SIEM: A Review of Techniques and Tools. *Engineering And Technology Journal*, *10*(7), 5738–5746. https://doi.org/10.47191/etj/v10i07.21

43. Смірнова, Т., Константинова, Л., Конопліцька-Слободенюк, О., Козлов, Я., Кравчук, О., Козірова, Н., Смірнов, О. (2024). Дослідження сучасного стану SIEM-систем. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, *1*(25), 6–18. https://doi.org/10.28925/2663-4023.2024.25.618

44. Корнієць, В., Складанний, П. (2024). Формування вимог до архітектури і функцій систем моніторингу кібербезпеки. *Телекомунікаційні та інформаційні технології*, 4(85), 90–96. https://doi.org/10.31673/2412-4338.2024.040224

45. Beckmeyer, M., Phadke, A. (2025). Blockchain-Enhanced SIEM for Defense Networks. https://doi.org/10.13140/RG.2.2.17269.84964

46. Шевченко, С., Жданова, Ю., Кія, О. (2025). Напівавтоматизований інструмент багатостандартної оцінки кіберзрілості організації на основі NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019 та CIS Controls v8. *Кібербезпека: освіта, наука, техніка*, 3(31), 43–60. https://doi.org/10.28925/2663-4023.2025.31.1004

47. Жданова, Ю., Шевченко, С., Спасітєлєва, С., Сокульський, О. (2024). Прийняття рішень на основі лінійної оптимізації у процесі управління ризиками інформаційної безпеки. *Кібербезпека: освіта, наука, техніка*, 1(25), 330–343. https://doi.org/10.28925/2663-4023.2024.25.330343

48. Fahrurozi, M., Tarigan, Tanjung, M., Mutijarsa, K. (2020). The Use of ISO/IEC 27005: 2018 for Strengthening Information Security Management (A Case Study at Data and Information Center of Ministry of Defence), 86-91. https://doi.org/10.1109/ICITEE49829.2020.9271748

49. Ross, R. (2012). Guide for conducting risk assessments (NIST Special Publication 800-30 Revision 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-30r1

50. Veluri, Y., Ramprasad, S. (2023). Operationally Critical Threat, Asset and Vulnerability Evaluation. https://surl.li/gtlzlv

51. Ferdinandsyah, R., Novita, A., Atmodjo, D., Nugroho, F. D. (2025). Enhancing access control security using ISO 27001:2013 and OCTAVE method. Bit-Tech, 8(1), 459–466. https://doi.org/10.32877/bt.v8i1.2590

52. Young, L., Cebula, J. (2014). A taxonomy of operational cyber security risks Version 2. https://doi.org/10.13140/RG.2.2.23973.91363

53. Nakonechnyi, V., Mordvyntsev, M., Husieva, V., Lutsenko, V. (2025). Hybrid approach to information security risk management. Information Systems and Technologies Security, 1(9), 32–41. https://doi.org/10.17721/ISTS.2025.9.32-41

54. Freund, J., Jones, J. (2025). Measuring and managing information risk: A FAIR approach. https://doi.org/10.1016/C2022-0-02439-9

55. Araujo, M. S., Machado, B. A. S., Passos, F. U. (2024). Resilience in the context of cyber security: A review of the fundamental concepts and relevance. Applied Sciences, 14(5), 2116. https://doi.org/10.3390/app14052116

56. Палко, Д., Мирутенко, Л. (2025). Метод побудови профілю ключових факторів ризику кібербезпеки сучасних розподілених інформаційних систем. *Захист інформації*, 26(2), 236–252. https://doi.org/10.18372/2410-7840.26.20014

57. Іваночко, Т., Семенюк, С. (2025). Управління ризиками кібербезпеки з використанням NIST CSF 2.0. *Сучасний захист інформації*, 3(63), 75–82. https://doi.org/10.31673/2409-7292.2025.030936

58. Шевченко, С., Жданова, Ю., Спасітєлєва, С. (2023). Математичні методи в кібербезпеці: теорія катастроф. *Кібербезпека: освіта, наука, техніка*, 3(19), 165–175. https://doi.org/10.28925/2663-4023.2023.19.165175

59. Thom, R. (1972). Stabilité structurelle et morphogénèse. New York, Benjamin, 362.

60. Marais, M. S., Steenpaß, A. (2013). The classification of real singularities using SINGULAR. Part I: Splitting lemma and simple singularities. *Journal of Symbolic Computation*, 68, 61–71. https://doi.org/10.1016/j.jsc.2014.08.007

61. Marszalek, W., Walczak, M. (2024). Bifurcation diagrams of nonlinear oscillatory dynamical systems: A brief review in 1D, 2D and 3D. *Entropy*, 26(9), 770. https://doi.org/10.3390/e26090770

62. Alpcan, T., Başar, T. (2010). Network security: A decision and game-theoretic approach. *Cambridge University Press*, IV(9), 219–243. https://doi.org/10.1017/CBO9780511760778

63. Manshaei, M., Zhu, Q., Alpcan, T., Başar, T., Hubaux, J.-P. (2013). Game theory meets network security and privacy. *ACM Computing Surveys*, 45(3), 1–39. https://doi.org/10.1145/2480741.2480742

64. Sun, R., Zhu, Y., Fei, J., Chen, X. (2023). A survey on moving target defense: Intelligently affordable, optimized and self-adaptive. *Applied Sciences*, 13(9), 5367. https://doi.org/10.3390/app13095367

65. Shevchenko, S., Zhdanova, Y., Astapenya, V., Nehodenko, O., & Spasiteleva, S. (2024). Conflicting subsystems in the information space: A study at the software and hardware levels. *Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2024)*, CEUR Workshop Proceedings, 3654, 333–342. https://ceur-ws.org/Vol-3654/paper28.pdf

66. Rieger, C., Kolias, C., Ulrich, J., McJunkin, T. (2020). A cyber resilient design for control systems. *Proceedings of the 2020 Resilience Week (RWS)*, 18–25. https://doi.org/10.1109/RWS50334.2020.9241300

67. Nicol, D., Sanders, W., Trivedi, K. (2004). Model-based evaluation of security. *IEEE Transactions on Dependable and Secure Computing*, 1(1), 48–65. https://sites.pitt.edu/~dtipper/3957/Paper7.pdf

68. Xu, S., Lu, W., Li, H. (2015). A Stochastic model of active cyber defense dynamics. *Internet Mathematics*, 134, 1–9. https://doi.org/10.1080/15427951.2013.830583

69. Lysenko, S., Bobrovnikova, K., Savenko, O., Shchuka, R. (2020). Technique for cyberattacks detection based on DNS traffic analysis. *In 16th International Conference on ICT in Education, Research and Industrial Applications (ICTERI 2020) Workshops*, 2732, 171–182. https://ceur-ws.org/Vol-2732/20200171.pdf

70. Kavallieratos, G., Spathoulas, G. P., Katsikas, S. K. (2021). Cyber risk propagation and optimal selection of cybersecurity controls for complex cyberphysical systems. *Sensors*, 21(5), 1691. https://doi.org/10.3390/s21051691

71. Roy, S., Ellis, C., Shiva, S., Dasgupta, D., Shandilya, V., Wu, Q. (2010). A survey of game theory as applied to network security. *In 43rd Hawaii International Conference on System Sciences (HICSS)*, 1–10. https://doi.org/10.1109/HICSS.2010.35

72. Zhu, Q., Başar, T. (2015). Game-theoretic methods for robustness, security, and resilience of cyber-physical control systems: An overview. IEEE Control Systems Magazine, 35(1), 46–65. https://doi.org/10.1109/MCS.2014.2364710

73. Ahmed, Y., Azad, M. A., Asyhari, T. (2024). Rapid forecasting of cyber events using machine learning-enabled features. *Information*, 15(1), 36. https://doi.org/10.3390/info15010036

74. Sun, R., Zhu, Y., Fei, J., Chen, X. (2023). A survey on moving target defense: Intelligently affordable, optimized and self-adaptive. *Applied Sciences*, 13(9), 5367. https://doi.org/10.3390/app13095367

75. Жданова, Ю., Спасітєлєва, С., Шевченко, С. (2019). Застосування бібліотеки класів Security.Cryptography для практичної підготовки спеціалістів з кібербезпеки. *Кібербезпека: освіта, наука, техніка*, 4(4), 44–53. https://doi.org/10.28925/2663-4023.2019.4.4453

76. Бурячок, В., Шевченко, С., Складанний, П. (2018). Віртуальна лабораторія моделювання процесів інформаційної та кібербезпеки як форма формування практичних навичок студентів. *Кібербезпека: освіта, наука, техніка*, 2(2), 98–104. https://doi.org/10.28925/2663-4023.2018.2.98104

77. Бурячок, В., Шевченко, С., Жданова, Ю., Складанний, П. (2021). Міждисциплінарний підхід до формування навичок управління ризиками інформаційної безпеки на основі теорії прийняття рішень. *Кібербезпека: освіта, наука, техніка*, 3(11), 155–165. https://doi.org/10.28925/2663-4023.2021.11.155165

78. Руснак, І., Шевченко, В., Артемов, Ю. (2002). Методологічні засади створення інтегрованої навчально-тренувальної системи оперативної та бойової підготовки військ. *Наука і оборона*, 2, 29–35.

79. Казмірчук, Р. В. (2012). Обґрунтування пропозицій щодо впровадження в процес бойової підготовки форм і методів навчання, заснованих на використанні сучасних систем імітаційного моделювання: НДР. Академія сухопутних військ ім. гетьмана Петра Сагайдачного. № держреєстрації 0213U007682.

80. Майстренко, О., Бубенщиков, Р., Стецiв, С. (2020). Застосування засобів імітаційного моделювання у процесі підготовки майбутніх офіцерів збройних сил України до виконання службових обов'язків. *Інформаційні технології і засоби навчання, 75*(1), 186–201. https://surl.li/zxntsp

81. Заїка, Л., Лаврінчук, О., Крайнов, В. (2021). Використання можливостей засобів імітаційного моделювання бойових дій у ході практичної підготовки органів військового управління. *Інтерактивні моделі розвитку науково-освітнього простору у сфері безпеки та оборони, 3*(42), 89–96. https://doi.org/10.33099/2311-7249/2021-42-3-89-96

82. Шевченко, С., Складанний, П., Негоденко, О., Негоденко, В. (2022). Дослідження прикладних аспектів теорії конфліктів у системах безпеки. Кібербезпека: освіта, наука, техніка, 2(18), 150–162. https://doi.org/10.28925/2663-4023.2022.18.150162

83. Zalcman, L., Blacklock, J., Foster, K., Lawrie, G. (2012). An air operations division live, virtual and constructive (LVC) corporate interoperability standards development strategy. Fishermans Bend, Vic.: Defence Science and Technology Organisation, 74–77. https://apps.dtic.mil/sti/pdfs/ADA559423.pdf

84. U.S. Army. (2012). *Homestation Instrumentation Training System (HITS): External Standard Operating Procedure*. https://home.army.mil/carson/8316/4918/4018/hits-external-sop.pdf

85. Bocetta, S. (2022). Resolving the Conflict Between Availability and Security in IT. *Security Bloggers Network. https://surl.li/daptbs*

86. Alkubaisy, D. (2021). A Framework Managing Conflicts between Security and Privacy Requirements. https://research.brighton.ac.uk/files/25764156/Alkubaisy_Thesis.pdf

87. Boonstra, A., Jan de Vries. (2015). Information system conflicts: causes and types. *International Journal of Information Systems and Project Management, 3*(4), 5–20. https://doi.org/10.12821/ijispm030401

88. Schmitt, M. (2012). Classification of Cyber Conflict. *Journal of Conflict and Security Law, 17*(2), 245–260. https://doi.org/10.1093/jcsl/krs018

89. CERT-UA. (2021). Перелік категорій кіберінцидентів. https://cert.gov.ua/recommendation/16904

90. Шевченко, С., Жданова, Ю., Спасітєлєва, С., Негоденко, О., Мазур, Н., & Кравчук, К. (2019). Математичні методи в кібербезпеці: фрактали та їх застосування в

інформаційній та кібернетичній безпеці. *Кібербезпека: освіта, наука, техніка,* 1(5), 31–39. https://doi.org/10.28925/2663-4023.2019.5.3139

91. Шевченко, С., Жданова, Ю., Складанний, П., & Спасітєлєва, С. (2021). Математичні методи в кібербезпеці: графи та їх застосування в інформаційній та кібернетичній безпеці. *Кібербезпека: освіта, наука, техніка*, 1(13), 133–144. https://doi.org/10.28925/2663-4023.2021.13.133144
92. Shevchenko, S., Zhdanova, Y., Shevchenko, H., Nehodenko, O., & Spasiteleva, S. (2023). Conflict Analysis in the "Subject-to-Subject" Security System. CEUR Workshop Proceedings, 3421, 56–66. https://ceur-ws.org/Vol-3421/paper6.pdf
93. Шевченко, С., Жданова, Ю., Складанний, П., & Бойко, С. (2023). Теоретико-ігровий підхід до моделювання конфліктів у системах інформаційної безпеки. *Кібербезпека: освіта, наука, техніка*, 2(22), 168–178. https://doi.org/10.28925/2663-4023.2023.22.168178
94. Levkin, D., Zhernovnykova, O., Synyavina, Y., & Levkin, A. (2023). Variability of the choice of the mathematical models in applied security problems. *Scientific Notes of Taurida National V. I. Vernadsky University. Series: Technical Sciences*, 5, 152–157. https://doi.org/10.32782/2663-5941/2023.5/24
95. Лисенко, Н., Мазуренко, В., Федорович, А., Астахов, Д., & Стаценко В. (2021). Огляд математичних методів у системах виявлення та попередження кіберзагроз. *Актуальні проблеми автоматизації та інформаційних технологій*, 25, 91–102. http://dx.doi.org/10.15421/432110
96. The MITRE Corporation. (2025). MITRE ATT&CK® framework. https://attack.mitre.org/
97. OASIS Open. (2021). TAXII Version 2.1 Standard. https://docs.oasis-open.org/cti/taxii/v2.1/
98. Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, 72, 212–233. https://doi.org/10.1016/j.cose.2017.09.001

99. Aggarwal, C., Reddy, C. (2014). Data Clustering: Algorithms and Applications. *Chapman & Hall/CRC*, 111–160. https://www.charuaggarwal.net/clusterbook.pdf

100. Негоденко, В., Шевченко, С., Жданова, Ю., Спасітєлєва, С., Мазур, Н., & Складанний, П. (2024). Математичні методи в кібербезпеці: кластерний аналіз та його застосування в інформаційній та кібернетичній безпеці. *Кібербезпека: освіта, наука, техніка*, 3(23), 258–273. https://doi.org/10.28925/2663-4023.2024.23.258273

101. Негоденко, В. (2024). Застосування математичної теорії катастроф для забезпечення стійкості системи управління інформаційною безпекою. *Кібербезпека: освіта, наука, техніка*, 2(26), 212–222. https://doi.org/10.28925/2663-4023.2024.26.692

102. Negodenko, O., Shevchenko, S., Trintina, N., Astapenya, V., & Tereshchenko, O. (2021). Problematic issues of approximation and interpolation in signal processing in secure information systems. In *Cybersecurity Providing in Information and Telecommunication Systems*, 3187(1), 276–283. http://ceur-ws.org/Vol-3187/

103. Poston, T., Stewart, I. (1978). Catastrophe Theory and Its Applications. *London: Pitman, 30–68.* https://archive.org/details/catastrophetheor0000post

104. Saunders, P. T. (1980). An Introduction to Catastrophe Theory. *Cambridge: Cambridge University Press*, 2–60.

105. Негоденко, В. (2023). Дослідження інформаційних конфліктів у системі навчання ЗСУ за допомогою імітаційного моделювання. *Кібербезпека: освіта, наука, техніка*, 4(20), 164–173. https://doi.org/10.28925/2663-4023.2023.20.164173

106. Alhidaifi, S. M., Asghar, M. R., & Ansari, I. S. (2024). A Survey on Cyber Resilience: Key Strategies, Research Challenges, and Future Directions. *ACM Computing Surveys*, 56(8(196)), 1–48. https://doi.org/10.1145/3649218

107. Bottou, L. (2012). Stochastic gradient descent tricks. In Neural Networks: Tricks of the Trade. *Springer*, 421–436. https://leon.bottou.org/publications/pdf/tricks-2012.pdf

108. Schneider, F. B. (2000). Enforceable security policies. *ACM Transactions on Information and System Security (TISSEC)*, 3(1), 30–50. https://doi.org/10.1145/353323.353382

109. Wanigasekara, C. (2026). Nonlinear system modelling and control: Trends, challenges, and future perspectives. *Computation*, 14(2), 44. https://doi.org/10.3390/computation14020044

110. Bu, C. (2018). Network Security Based on K-Means Clustering Algorithm in Data Mining Research. *Advances in Computer Science Research*, 83, 642–645. https://doi.org/10.2991/snce-18.2018.130

111. Cheon, J. H., Kim, D., & Park, J. H. (2020). Towards a practical cluster analysis over encrypted data. *Selected Areas in Cryptography – SAC 2019*, 11959, 227–249. https://doi.org/10.1007/978-3-030-38471-5_10

112. Raptis, G., Katsini, C., Alexakos, C. (2021). Towards automated matching of cyber threat intelligence reports based on cluster analysis in an Internet-of-Vehicles environment. *IEEE International Conference on Cyber Security and Resilience (CSR)*, 366–371. https://doi.org/10.1109/CSR51186.2021.9527983

113. Gao, Y., Li, X., Peng, H., Fang, B., Yu, P. S. (2022). A Cyber Threat Intelligence Modeling and Identification System Based on Heterogeneous Information Network. *IEEE Transactions on Knowledge and Data Engineering*, 34(2), 708–722. https://doi.org/10.1109/TKDE.2020.2987019

114. Lee, C. J., Poh, J. P., Tan, K. X., & Tan, E. (2020). Physical access log analysis: An unsupervised clustering approach for anomaly detection. *In the 3rd International Conference on Data Science and Information Technology*, 12–18. https://doi.org/10.1145/3414274.3414285

115. Rosli, N., Jantan, A., Sulaiman, R. (2019). Clustering analysis for malware behavior detection using registry data. *International Journal of Advanced Computer Science and Applications (IJACSA)*, 10(12), 93–102. http://dx.doi.org/10.14569/IJACSA.2019.0101213

116. Лисенко, С., Гуменюк, В. (2017). Метод виявлення шкідливих програмних засобів на основі алгоритму найближчих сусідів. *Вісник Хмельницького національного університету*, 6(255), 96–101. https://surl.lt/dtbvyf

117. Reddy, K. T. (2023). Unveiling the power of k-nearest neighbors in phishing detection. *Insights2Techinfo*. https://surl.lu/kqpeol

118. Kuehn, P., Dietrich, S., Rossow, C. (2022). Clustering of threat information to mitigate information overload for computer emergency response teams. *Computer Science*, 1–11. https://arxiv.org/pdf/2210.14067

119. Patton, R., McEwen, I., Potts, M. (2011). Hierarchical clustering and visualization of aggregate cyber data. *In 7th International Wireless Communications and Mobile Computing Conference (IWCMC)*, 1287–1291. https://doi.org/10.1109/IWCMC.2011.5982725

120. Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security—A survey. *IEEE Internet of Things Journal*, 4(6), 1802–1831. https://doi.org/10.1109/JIOT.2017.2703172

121. Лисенко, С. (2019). Метод забезпечення резильєнтності комп'ютерних систем в умовах кіберзагроз на основі самоадаптивності. *Радіоелектронні і комп'ютерні системи*, 4(92), 4–16. https://doi.org/10.32620/reks.2019.4.01

122. Герасіна, О., Корнієнко, В., Гусєв, О., Соснін, К., & Мацюк, С. (2022). Виявлення фішингових URL-адрес за допомогою алгоритмів нечіткої кластеризації із глобальною оптимізацією. *Системні технології*, 2(139), 53–67. https://doi.org/10.34185/1562-9945-2-139-2022-06

123. Landauer, M., Wurzenberger, M., Skopik, F., Settanni, G., Filzmoser, P. (2020). System log clustering approaches for cyber security applications: A survey. *Computers & Security*, 92, 1–18. https://doi.org/10.1016/j.cose.2020.101739

124. Raptis, G., Katsini, C., Alexakos, C. (2021). Towards automated matching of cyber threat intelligence reports based on cluster analysis in an Internet-of-Vehicles environment. *IEEE International Conference on Cyber Security and Resilience (CSR)*, 366–371. https://doi.org/10.1109/CSR51186.2021.9527983

125. Buczak, A. L., Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, 18(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502

126. Shone, N., Ngoc, T., Phai, V., Shi, Q. (2018). A deep learning approach to network intrusion detection. *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2(1), 41–50. https://doi.org/10.1109/TETCI.2017.2772792

127. Stehr, M.-O., & Kim, M. (2023). Vulnerability clustering and other machine learning applications of semantic vulnerability embeddings. *Computer Science*, 1–27. https://arxiv.org/abs/2310.05935

128. González-Granadillo, G., González-Zarzosa, S., Diaz, R. (2021). Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures. *Sensors*, 21(14), 1–28. https://doi.org/10.3390/s21144759

129. Bryant, B. D., & Saiedian, H. (2020). Improving SIEM alert metadata aggregation with a novel kill-chain based classification model. *Computers & Security*, 94, 1–27. https://doi.org/10.1016/j.cose.2020.101817

130. Lee, J., Tang, F., Thet, P. M., Yeoh, D., Rybczynski, M., & Divakaran, D. M. (2022). SIERRA: Ranking anomalous activities in enterprise networks. *Computer Science*, 1–16. https://arxiv.org/pdf/2203.16802

131. Uetz, R., Herzog, M., Hackländer, L., Schwarz, S., & Henze, M. (2024). You cannot escape me: Detecting evasions of SIEM rules in enterprise networks. *Proceedings of the 33rd USENIX Security Symposium*, 5179–5196. https://www.usenix.org/system/files/usenixsecurity24-uetz.pdf

132. Субач, І. Ю., Власенко, О. В. (2023). Архітектура інтелектуальної SIEM-системи для виявлення кіберінцидентів у базах даних інформаційно-комунікаційних систем військового призначення. *Системи і технології зв'язку, інформатизації та кібербезпеки*, 4, 82–92. https://doi.org/10.58254/viti.4.2023.07.82

133. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2(1), 41–50. https://doi.org/10.1109/TETCI.2017.2772792

134. Ormrod, D., & Turnbull, B. (2017). Developing a Military Cyber Maturity Model for Multi-Domain Battle Mission Resilience and Success. *International Journal of Cyber Warfare and Terrorism*, 7(4), 1–13. https://doi.org/10.4018/IJCWT.2017100101

135. Hrozdov, A., Zinchenko, I., Hromliuk, M., Bily, O., Ivchenko, M., & Tsymbal, I. (2024). The method of assessing the sustainability of the functioning system based on the combat capabilities of the armies. *Системи і технології зв'язку, інформатизації та кібербезпеки*, 5, 64–72. https://doi.org/10.58254/viti.5.2024.05.64

136. Savant, S. S., & Sharma, S. (2024). The role of Internet of Battlefield Things in modern warfare: A cybersecurity perspective. *Journal of Research in Pharmacy Sciences*, 15(3), 1534–1542. https://doi.org/10.36676/jrps.v15.i3.1534

137. Негоденко, В. (2025). Моделювання критичних станів у SIEM-системі на основі теорії катастроф. *Телекомунікаційні та інформаційні технології*, 2, 118–125. https://doi.org/10.31673/2412-4338.2025.028289

138. Nabiyeva, A. (2025). Integration of artificial intelligence into communication systems: Enhancing performance, adaptability, and security. *Матеріали конференцій МЦНД*, 239–248. https://doi.org/10.62731/mcnd-29.08.2025.011

139. Rachapalli, S. K. (2023). Hybrid AI-edge architectures for mission-critical decision systems. *International Journal for Sciences and Technology*, 14(4). https://doi.org/10.71097/ijsat.v14.i4.5505

140. Scholtz, J. (2003). Theory and evaluation of human-robot interactions. *Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS)*, 1–11. https://doi.org/10.1109/HICSS.2003.1174284

141. Магденко, А. Р., Бучацький, І. О., & Бондаренко, І. О. (2024). Штучний інтелект: нова зброя в руках кіберзлочинців і шахраїв. https://ir.lib.vntu.edu.ua/handle/123456789/42455

142. Leenen, L., & Meyer, T. (2016). Semantic technologies and big data analytics for cyber defence. *International Journal of Cyber Warfare and Terrorism*, 6(3), 1–18. https://doi.org/10.4018/IJCWT.2016070105

143. Huang, S., Poskitt, C. M., Shar, L. K. (2025). Bayesian and multi-objective decision support for real-time cyber-physical incident mitigation. Computer Science, 1–43. https://doi.org/10.48550/arXiv.2509.00770

144. Skladannyi, P., Nehodenko, O., Shevchenko, S., Zolotukhina, O., Nehodenko, V. (2022). Modified delta maintainability model of object-oriented software. *CEUR Workshop Proceedings*, 3288, 117–124. https://surl.li/nvwlhp

145. Jabez, J., & Muthukumar, B. (2015). Intrusion detection system (IDS): Anomaly detection using outlier detection approach. *Procedia Computer Science*, 48, 338–346. https://doi.org/10.1016/j.procs.2015.04.191

146. Sheeraz, M., Paracha, M. A., Ulhaq, M., Mosavi, A. (2023). Effective security monitoring using efficient SIEM architecture. *Human-centric Computing and Information Sciences*, 13, 23. https://doi.org/10.22967/HCIS.2023.13.023

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

148. Goodfellow, I., Bengio, Y., Courville, A. (2016). Deep learning. Cambridge, MA: MIT Press., 31-44

149. IBM Security. (2021). IBM QRadar SIEM architecture overview: Whitepaper. IBM Corporation. https://www.ibm.com/security/security-intelligence/qradar

150. Splunk Inc. (2022). *Machine Learning Toolkit documentation*. https://docs.splunk.com/Documentation/MLApp

151. Гончар, С., Бакалинський, О., Дибач, О., Дмитрієва, Д. (2022). Метод агрегування ризиків у разі множини сумісних випадкових подій. *Ядерна та радіаційна безпека*, 1(93), 46–52. https://doi.org/10.32918/nrs.2022.1(93).05

152. Carannante, M., & Mazzoccoli, A. (2025). An analytical review of cyber risk management by insurance companies: A mathematical perspective. *Risks*, 13(8), 1–27. https://doi.org/10.3390/risks13080144

153. ENISA. (2024). Cyber insurance – Models and methods and the use of AI. ENISA Research Report. https://surl.li/vwsqhn

154. Dakos, V., Carpenter, S. R., Brock, W. A., Ellison, A. M., Guttal, V., Ives, A. R., Kéfi, S., Livina, V., Seekell, D., van Nes, E., & Scheffer, M. (2012). Methods for

detecting early warnings of critical transitions in time series illustrated using simulated ecological data. *PLoS ONE*, 7(7), https://doi.org/10.1371/journal.pone.0041010

155. Bury, T. M., Bauch, C. T., & Anand, M. (2021). Detecting and distinguishing tipping points using spectral early warning signals. *Journal of the Royal Society Interface*, 18(182), 1–10. https://doi.org/10.1098/rsif.2021.0354

156. Chen, S., Wang, H., & Wang, X. (2023). Early warning signals for cyber-physical systems based on critical slowing down theory. *Physica Scripta*. https://doi.org/10.1088/1402-4896/acde20

157. Zhang, H., Yin, Y., Zhao, D., & Liu, B. (2021). Network security situational awareness model based on threat intelligence. *Journal on Communications*, 42(6). https://doi.org/10.11959/j.issn.1000-436x.2021106

158. Li, X., Li, B., Li, H. (2026). Intelligent detection and early warning of power system cybersecurity threats based on multi-modal large language models. *Journal of Cyber Security and Mobility*, 1347–1372. https://doi.org/10.13052/jcsm2245-1439.1463

159. Landauer, M., Skopik, F., Stojanović, B., Friedberg, I. (2024). A review of time-series analysis for cyber security analytics: From intrusion detection to attack prediction. *International Journal of Information Security*, 24(1). https://doi.org/10.1007/s10207-024-00921-0

160. Kabir, S., Chowdhury, M., Zishan, M. S. R. (2025). Proactive detection of cyber-physical grid attacks: Pre-attack phase identification. *Research Square*, 1–20. https://doi.org/10.21203/rs.3.rs-5828184/v1

161. Mliki, H., Hadj Kacem, A., & Chaari Fourati, L. (2021). A comprehensive survey of intrusion detection systems based on machine and deep learning. *EAI Endorsed Transactions on Security and Safety*, 8(29), 1–23. https://doi.org/10.4108/eai.6-10-2021.171246

162. Kravchik, M., Demetrio, L., Biggio, B., & Shabtai, A. (2022). Practical evaluation of poisoning attacks on online anomaly detectors in industrial control systems. *Computers & Security*, 22. https://doi.org/10.1016/j.cose.2022.102901

163. Tiwari, S., Sresth, V., Srivastava, A. (2020). The role of explainable AI in cybersecurity: Addressing transparency challenges in autonomous defense systems. *International Journal of Innovative Research in Science, Engineering and Technology*, 9, 718–733. https://doi.org/10.15680/IJIRSET.2020.0903165

164. Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J. (2019). Survey of intrusion detection systems: Techniques, datasets and challenges. *Cybersecurity*, 2(1(20)), 1–22. https://doi.org/10.1186/s42400-019-0038-7

165. Ahmed, M., Mahmood, A. N., Hu, J. (2019). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications*, 60, 19–31. https://doi.org/10.1016/j.jnca.2015.11.016

166. Dias, T., Vitorino, J., Maia, E., Praça, I. (2024). Network simulation with complex cyber-attack scenarios. *Computer Science*, 1–6. https://doi.org/10.48550/arXiv.2412.01421

167. Serena, L., D'Angelo, G., Ferretti, S., Marzolla, M. (2025). Simulation in cybersecurity: Understanding techniques, applications, and goals. *Computer Science*, 1–6. https://doi.org/10.48550/arXiv.2508.06106

168. Morton, R. (2024). Measuring data protection: A causal artificial intelligence modeling approach. CERIAS Tech Report. Center for Education and Research in Information Assurance and Security, Purdue University. https://www.cerias.purdue.edu

169. Wani, A. A. (2024). Comprehensive analysis of clustering algorithms: Exploring limitations and innovative solutions. *PeerJ Computer Science*. https://doi.org/10.7717/peerj-cs.2286

170. Xu, R., Wunsch, D. (2005). Survey of clustering algorithms. *IEEE Transactions on Neural Networks*, 16(3), 645–678. https://doi.org/10.1109/TNN.2005.845141

171. Aldirawi, H., Morales, F. G. (2023). Univariate and multivariate statistical analysis of microbiome data: An overview. *Applied Microbiology*, 3(2), 322–338. https://doi.org/10.3390/applmicrobiol3020023

172. Xu, D., Tian, Y. (2015). Comprehensive survey of clustering algorithms. *Annals of Data Science*, 2, 165–193. https://doi.org/10.1007/s40745-015-0040-1

173. Abdul Nazeer, K., Sebastian, M. (2009). Improving the accuracy and efficiency of the k-means clustering algorithm. *In the World Congress on Engineering*, 1, 308–312. https://surli.cc/ntavod

174. Zheng, H., Yan, Y., Zhang, N. (2021). Human mobility prediction based on DBSCAN and RNN. *In the 2021 IEEE 4th International Conference on Computer and Communication Engineering Technology (CCET)*, 774–782. https://doi.org/10.1109/CCET52649.2021.9544246

175. Wadnare, R. J., Sherekar, S. S., Thakare, V. M. (2021). Efficient accessibility in cloud databases of health networks with natural neighbor approach for RNN-DBSCAN. In *Cloud Computing Technologies for Smart Agriculture and Healthcare*, 217–232. https://surli.cc/kiaecn

176. Bechini, A., Marcelloni, F., Renda, A. (2020). TSF-DBSCAN: A novel fuzzy density-based approach for clustering unbounded data streams. *IEEE Transactions on Fuzzy Systems*, 30(3), 623–637. https://doi.org/10.1109/TFUZZ.2020.3042645

176. Arbelaitz, O., Gurrutxaga, I., Muguerza, J., Pérez, J. M., Perona, I. (2019). An extensive comparative study of cluster validity indices. *Pattern Recognition*, 46(1), 243–256. https://doi.org/10.1016/j.patcog.2012.07.021

177. Warrens, M. J., Van der Hoef, H. (2022). Understanding the adjusted Rand index and other partition comparison indices based on counting object pairs. *Journal of Classification*, 39, 487–509. https://doi.org/10.1007/s00357-022-09413-z

178. Li, H., Zhang, L. (2022). Summary of clustering research in time series data mining. *Journal of University of Electronic Science and Technology of China*, 51(3), 416–424. https://doi.org/10.12178/1001-0548.2022055

179. Aghabozorgi, S., Shirkhorshidi, A. S., Wah, T. Y. (2015). Time-series clustering – A decade review. *Information Systems*, 53, 16–38. https://doi.org/10.1016/j.is.2015.04.007

180. Rodrigues, P. P., Gama, J. (2021). A survey on time-series clustering. *ACM Computing Surveys*, 54(6(120)), 1-38. https://doi.org/10.1145/3463602

181. ENISA. (2024). *ENISA threat landscape 2024*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

182. Powers, D. (2011). Evaluation: From precision, recall and F-measure to ROC, informedness, markedness and correlation. *Journal of Machine Learning Technologies*, 2(1), 37–63. https://doi.org/10.48550/arXiv.2010.16061

183. Sujon, K., Hassan, R., Choi, K., Samad, M. (2025). Accuracy, precision, recall, F1-score, or MCC? Empirical evidence from advanced statistics, ML, and XAI for evaluating predictive models. *Journal of Big Data*, 12(313). https://doi.org/10.1186/s40537-025-01313-4

184. Vakili, M., Ghamsari, M., Rezaei, M. (2020). Performance analysis and comparison of machine and deep learning algorithms for IoT data classification. Computer Science. https://doi.org/10.48550/arXiv.2001.09636

185. Fourure, D., Javaid, M., Posocco, N., Tihon, S. (2021). Anomaly detection: How to artificially increase your F1-score with a biased evaluation protocol. Computer Science. https://doi.org/10.48550/arXiv.2106.16020

186. Siblini, W., Fréry, J., He-Guelton, L., Oblé, F., Wang, Y. (2020). Master your metrics with calibration. In *Machine Learning and Knowledge Discovery in Databases*, 457–474. https://doi.org/10.1007/978-3-030-44584-3_36

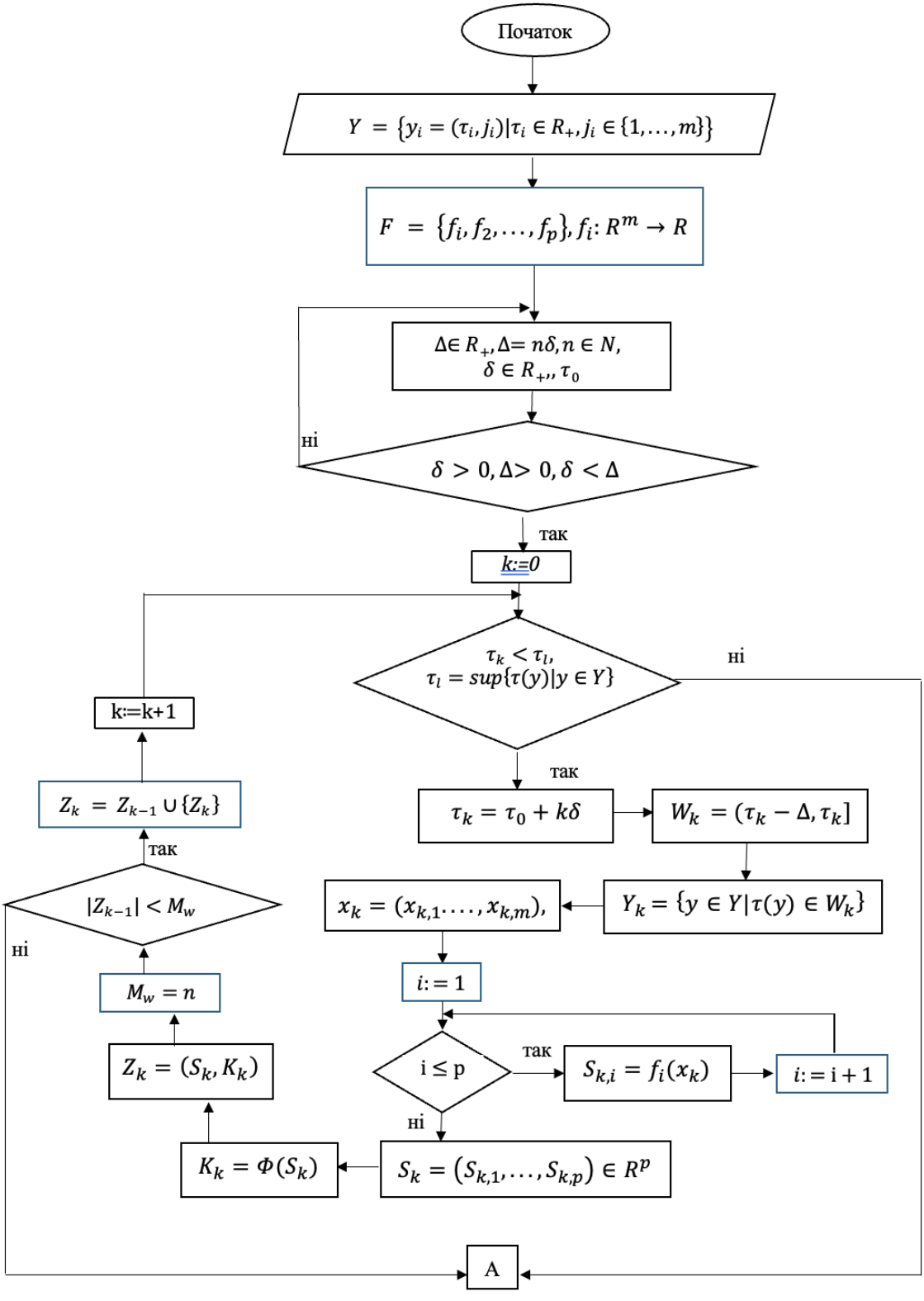
187. Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., Marchetti, M. (2018). On the effectiveness of machine and deep learning for cyber security. *In the 2018 10th International Conference on Cyber Conflict (CyCon)*, 371–390. https://doi.org/10.23919/CYCON.2018.8405026

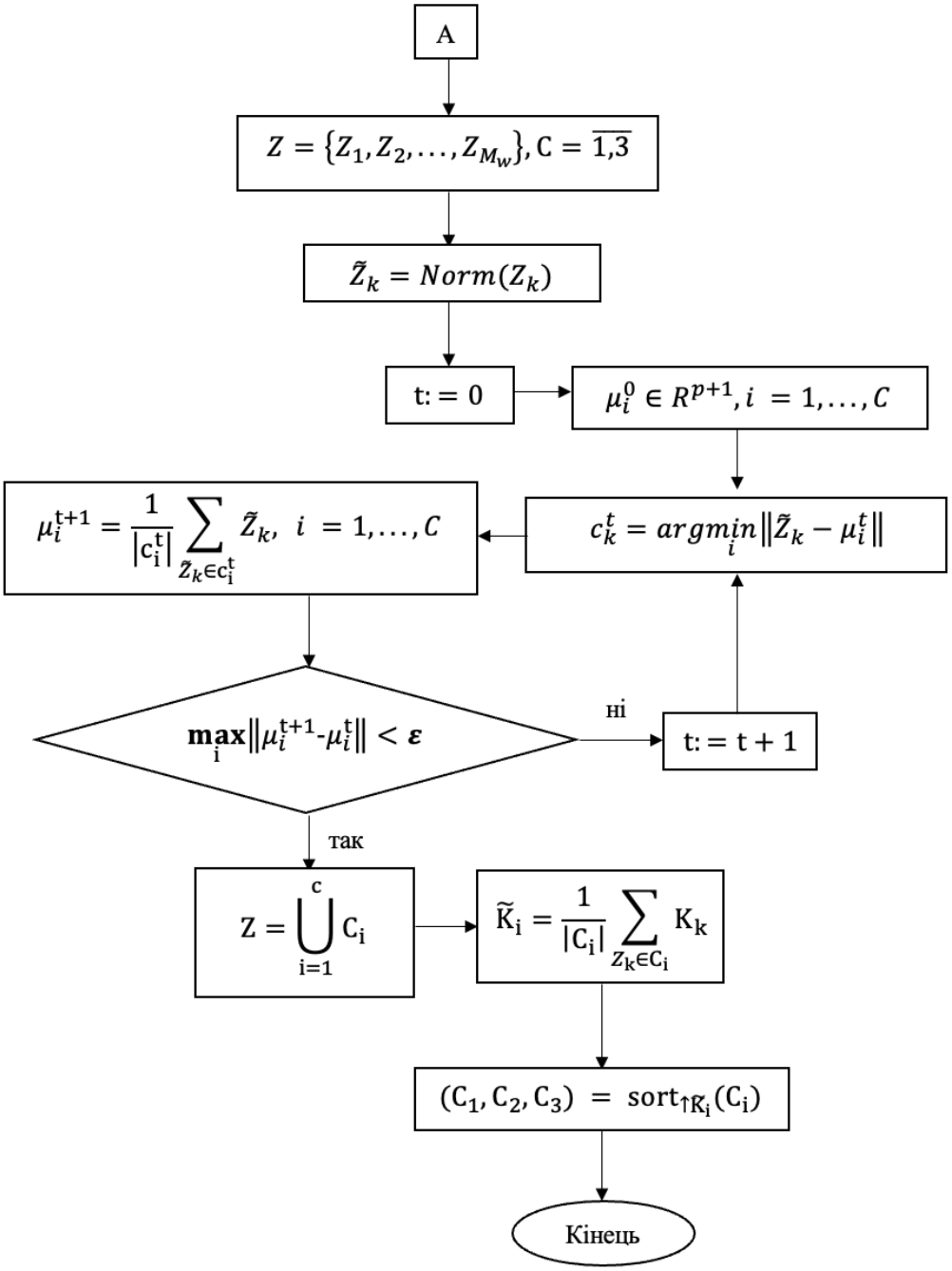
188. Bowers, A. J., Zhou, X. (2019). Receiver operating characteristic (ROC) area under the curve (AUC): A diagnostic measure for evaluating the accuracy of predictors of education outcomes. *Journal of Education for Students Placed at Risk (JESPAR)*, 24(7), 1–25. https://doi.org/10.1080/10824669.2018.1523734

189. García, V., Mollineda, R. A., Sánchez, J. S. (2009). Index of balanced accuracy: A performance measure for skewed class distributions. In *Lecture Notes in Computer Science*, 5524, 441–448. https://doi.org/10.1007/978-3-642-02172-5_57

ДОДАТОК А

Схема алгоритму кластеризації станів військових інформаційних систем на основі аналізу загроз та уразливостей




A
$Z = \{Z_1, Z_2, \ldots, Z_{M_w}\}, \mathrm{C} = \overline{1,3}$
$\tilde{Z}_k = Norm(Z_k)$
t: = 0
$\mu_i^0 \in R^{p+1}, i = 1, \ldots, C$
$c_k^t = \underset{i}{argmin} \|\tilde{Z}_k - \mu_i^t\|$
$\mu_i^{t+1} = \frac{1}{|c_i^t|} \sum_{\tilde{Z}_k \in c_i^t} \tilde{Z}_k, \ i = 1, \ldots, C$
$\max_i \|\mu_i^{t+1} - \mu_i^t\| < \varepsilon$
ні
t: = t + 1
так
$Z = \bigcup_{i=1}^{c} C_i$
$\widetilde{K}_i = \frac{1}{|C_i|} \sum_{Z_k \in C_i} K_k$
$(C_1, C_2, C_3) = \mathrm{sort}_{\uparrow \widetilde{K}_i}(C_i)$
Кінець

ДОДАТОК Б

Програмний код для представлення множини рівноважних станів нелінійної моделі катастрофи типу «метелик» у просторі вагових параметрів

```
import numpy as np
import plotly.graph_objects as go
from scipy.optimize import fsolve

# Вагові коефіцієнти для різних типів інцидентів
c = 0.0124
d = 0.9809
e = 0.0011
f = 0.0056

# Похідна потенціалу з урахуванням вагових коефіцієнтів
def butterfly_potential_derivative(x, a, b, c, d, e, f):
return 6 * x**5 + 4 * a * x**3 + 3 * b * x**2 + 2 * c * x + d + e * x**6 + f * x**4

# Діапазони параметрів a і b
a_vals = np.linspace(-1, 1, 30)
b_vals = np.linspace(-1, 1, 30)
a_grid, b_grid = np.meshgrid(a_vals, b_vals)

# Ініціалізація списку для рівноважних точок
x_equilibrium_points = []

# Знаходження  коренів
```

```
initial_guesses = np.linspace(-5, 5, 10)

# Пошук рівноважних точок для кожного типу інциденту
for i in range(a_grid.shape[0]):
    for j in range(a_grid.shape[1]):
        a = a_grid[i, j]
        b = b_grid[i, j]

        # Знаходження коренів для кожного типу інциденту
        roots_spam = []
        roots_malware = []
        roots_dos = []
        roots_vulnerability = []

        for guess in initial_guesses:
            try:
                root_spam = fsolve(butterfly_potential_derivative, guess, args=(a, b, c, 0, 0, 0),
xtol=1e-6, maxfev=2000)
                if not any(np.isclose(root_spam[0], roots_spam, atol=1e-3)):
                    roots_spam.append(root_spam[0])

                root_malware = fsolve(butterfly_potential_derivative, guess, args=(a, b, 0, d,
0, 0), xtol=1e-6, maxfev=2000)
                if not any(np.isclose(root_malware[0], roots_malware, atol=1e-3)):
                    roots_malware.append(root_malware[0])

                root_dos = fsolve(butterfly_potential_derivative, guess, args=(a, b, 0, 0, e, 0),
xtol=1e-6, maxfev=2000)
                if not any(np.isclose(root_dos[0], roots_dos, atol=1e-3)):
```

```
                roots_dos.append(root_dos[0])

            root_vulnerability = fsolve(butterfly_potential_derivative, guess, args=(a, b, 0, 0, 0, f), xtol=1e-6, maxfev=2000)
            if not any(np.isclose(root_vulnerability[0], roots_vulnerability, atol=1e-3)):
                roots_vulnerability.append(root_vulnerability[0])
        except RuntimeWarning:
            print(f"Warning: No convergence for a={a}, b={b}, guess={guess}")

    # Додаємо унікальні корені для кожного типу інциденту
    for root in roots_spam:
        x_equilibrium_points.append((a, b, root, "Spam"))
    for root in roots_malware:
        x_equilibrium_points.append((a, b, root, "Malware"))
    for root in roots_dos:
        x_equilibrium_points.append((a, b, root, "DoS"))
    for root in roots_vulnerability:
        x_equilibrium_points.append((a, b, root, "Vulnerability"))

# Перетворення списку у масив для зручності роботи
x_equilibrium_points = np.array(x_equilibrium_points, dtype=object)
# Побудова інтерактивного графіка
fig = go.Figure()

# Додавання точок на графік
for incident_type in ["Spam", "Malware", "DoS", "Vulnerability"]:
    incident_points = x_equilibrium_points[x_equilibrium_points[:, 3] == incident_type]

    fig.add_trace(go.Scatter3d(
```

```
        x=incident_points[:, 0],
        y=incident_points[:, 1],
        z=incident_points[:, 2],
        mode='markers',
        name=incident_type,
        marker=dict(
            size=5,
            color=incident_points[:, 2],
            colorscale='Viridis',
            colorbar=dict(
                title=dict(
                    text="Стан рівноваги x",
                    font=dict(size=12)
                ),
                tickfont=dict(size=10),
                len=0.8,
                thickness=15,
                x=1.1,
                y=0.5
            ),
            opacity=0.8
        )
    ))

# Налаштування графіка
fig.update_layout(
    title="Точки біфуркації для катастрофи 'Метелик' з ваговими коефіцієнтами",
    scene=dict(
        xaxis_title="Параметр a",
```

```
        yaxis_title="Параметр b",
        zaxis_title="Стан рівноваги x"
    ),
    margin=dict(l=0, r=0, b=0, t=40)
)
# Відображення графіка
fig.show()
```

ДОДАТОК В

АКТ ВПРОВАДЖЕННЯ В КИЇВСЬКОМУ СТОЛИЧНОМУ УНІВЕРСИТЕТІ ІМЕНІ БОРИСА ГРІНЧЕНКА

КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА

ФАКУЛЬТЕТ
ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
ТА МАТЕМАТИКИ
вул. Левка Лук'яненка, 13-Б, м. Київ, Україна, 04207
Тел.: +380 44 428-34-14
fitm.kubg.edu.ua, fitm@kubg.edu.ua

BORYS GRINCHENKO
KYIV METROPOLITAN UNIVERSITY

FACULTY
OF INFORMATION TECHNOLOGIES
AND MATHEMATICS
13-B Levka Lukianenka St, Kyiv, Ukraine, 04207
Tel.: +380 44 428-34-14
fitm.kubg.edu.ua, fitm@kubg.edu.ua

09.12.2025 № 26

АКТ
про впровадження результатів дисертаційного дослідження
Негоденко Віталія Петровича
на тему «Моделі та методи забезпечення кібербезпеки військових інформаційних систем на основі теорій конфліктів та катастроф»
поданого на здобуття наукового ступеня доктора філософії (PhD)
зі спеціальності 125 Кібербезпека

Цей Акт засвідчує, що на підставі рішення кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка наукові результати, отримані в дисертаційному дослідженні, впроваджені в освітню та наукову діяльність кафедри. Впроваджено такі наукові результати:

- математичну модель впливу кіберінцидентів на стійкість систем управління інформаційною безпекою з використанням катастрофи типу «Метелик»;
- метод кластеризації загроз та уразливостей на основі даних з ковзними часовими вікнами;
- модель прогнозування критичних переходів, яка забезпечує підвищення рівня кіберстійкості військових інформаційних систем за рахунок інтеграції теорії катастроф у SIEM-системи;
- метод підтримки прийняття рішень для забезпечення кіберстійкості військових інформаційних систем, який базується на інтеграції математичних моделей, методів аналізу та прогнозування на основі теорій конфліктів та

катастроф.

Наукові результати розроблені особисто Негоденко Віталієм Петровичем у ході проведення ним дисертаційних досліджень та отримали високу оцінку при обговоренні на засіданнях кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка.

Отримані результати використовуються:

у навчальному процесі кафедри інформаційної та кібербезпеки при підготовці студентів спеціальності 125 «Кібербезпека та захист інформації» на бакалаврському та магістерському рівнях;

під час лабораторних та практичних занять, пов'язаних з управлінням інформаційною безпекою, аналізом кіберінцидентів, математичним моделюванням у кібербезпеці та системами моніторингу безпеки;

у науково-дослідній діяльності кафедри, пов'язаній з підвищенням кіберстійкості військових інформаційних систем та прогнозуванням критичних станів інформаційних систем.

Дослідження Негоденко Віталія Петровича відповідає всім вимогам до організації наукового пошуку та дає позитивний результат у практичному застосуванні.

Декан
Факультету інформаційних технологій та математики
кандидат фізико-математичних наук,
старший науковий співробітник Оксана ЛИТВИН

ДОДАТОК Г

АКТ ВПРОВАДЖЕННЯ В ІНСТИТУТІ ПРОГРАМНИХ СИСТЕМ НАЦІОНАЛЬНОЇ АКАДЕМІЇ НАУК УКРАЇНИ

ЗАТВЕРДЖУЮ
Директор Інституту програмних систем
Національної академії наук України
_____Ігор СІНІЦИН
09 грудня 2025 року

АКТ
про впровадження результатів дисертаційного дослідження
Негоденко Віталія Петрович
на тему:
«Моделі та методи забезпечення кібербезпеки військових інформаційних систем на основі теорій конфлікту та катастроф»

Комісія у складі:
голова комісії – заступник директора з наукової роботи Шевченко В.Л.;
члени комісії:
учений секретар Дергильова О.В.
заступник завідувача відділу Ігнатенко П.П.

Комісія цим актом засвідчує, що наступні результати дисертаційного дослідження Негоденко Віталія Петрович, а саме:

- математична модель впливу кіберінцидентів на стійкість систем управління інформаційною безпекою, розроблена на основі теорії катастроф типу «Метелик», яка дозволяє прогнозувати критичні переходи станів інформаційних систем;
- вдосконалений метод кластеризації загроз та уразливостей інформаційних систем, що підвищує об'єктивність аналізу кіберризиків та покращує ефективність класифікації кіберінцидентів;
- модель прогнозування критичних станів інформаційних систем, що інтегрує методи теорії катастроф у системи моніторингу безпеки (SIEM) для виявлення нестабільних станів систем на ранніх стадіях;
- метод підтримки рішень для забезпечення кіберстійкості інформаційних систем, заснований на інтеграції математичних моделей теорії катастроф та конфліктів

впроваджено в Інституті програмних систем Національної академії наук України та можуть бути використані в наукових дослідженнях, пов'язаних з аналізом кіберінцидентів та кіберзагроз, моделюванням процесів інформаційної безпеки, прогнозуванням критичних станів інформаційних систем та розробкою методів підвищення кіберстійкості інформаційних систем. Надані матеріали можуть бути використані при формуванні перспективних планів досліджень. Цей Акт не є підставою для фінансових зобов'язань.

Голова комісії Віктор ШЕВЧЕНКО

Члени комісії Олена ДЕРГИЛЬОВА

Петро ІГНАТЕНКО

ДОДАТОК Д

ДОВІДКА ПРО ВПРОВАДЖЕННЯ У ВІЙСЬКОВІЙ ЧАСТИНІ А2393

Прим. № ___
Відкрита інформація

ДОВІДКА
про впровадження результатів отриманих при виконанні дисертаційного дослідження Негоденка Віталія Петровича на тему:
“Моделі та методи забезпечення кібербезпеки військових інформаційних систем на основі теорій конфлікту та катастроф”

Ця довідка свідчить про те, що результати, отримані в дисертаційному дослідженні Негоденка Віталія Петровича, були використані в ході повсякденної (службової) діяльності військової частини А2393 щодо підвищення рівня безпеки інформації у військових системах управління безпекою, а саме використано метод підтримки прийняття рішень для забезпечення кіберстійкості військових інформаційних систем, який базується на інтеграції математичних моделей, методів аналізу та прогнозування на основі теорій конфліктів і катастроф, що дозволяє підвищити ефективність виявлення та прогнозування переходів системи до критичних станів.

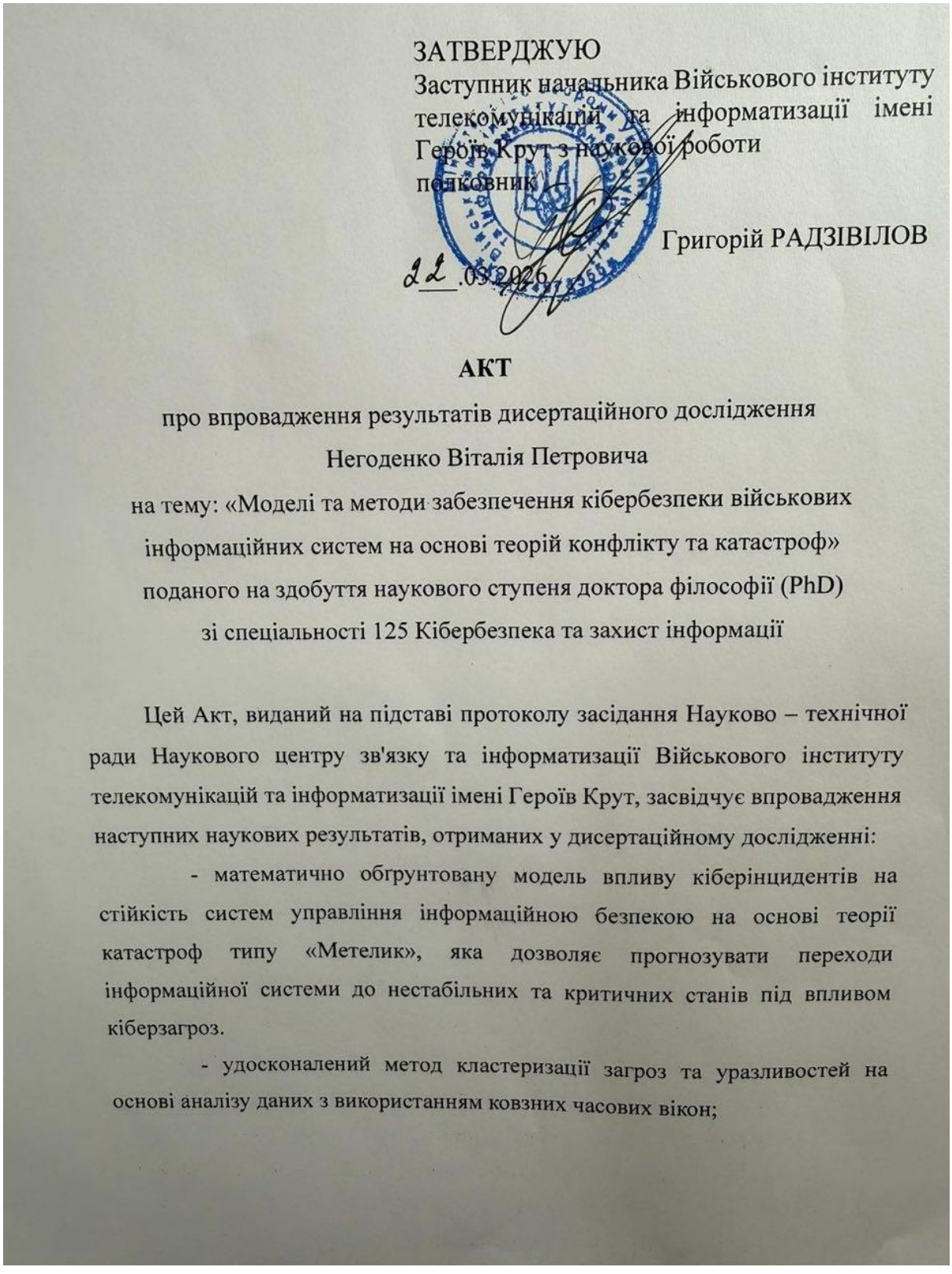
Тимчасово виконуючий обов’язки начальника штабу – заступника командира військової частини А2393
майор Микола ПАВЛЕНКО
05 лютого 2026 року

М.П.

ВІДКРИТА ІНФОРМАЦІЯ

ДОДАТОК Е

АКТ ВПРОВАДЖЕННЯ У ВІЙСЬКОВИЙ ІНСТИТУТУ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ ІМЕНІ ГЕРОЇВ КРУТ



ЗАТВЕРДЖУЮ
Заступник начальника Військового інституту телекомунікацій та інформатизації імені Героїв Крут з наукової роботи
полковник

Григорій РАДЗІВІЛОВ

22.09.2025

АКТ

про впровадження результатів дисертаційного дослідження
Негоденко Віталія Петровича
на тему: «Моделі та методи забезпечення кібербезпеки військових інформаційних систем на основі теорій конфлікту та катастроф»
поданого на здобуття наукового ступеня доктора філософії (PhD)
зі спеціальності 125 Кібербезпека та захист інформації

Цей Акт, виданий на підставі протоколу засідання Науково – технічної ради Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут, засвідчує впровадження наступних наукових результатів, отриманих у дисертаційному дослідженні:

- математично обгрунтовану модель впливу кіберінцидентів на стійкість систем управління інформаційною безпекою на основі теорії катастроф типу «Метелик», яка дозволяє прогнозувати переходи інформаційної системи до нестабільних та критичних станів під впливом кіберзагроз.

- удосконалений метод кластеризації загроз та уразливостей на основі аналізу даних з використанням ковзних часових вікон;

- модель прогнозування критичних переходів станів інформаційної системи, яка забезпечує підвищення рівня кіберстійкості військових інформаційних систем за рахунок інтеграції методів теорії катастроф у системи управління подіями та інформацією безпеки (SIEM);

- метод підтримки прийняття рішень для забезпечення кіберстійкості військових інформаційних систем, який базується на інтеграції математичних моделей, методів аналізу та прогнозування на основі теорій конфліктів і катастроф, що дозволяє підвищити ефективність виявлення та прогнозування переходів системи до критичних станів.

Наукові результати, отримані під час дисертаційного дослідження, отримали позитивну оцінку на засіданні Науково-технічної ради Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут. Зазначені результати впроваджені в наукові дослідження, які пов'язані з аналізом кіберінцидентів, моделюванням процесів інформаційної безпеки, прогнозуванням критичних станів інформаційних систем.

Результати дисертаційного дослідження Негоденко Віталія Петровича відповідають вимогам до організації наукових досліджень та використані при відпрацюванні наукової продукції при розробці оперативного завдання шифр "Центр".

Начальник Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут
полковник
21.03.2026 Артур ЗАРУБЕНКО