УДК 004.056.53 DOI 10.31673/2412-4338.2025.028289

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

МОДЕЛЮВАННЯ КРИТИЧНИХ СТАНІВ В SIEM-СИСТЕМІ НА ОСНОВІ ТЕОРІЇ КАТАСТРОФ

Анотація: *Проведено дослідження впливу кіберінцидентів на військові системи управління інформаційної безпеки при підготовці військових підрозділів в тренувальних центрах. Проведено аналіз наукових досліджень щодо виявлення кіберінцидентів за допомогою методів машинного навчання, які мають свої переваги та важливі недоліки. Виявлено, що в роботах не розглядаються питання стійкості системи та прогнозу критичних переходів станів безпеки інформаційних систем. Визначено основні переваги використання SIEM-системи, яка дозволяє збирати, агрегувати, зберігати та корелювати події, створені керованою інфраструктурою. Встановлено, що SIEM-системи мають значні недоліки, серед яких фальшиві спрацювання, що перешкоджають виявленню важливих загроз, не здійснюється прогнозування розвитку подій, що не дозволяє оцінити майбутні ризики. Проведено аналіз основних недоліків SIEM-системи та запропоновано шляхи вирішення із застосуванням блоку із теорією катастроф у SIEM-системі. Проведено аналіз сучасних систем імітаційного моделювання динаміки бойових дій у форматі командно-штабних навчань в режимі реального часу. Визначено структуру інтегрованої системи навчання, а також основні логічні блоки, які доцільно об'єднати за допомогою SIEM в один ланцюг подій. Встановлено основні компоненти інтегрованої системи навчання, їх призначення та роль SIEM-системи для реагування на кіберінциденти для встановлення безпеки даних. Розроблено алгоритм виявлення нестабільних станів системи під час дії кіберінцидентів із використанням SIEM 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 системи.*

Ключові слова: *система управління інформаційною безпекою (СУІБ), SIEM-система, критичні стани, теорія катастроф, точки біфуркації, кіберінцидент.*

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

MODELING OF CRITICAL STATES IN SIEM SYSTEM BASED ON CATASTROPHE THEORY

Abstract: *A study of the impact of cyber incidents on military information security management systems during the training of military units in training centers was conducted. An analysis of scientific research on the detection of cyber incidents using machine learning methods, which have their advantages and important disadvantages, has been carried out. It was found that the works do not consider the issues of system stability and the forecast of critical transitions of information system security states. The main advantages of using a SIEM system, which allows collecting, aggregating, storing and correlating events generated by a managed infrastructure, were determined. It was found that SIEM systems have significant disadvantages, including malfunction that prevent the detection of important threats, and no prediction of the development of events is carried out, which does not allow assessing future risks. An analysis of the main disadvantages of the SIEM system was conducted and solutions were proposed using a block with the catastrophe theory in the SIEM system. An*

analysis of modern systems for simulating the dynamics of combat operations in the format of command and staff training exercises in real time has been carried out. The structure of the integrated training system has been determined, as well as the main logical blocks that should be combined using SIEM into a single chain of events. The main components of the integrated training system, their purpose and the role of the SIEM system for responding to cyber incidents to establish data security have been established. An algorithm for detecting unstable system states during cyber incidents using SIEM and catastrophe theory in the integrated training system has been developed, which allows predicting and detecting unstable system states, as well as responding to information leaks in real time, which ensures an increase in the level of cyber resilience of the system.

Keywords: *information security management system (ISMS), SIEM system, critical states, catastrophe theory, bifurcation points, cyber incident.*

1. Вступ

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 з етапів 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 [1].

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 [2]. 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 [3].

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

2. Аналіз літературних даних і постановка проблеми

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 [3].

В роботах [4,5] 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 [6] 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 [7] 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 і 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.

3. Мета і задачі дослідження

Метою дослідження є розробка алгоритму 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 вирішено завдання:

– проаналізовано технічні можливості SIEM-системи для прогнозування, виявлення та попередження кіберінцидентів;

– побудовано модель виявлення нестабільних станів системи під час кіберінцидентів із використанням SIEM та теорії катастроф

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

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 [2] на стійкість системи управління інформаційної безпеки.

В роботах [8-9] 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 змін, які призводять до порушення стійкості всієї системи управління інформаційної безпеки [9]. 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.

Но 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.1).

Таблиця 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

4.2. Побудова моделі виявлення нестабільних станів системи під час кіберінцидентів із використанням SIEM та теорії катастроф

Таблиця 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

В роботі [10] проведено аналіз сучасних систем імітаційного моделювання динаміки бойових дій у форматі командно-штабних навчань в режимі реального часу. 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 [10], їх призначення та роль SIEM-системи наведено в Таб.2.

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. Вплив кіберінцидентів, що детально досліджено в роботі [9], 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 системи навчання, 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 роботі [9].

Доцільно описати кроки побудови моделі виявлення нестабільних станів системи під час кіберінцидентів із використанням SIEM-системи та теорії катастроф в інтегрованій системі навчання (Рис.1), що дозволить показати комплексне дослідження, щодо побудови системи управління інформаційною безпекою у процесі підготовки військових підрозділів.

Рис.1 Структурна схема інтегрованого тренувального середовища [10]

Визначено основні кроки для побудови даної моделі.

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:

- нормалізує кіберінциденти, які досліджено в роботі [9] і виділено найбільш впливові;
- будує функцію на основі виділених контрольних параметрів, яка моделює асимптотичну поведінку системи, а також дозволяє аналізувати стійкість складних систем та має вигляд [1], як приклад " катастрофа метелик" [9]:
-

$$V(x) = 6x^5 + 4ax^3 + 3bx^2 + 2cx + d + ex^6 + fx^4 \quad (1)$$

де $a, b -$ контрольні параметри;

c – Спам (Spam);

d – Шкідливий програмний код (Malware);

e – Атака на відмову в обслуговуванні (DoS/Ddos);

f – Вразливість (Vulnerability);

- аналізує критичні токи та стабільність системи, де

$$\frac{dx}{dt} = -\frac{dV(x)}{dx}) = 0 \quad (2)$$

- визначає нестійкість системи, а саме виявлення точок біфуракції [11,12], 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 біфуракції і подального аналізу.

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

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

Запропоновано алгоритм (Рис.2) виявлення нестабільних станів системи під час дії кіберінцидентів із використанням SIEM 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 системи.

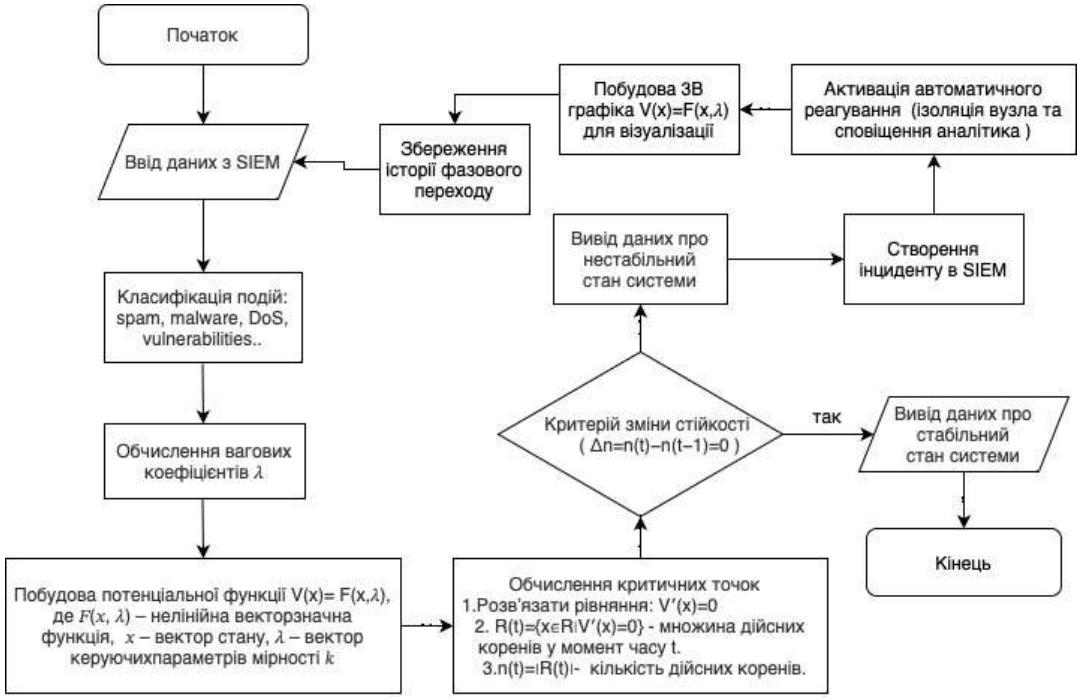

Рис.2 Схема алгоритму виявлення нестабільних станів системи із SIEM та теорії катастроф

Висновки і перспективи подальших досліджень

Проведене дослідження є послідовним і логічним продовженням цілісної мети, яка реалізовує підвищення рівня захисту інформації від кібервпливів в інтегрованих системах для ефективного навчання військових підроздів. Дана робота представляє вичерпний 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 практичних [10] і математичних досідженнь [9] 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 [10], математичного застосування теорії катастроф та покрокового алгоритму його реалізації в SIEM системі.

Майбутні дослідження важливо зосередити на розробці програмного забезпечення для аналізу ефективності прийнятих управлінських рішень, яке дозволить автоматично визначити вплив кіберінцидентів на систему і реагувати на них.

Список використаної літератури

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

2. González-Granadillo, G. González-Zarzosa, S. Diaz, R. Security Information and Event Management (SIEM): Analysis,Trends, and Usage in CriticalInfrastructures. Sensors 2021, 21, 4759.

3. Bryant, B.D., Saiedian, H. Improving SIEM alert metadata aggregation with a novel kill-chain based classification model. Comput.Secur. 2020, 94.

4. Lee J., Tang F., Thet P.M., Yeoh D., Rybczynski M., Divakaran D.M. SIERRA: Ranking Anomalous Activities in Enterprise Networks. Conference 2022 IEEE 7th European Symposium on Security and Privacy (EuroS&P)

Year: 2022, Volume: 1, Pages: 44-59.

5. Uetz R., Herzog M., Hacklander L., Schwarz S., Henze M. You cannot escape me: detecting evasions of SIEM rules in enterprise networks. Proceedings of the 33rd USENIX Conference on Security Symposium. 2024, Volume 290, Pages 5179-5196.

6. Субач І.Ю., Власенко О.В. Архітектура інтелектуальної SIEM-системи для виявлення кіберінцидентів у базах даних інформаційно-комунікаційних систем військового призначенняю // Системи і технології зв'язку, інформатизації та кібербезпеки. ВІТІ. 2023. No 4. С. 82 – 92.

7. Кубарич З. П. Використання штучного інтелекту для ефективного реагування на інциденти у SIEM системі : кваліфікаційна робота на здобуття освітнього ступеня магістр за спеціальністю „125 — кібербезпека" /З. П. Кубарич. — Тернопіль: ТНТУ, 2023. — 98 с.

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

9. Негоденко В. Застосування математичної теорії катастроф для забезпечення стійкості системи управління інформаційною безпекою // Кібербезпека: освіта, наука, техніка. 2024, №2(26). 212 – 222.

10. Негоденко Віталій. Дослідження інформаційних конфліктів у системі навчання ЗСУ за допомогою імітаційного моделювання / В. Негоденко // Кібербезпека: освіта, наука, техніка : електронне наукове видання. - 2023. - Том 4, N 20. - С. 164-173, DOI 10.28925/2663-4023.2023.20.164173. - Бібліогр. в кінці ст. . - ISSN 2663-4023.

11. Arnold, V. I., Davydov, A. A., Vassiliev, V. A., Zakalyukin, V. M. (2006). Mathematical Models of Catastrophes. Control of Catastrophic Processes. Encyclopedia of Life Support Systems (EOLSS), EOLSS Publishers, Oxford. https://pure.iiasa.ac.at/8095/1/RP-06-007.pdf

12. Tom, R. (1977). Structural stability, catastrophe theory, and applied mathematics. SIAM Review, 19(2), 189–201.