КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.26.692
УДК 004.94

Негоденко Віталій Петрович
аспірант кафедри інформаційної та кібернетичної
безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0002-7678-9138
v.nehodenko.asp@kubg.edu.ua

ЗАСТОСУВАННЯ МАТЕМАТИЧНОЇ ТЕОРІЇ КАТАСТРОФ ДЛЯ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Анотація. 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. Прогнозування впливу різних типів інцидентів дозволяє забезпечити стабільність та рівновагу складних динамічних систем, їх конфіденційність, цілісність та доступність. Проведено дослідження стійкості системи управління інформаційною безпекою до кіберінцидентів різних типів. Використано математичну теорію катастроф для моделювання динаміки інформаційної системи. Проаналізовано та досліджено типи катастроф, які залежать від різної кількості параметрів впливу на динамічну систему. На основі наданого звіту про виявлені кіберінциденти у період 2022–2024 роки встановлено основні типи інцидентів для дослідження. Проаналізовано перелік категорій кіберінцидентів, який постійно оновлюється з урахуванням появи нових типів, та включає також опис даних інцидентів і їх вплив на інформаційну систему. Для моделювання поведінки динамічної системи в кризових ситуаціях, оцінювання рівня стійкості системи та визначення критичних точок, в яких система стає особливо вразливою до зовнішніх або внутрішніх деструктивних впливів вибрано тип катастрофи «Метелик». Встановлено точки рівноваги, точки біфуркації та зону ризику на площині точок рівноваги системи, яка критично важлива і чутлива до збурень, що відповідає небезпечним або хаотичним режимам збою інформаційної системи під впливом деяких типів кіберінцидентів. Для розрахунків та візуалізації використано Python, бібліотеки Numpy, Pandas та інші. На 3D графіках представлено залежність стану рівноваги динамічної системи від параметрів впливу кожного типу інцидентів, що дозволяє виявити можливі збої інформаційної системи та оптимізувати роботу системи управління інформаційною безпекою для запобігання катастрофам.

Ключові слова: Система управління інформаційною безпекою (СУІБ); теорія катастроф; катастрофа «Метелик»; кіберінцидент; Python; градієнтний спуск; диференціальне рівняння.

ВСТУП

Постановка проблеми. У сучасних умовах інформаційна безпека систем має вирішальне значення для ефективності та безпеки військових операцій. Однією з важливих 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.

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 [1] – [9].

Для дослідження даних наслідків доцільно розглянути математичну теорію катастроф, яка дозволяє аналізувати зміни стану системи через незначні флуктуації вхідних параметрів. Теорія катастроф дозволяє моделювати кризові ситуації, оцінювати рівень стійкості системи та визначати критичні точки, в яких система стає особливо вразливою до зовнішніх або внутрішніх деструктивних впливів. Використання цього підходу при аналізі СУІБ для ЗСУ дозволяє краще зрозуміти, як система реагуватиме на різні сценарії атак і як уникнути можливі переходи у критичний стан [10].

Аналіз останніх досліджень і публікацій. Теорію катастроф, як програму прогнозування нестійкості різних систем, використовують в задачах забезпечення захисту інформації [9]. В даній роботі 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 [11]. Перелік категорій кіберінцидентів [12], який постійно оновлюється з урахуванням появи нових видів та типів, включає також опис даних інцидентів і їх в плив на інформаційну систему.

Метою статті є моделювання впливу кіберінцидентів на стійкість системи управління інформаційної безпеки на основі теорії катастроф.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Відповідно до переліку категорій кіберінцидентів [12] 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 вразливості (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 to information)
   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; виявити аномалії, які вказують на інцидент у реальному часі та вжити заходів для протидії атакам до їх початку; оцінити вразливі місця інформаційної системи та підвищити її рівень кіберстійкості з урахуванням частоти, інтенсивності і типу атак; оцінити ризики, а саме розробити та протестувати плани реагування на інциденти, які швидко змінюються та адаптуються до нових умов.

В 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, також встановити пороги критичних змін, які можуть призвести до збоїв в даній системі [10].

МЕТОДИКА ДОСЛІДЖЕННЯ

Побудова моделі впливу кіберінцидентів на стійкість СУІБ в ЗСУ здійснена на основі наданого звіту відділу Кібербезпеки ЗСУ щодо виявлених кіберінцидентів у період 2022–2024 років. Проведений аналіз наданих даних показав необхідність зосередити увагу на 5 категоріях кіберінциденів, що дозволяє визначити 5 основних параметрів, які будуть змінюватись і мати вплив на стійкість інформаційної системи та її потенційний перехід у нестабільний стан.

Визначено основні кроки для побудови моделі впливу інцидентів кібербезпеки на стійкість системи управління інформаційної безпеки в ЗСУ.

1. Вибір параметрів впливу на систему. Нехай на систему впливають 5 параметри кіберінцидентів:
   x_1 — Шкідливий вміст;
   x_2 — Шкідливий програмний код;
   x_3 — Збір інформації зловмисником;
   x_4 — Порушення доступності;
   x_5 — Відома вразливість.

2. Вибір типу катастрофи, який дозволяє показати перехід від стабільного до змінного стану під впливом 5 важливих параметрів, можливий за допомогою наступних моделей:
   – Катастрофа метелик — за умови швидкої зміни стану системи під впливом п'яти параметрів управління;
   – Хвіст ластівки — за умови об'єднання двох параметрів, оскільки даний тип описує систему, що залежить від чотирьох параметрів;
   – Складка — за умови випливу двох параметрів, яка можлива при моделюванні впливу доступності та властивостей інформації [10].
3. 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 [11].
4. 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 [13]. Формула для кроку 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:
$$\frac{dx}{dt} = -\frac{dV(x)}{dx} = -(6x^5 + 4ax^3 + 3bx^4 + 2cx + d) \quad (1)$$
Проведений аналіз даного диференціально рівняння показує, що точки, де
$$\frac{dx}{dt} = 0, \quad (2)$$
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 [14] – [16]. Даний стан можливий при моделюванні ситуації, коли кількість кіберінцидентів стрибне до критичних значень, що призведе до збоїв системи.

Дана модель описує реакції системи на різні типи кіберінцидентів, а також важливо встановити пріоритетність параметрів, які мають найбільший вплив на стійкість інформаційної системи, що дозволить виявити катастрофічні зміни в стані системи в майбутньому.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Теорії катастроф для моделювання систем захисту у кібербезпеці доцільно реалізовувати за допомогою Python, з бібліотекою Pandas для обробки даних, математичних обчислень та чисельного моделювання.

Дослідження впливу інцидентів, які зібрані за 2022–2024 роки, на стійкість системи управління інформаційної безпеки в ЗСУ реалізовано наступними кроками.

Визначення категорій інцидентів і параметрів. Проведено аналіз категорій інцидентів і параметрів за допомогою бібліотеки Pandas. Початкову оцінку впливу кожного інциденту можна встановити, якщо підрахувати кількість інцидентів по кожній

категорії, а також визначити частоту інцидентів, яка характерна для кожної категорії за період 2022–2024 років (табл. 1). Чим вищий середній рівень інцидентів, тим більше даний вид загрози впливає на систему.

Таблиця 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

Для візуалізації досліджених даних побудовано графіки розподілу інцидентів по категоріях за допомогою бібліотек Matplotlib та Seaborn (рис. 1 та рис. 2).

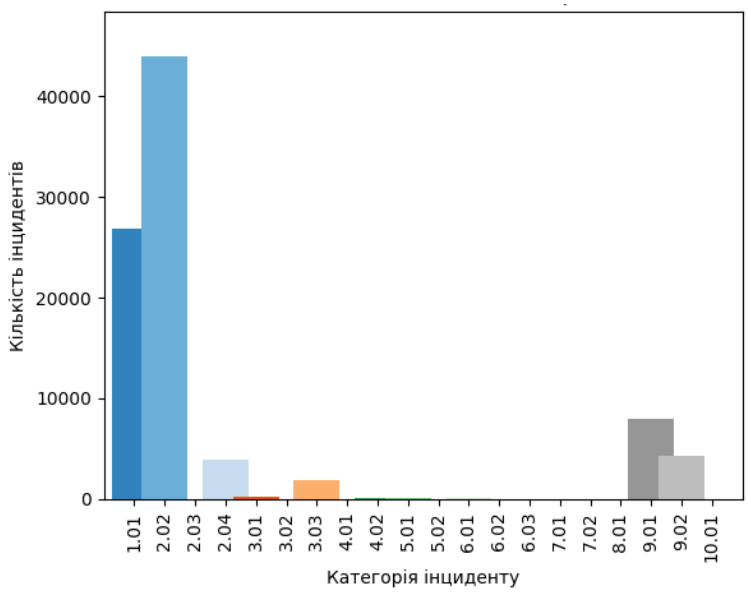

Рис. 1. Кількість інцидентів за 2022–2024 роки

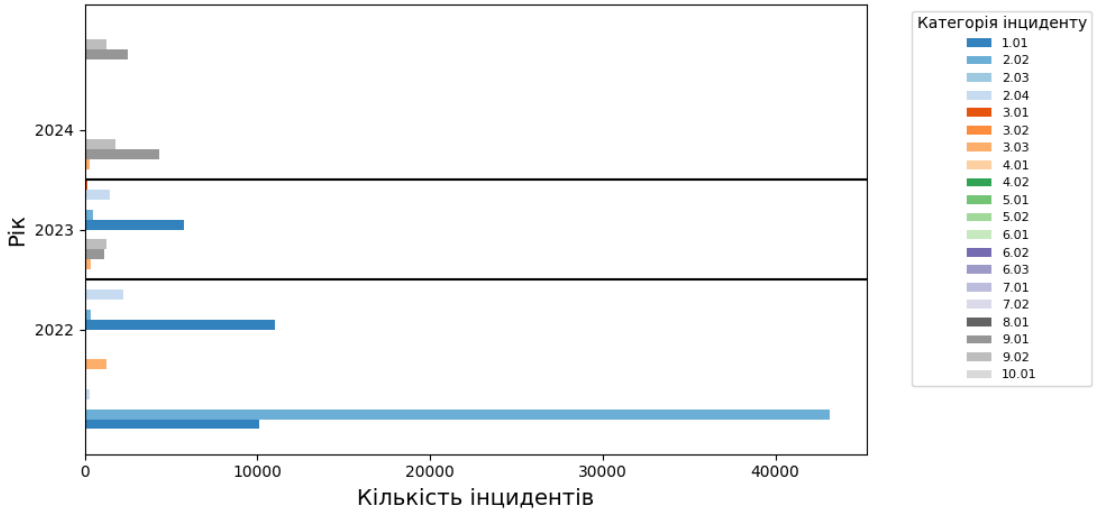

Рис. 2. Кількість інцидентів по роках і категоріях

Проведений аналіз набору даних показав категорій інцидентів, які виявлені у період 2022–2024 років, 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 вразливість (9.01, 9.02), які мали найбільший вплив на інформаційну систему ЗСУ. Тому дані категорії вибрані, як основні параметри для побудови моделі впливу інцидентів кібербезпеки на стійкість системи управління інформаційної безпеки в ЗСУ.

Визначення ваги параметрів впливу на систему. Інформація про кількість інцидентів кожної категорії, а також середній рівень (кількість) кожної категорії, дозволяє розрахувати вагу для кожної категорії інцидентів за формулою:

$$\frac{dx}{dt} = 0, \tag{3}$$

де n_i — кількість інцидентів у i-категорії; $i = \overline{1,m}$ — категорії інцидентів; k_i — середня кількість інцидентів у кожній i-категорії

Вагу для кожної з 5-ти категорій інцидентів знаходимо за допомогою Python і наданої бази даних інцидентів. Для початку підсумували кількість інцидентів кожної вибраної категорії і використали формулу (3). Результати розрахунків наведено в табл. 2.

Таблиця 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 вразливість	9.01 Вразливість 9.02 Некоректна конфігурація	0.0056

Побудова моделі виявлення впливу кіберінцидентів на стійкість інфопмаційної системи на основі теорії катастроф.

Для побудов математичної моделі використано теорію катастроф, розрахунок і візуалізацію здійснено за допомогою Python, бібліотек Numpy та Plotly.graph_objects. В рівняння (1) закладено параметри (спам, шкідливий програмний код, атаки на відмову в обслуговуванні, вразливості) і їх вагу з табл. 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.

Потрібно відмітити, що рівняння (1) модифікувано для врахування 4-х інцидентів впливу з табл. 2 та аналізу фазових переходів між станами:

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

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).

ISSN 2663 - 4023

Вміст рівняння (4) дозволяє моделювати асимптотичну поведінку системи, особливо в умовах значень змінної x, які виходять за межі допустимого діапазону. Також дана модель описує 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. 3). Дана візуалізація показує, що параметри $e\ i\ f$, мають малі ваги і змінюють лише асимптотику потенціалу, що впливає на зображення моделі катастрофи.

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.

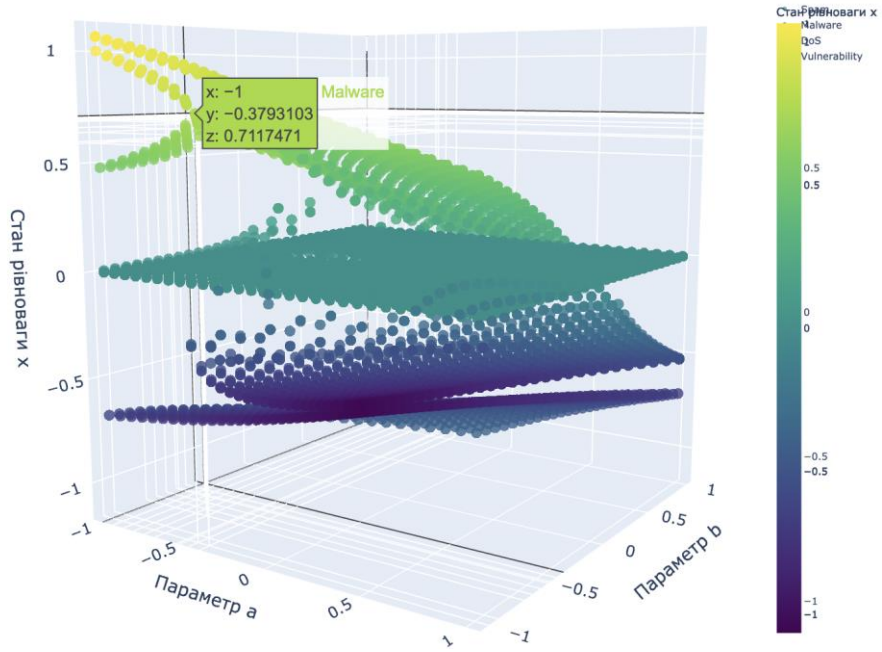

Рис. 3. Точки рівноваги та біфуркації для моделі катастрофа «Метелик»

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. 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 біфуракції 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 Вразливість ($w = 0.0056$) створює потенційні точки входу для інших інцидентів, таких як Malware або DoS.

ISSN 2663 - 4023

На графіку (рис. 3) точки біфуракції 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), 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.

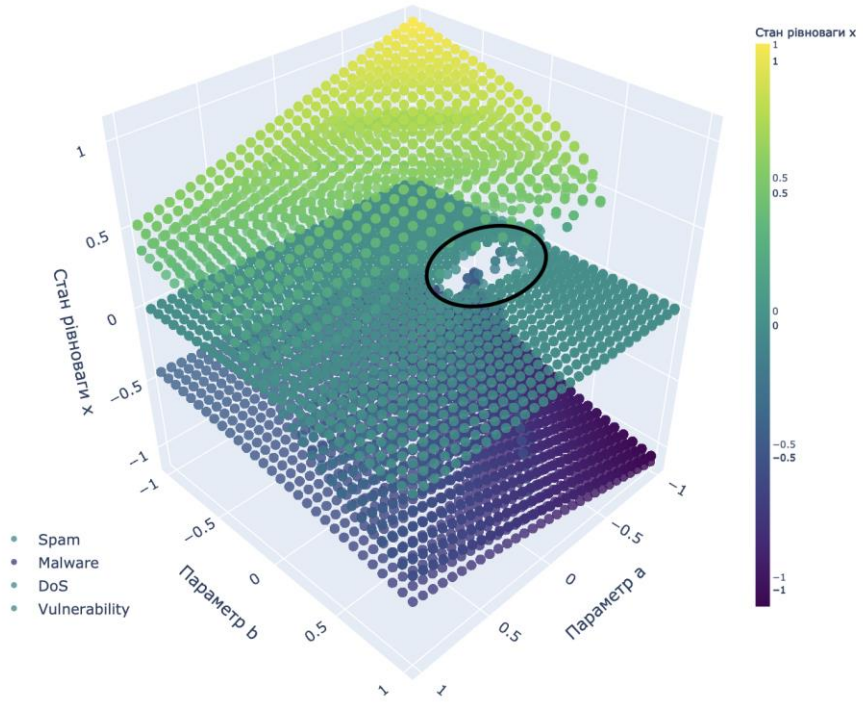

Рис. 4. Наявність зони ризику «дірки» на площині точок рівноваги

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

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 Вразливості систем) впливають на стійкість і рівновагу інформаційної системи.

На основі проведених досліджень виявлено, що кожен з інцидентів має свій вплив на стійкість інформаційної системи. Для встановлення даного впливу проаналізовано різні типи інцидентів, які представлені у звіті відділу Кібербезпеки ЗСУ за 2022–2024 роки. Розрахунок ваги кожного типу інциденту здійснено на основі їх кількості та частоти появи. Але цікавою постає задача про дослідження даних типів інцидентів, якщо вагу коефіцієнтів розраховувати як якісний показник впливу кожного типу інциденту на інформаційну систему.

Проведено моделювання на основі катастрофи «Метелик» для знаходження точок рівноваги та критичних точок, які характеризують стійкіст та біфуркацію динамічної

системи. Встановлено також наявність зони ризику «дірки» на площині точок рівноваги системи, яка критично важливу і чутлива до збурень, що відповідає небезпечним або хаотичним режимам збою інформаційної системи під впливом кіберінцидентів типу Malware та Vulnerability.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Shevchenko, S., Zhdanova, Y., Spasiteleva, S., Negodenko, O., Mazur, N., & Kravchuk, K. (2019). Mathematical methods in cyber security: fractals and their applications in information and cyber security. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 1(5),* 31–39. https://doi.org/10.28925/2663-4023.2019.5.3139
2. Shevchenko, S., Zhdanova, Y., Skladannyi, P., & Spasiteleva, S. (2021). Mathematical methods in cibernetic security: graphs and their application in information and cybernetic security. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 1(13),* 133–144. https://doi.org/10.28925/2663-4023.2021.13.133144
3. 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, vol. 3187(1),* 276–283.
4. 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
5. Lysenko, N. O., Mazurenko, V. B,. Fedorovych, A. I., Astakhov, D. S., & Statsenko, V. I. (2021). Overview of mathematical methods in cyber threat detection and prevention systems. *Actual problems of automation and information technologies, 25,* 91–102
6. 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.*
7. Tom, R. (1977). Structural stability, catastrophe theory, and applied mathematics. *SIAM Review, 19(2),* 189–201.
8. Zeeman, E. C. (1976). Catastrophe theory. *Scientifc American, 234(4),* 65–83.
9. Negodenko, V. (2023). Investigation of information conflicts in the education system of the zsu with the help of simulation. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 4(20),* 164–173. https://doi.org/10.28925/2663-4023.2023.20.164173
10. Shevchenko, S., Zhdanova Y., & Spasiteleva, S. (2023). Mathematical methods in cybersecurity: catastrophe theory. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 3(19),* 165–175. https://doi.org/10.28925/2663-4023.2023.19.165175
11. Alhidaifi, S. M., Asghar, M. R., & Ansari, I. S. (2024). 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
12. *LIST of categories of cyber incidents.* (б. д.). https://cert.gov.ua/recommendation/16904
13. Bottou L. (2012). *Stochastic Gradient Descent Tricks//Microsoft. Research*. http://research.microsoft.com/pubs/192769/tricks-2012.pdf
14. Schneider, F. B. (2000). Enforceable Security Policies. *ACM Transactions on Information and System Security (TISSEC), 2(4),* 234–260.
15. Khalil H. K. (2002). *Nonlinear systems*. NJ.: Prentice Hall.
16. Гулак, Г. М., Жильцов, О. Б., Киричок, Р. В., Коршун, Н. В., & Складанний, П. М. (2024). *Інформаційна та кібернетична безпека підприємства.* Підручник. Львів : Видавець Марченко Т. В.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023

Vitalii Nehodenko
Postgraduate student of the Department of Information and Cyber Security
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0002-7678-9138
v.nehodenko.asp@kubg.edu.ua

APPLICATION OF THE MATHEMATICAL CATASTROPHE THEORY TO ENSURE THE STABILITY OF THE INFORMATION SECURITY MANAGEMENT SYSTEM

Abstract. The Information Security Management System is an important element in preventing possible threats and failures, exposure to various internal and external factors, which could lead to irreversible consequences. Predicting the impact of various types of incidents allows to ensure the stability and balance of complex dynamic systems, their confidentiality, integrity and availability. The resilience of the information security management system to different types of cyber incidents has been researched. Mathematical Catastrophe theory has been applied to model the dynamics of the information system. Different types of catastrophes that depend on the number of influencing parameters on the dynamic system were analyzed and investigated. The main types of incidents for research have been identified based on the report of detected cyber incidents in the period 2022–2024. It was analyzed the list of categories of cyber incidents, which is constantly updated taking into account the appearance of new types, and also includes a description of these incidents and their impact on the information system. The "Butterfly" type of catastrophe has been chosen to simulate the behavior of dynamic systems in crisis situations, assess the degree of system stability, and identify critical points where the system is particularly vulnerable to external or internal disruptive influences. Equilibrium points, bifurcation points, and a risk zone have been identified on the system's equilibrium plane, which is critically important and sensitive to disturbances, corresponding to information system failures of dangerous or chaotic types under the influence of certain types of cyber incidents. Python and some libraries (such as Numpy, Pandas etc) have been used for calculations and visualization. The 3D graphs show the dependence of the dynamic system's equilibrium state on the parameters of the impact of each type of incident.This allows to identify possible failures of the information system and optimize the operation of the information security management system to prevent catastrophes.

Keywords: Information security management system (ISMS); catastrophe theory; "Butterfly" type of catastrophe; cyber incident; Python; gradient descent; differential equation.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Shevchenko, S., Zhdanova, Y., Spasiteleva, S., Negodenko, O., Mazur, N., & Kravchuk, K. (2019). Mathematical methods in cyber security: fractals and their applications in information and cyber security. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 1(5),* 31–39. https://doi.org/10.28925/2663-4023.2019.5.3139
2. Shevchenko, S., Zhdanova, Y., Skladannyi, P., & Spasiteleva, S. (2021). Mathematical methods in cibernetic security: graphs and their application in information and cybernetic security. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 1(13),* 133–144. https://doi.org/10.28925/2663-4023.2021.13.133144
3. 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, vol. 3187(1),* 276–283.
4. 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

5. Lysenko, N. O., Mazurenko, V. B,. Fedorovych, A. I., Astakhov, D. S., & Statsenko, V. I. (2021). Overview of mathematical methods in cyber threat detection and prevention systems. *Actual problems of automation and information technologies, 25*, 91–102
6. 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.*
7. Tom, R. (1977). Structural stability, catastrophe theory, and applied mathematics. *SIAM Review, 19(2),* 189–201.
8. Zeeman, E. C. (1976). Catastrophe theory. *Scientifc American, 234(4),* 65–83.
9. Negodenko, V. (2023). Investigation of information conflicts in the education system of the zsu with the help of simulation. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 4(20),* 164–173. https://doi.org/10.28925/2663-4023.2023.20.164173
10. Shevchenko, S., Zhdanova Y., & Spasiteleva, S. (2023). Mathematical methods in cybersecurity: catastrophe theory. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 3(19),* 165–175. https://doi.org/10.28925/2663-4023.2023.19.165175
11. Alhidaifi, S. M., Asghar, M. R., & Ansari, I. S. (2024). 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
12. *LIST of categories of cyber incidents.* (n. d.). https://cert.gov.ua/recommendation/16904
13. Bottou L. (2012). *Stochastic Gradient Descent Tricks//Microsoft. Research*. http://research.microsoft.com/pubs/192769/tricks-2012.pdf
14. Schneider, F. B. (2000). Enforceable Security Policies. *ACM Transactions on Information and System Security (TISSEC), 2(4),* 234–260.
15. Khalil H. K. (2002). *Nonlinear systems*. NJ.: Prentice Hall.
16. Hulak, H. M., Zhiltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2024). *Information and cyber security of the enterprise.* Textbook. Lviv: Publisher Marchenko T. V.