КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (19), 2023
ISSN 2663 - 4023

DOI 10.28925/2663-4023.2023.19.165175
УДК 004.94:519.21

Шевченко Світлана Миколаївна
кандидат педагогічних наук, доцент,
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID: 0000-0002-9736-8623
s.shevchenko@kubg.edu.ua

Жданова Юлія Дмитрівна
кандидат фізико-математичних наук, доцент,
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID: 0000-0002-9277-4972
y.zhdanova@kubg.edu.ua

Спасітєлєва Світлана Олексіївна
кандидат фізико-математичних наук, доцент,
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID: 0000-0003-4993-6355
s.spasitielieva@kubg.edu.ua

МАТЕМАТИЧНІ МЕТОДИ В КІБЕРБЕЗПЕЦІ: ТЕОРІЯ КАТАСТРОФ

Анотація. Удосконалення систем захисту інформації базується на впровадженні і застосуванні математичного апарату. Забезпечення конфіденційності, цілісності і доступності інформації є актуальною і важливою проблемою сучасного світу. Кризові процеси є характерними явищами у системах безпеки, тому стохастичні моделі не завжди можуть описати їх функціонування та надати рішення. Ефективним інструментарієм для вирішення даної проблеми може стати використання динамічних моделей, що ґрунтуються на положеннях теорії катастроф.

Дане дослідження присвячене аналізу сучасних підходів до використання основних положень теорії катастроф у системах кібербезпеки. У роботі представлено стисло історичний ракурс розвитку даної теорії та висвітлені основні дефініції: біфуркації, атрактори, катастрофи. Охарактеризовані елементарні катастрофи, їх форми та особливості. Здійснено огляд літературних джерел щодо застосування теорії катастроф в інформаційній та кібернетичній безпеці. Аналіз дозволив виділити, що дана теорія не набула ще широкого впровадження, але є точкові наукові наробки у процесі виявлення мережевих аномалій у хмарному середовищі.

Розглянуті підходи до застосування теорії катастроф в інформаційній та кібернетичній безпеці можуть бути використані при підготовці фахівців спеціальності 125 Кібербезпека у процесі науково-дослідної роботи.

Ключові слова: системи кібербезпеки; захист інформації; динамічні моделі; математичні методи; теорія катастроф; біфуркації; аттрактори; елементарні катастрофи.

ВСТУП

Постановка проблеми. Увага до теорії катастроф обумовлена розробкою нових принципів побудови та реалізації систем захисту інформації. Сучасний світ – інформаційний, тому забезпечення конфіденційності, цілісності та доступності інформації є важливою та актуальною проблемою сьогодення. Все це спонукає науковців та практиків до удосконалення та пошуку стійких і ефективних методів та технологій для вирішення даної проблеми. Раціональним інструментарієм, як показує практика, є розробка математичних моделей та їх реалізація у системах безпеки [1 – 7].

Системи інформаційної та кібернетичної безпеки – динамічні системи, які не можуть перебувати тривалий час у рівновазі. Їм властиві випадкові рухи, переходи із одного стану в інший, у результаті яких можливі деградації та руйнації попередніх структур та відновлення у якісно іншому стані [8]. Для дослідження таких систем, коли виникають різкі зміни та стрибкоподібні процеси, що пов'язані з інцидентами у інформаційній та кібернетичній безпеці, є логічним застосувати положення теорії катастроф.

Аналіз основних досліджень і публікацій. Теорія катастроф – частина теорії складних нелінійних систем. Завдяки зусиллям вчених, елементарна теорія катастроф дозволяє звести величезну кількість ситуацій до невеликого числа стандартних схем, які можна детально дослідити. Значний вклад в розвиток даної науки внесли дослідники Х.Утні, А. Пуанкаре, А. Ляпунов, О. Андронов, В. Арнольд, Р. Том, К. Зіман, Р. Гілмор та інші [9 – 15].

Теорія катастроф – програма прогнозування нестійкості різних систем. Таку назву вона отримала у зв'язку з тим, що втрата стійкості може бути катастрофічною, навіть якщо вона не призводить до загибелі або руйнуванню системи, а лише обумовлює перехід до іншої траєкторії розвитку.

Основними припущеннями теорії катастроф є:

- система динамічна, тобто її стан змінюється з часом;
- принцип максимального зволікання: система прагне зберегти свій стан як можна довше;
- поточний стан системи залежить від того, яким чином система прийшла у цей стан;
- траєкторії системи незворотні, тобто при зміні основних (управлінських) параметрів системи в точності протилежним чином система не обов'язково повернеться до початкового стану.

Математичний опис світу заснований на тонкій грі неперервного та дискретного. Особливості, біфуркації, катастрофи – терміни, які описують виникнення дискретних структур з гладких і неперервних [9, 10]. Тому математичний апарат теорії катастроф має широке застосування у різних галузях суспільства, зокрема, на фінансовому ринку (в дослідженнях, прогнозуванні та оцінці ступеня стабільності економічних систем) [16]; в екологічних процесах [17]; у теорії соціальних відносин та педагогіці [18 – 20]; у інженерній справі [21].

Застосування положень теорії катастроф у задачах забезпечення захисту інформації розглянуто у працях [22 – 25].

Мета статті. Метою даної статті є аналіз існуючих підходів до використання математичного апарату теорії катастроф в області захисту інформації та визначення шляхів подальшого використання динамічних моделей у даній сфері.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Теорія катастроф – розділ прикладної математики, що вивчає сукупність математичних моделей теорії біфуркацій, теорії особливостей і деяких інших теорій, призначених для опису й аналізу якісного (зазвичай стрибкоподібного) поводження економічних, екологічних, біологічних, хімічних та інших систем за неперервної зміни параметрів [26]. Як свідчить аналіз наукових джерел [9 - 15] математичний апарат теорії катастроф базується на положеннях топології та математичного аналізу, а саме, теорії особливостей гладких відображень Х. Уітні, теорії стійкості та біфуркацій динамічних систем А. Пуанкаре, А. Ляпунова, А. Андронова. Ці наукові наробки мали розвиток у дослідженнях Р. Тома, який у 1960-х роках і виклав дану теорію у дослідженні «Структурна стабільність і морфогенез».

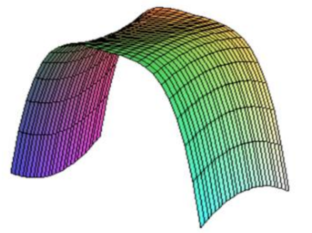
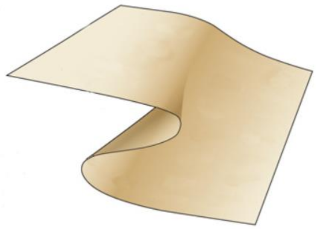
Динамічною системою називають математичну абстракцію, призначену для опису та вивчення еволюції систем у часі, тобто це математична модель деякого об'єкта, процесу або явища. Для вивчення ж динаміки систем необхідно знати, яким саме чином нові розв'язки рівнянь "відгалужуються" від відомого розв'язку. Відповідь на такі питання дає теорія біфуркацій (розгалужень), тобто виникнення нових розв'язків при критичному значенні певного параметра. Момент переходу (катастрофічний стрибок) залежить від властивостей системи і рівня флуктуацій (коливань). Отже, біфуркація – придбання нової якості в рухах динамічної системи при малій зміні її параметрів. Біфуркація означає роздвоєння, поділ, розгалуження чогось, стан процесу в динамічній системі, при якому різко зростають флуктуації, і вихід з якого можливий за двома суттєво різними і важко передбачуваними напрямами — хаотичному чи впорядкованому.

Множини, що характеризують значення параметрів системи на альтернативних траєкторіях, називаються атракторами. У точці біфуркації відбувається катастрофа – перехід системи від області притягнення одного атрактора до іншого.

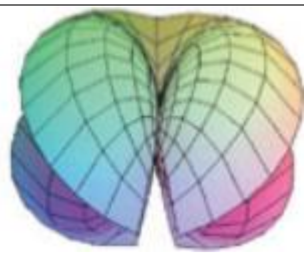
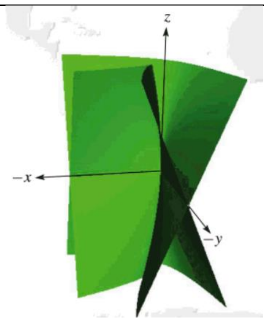
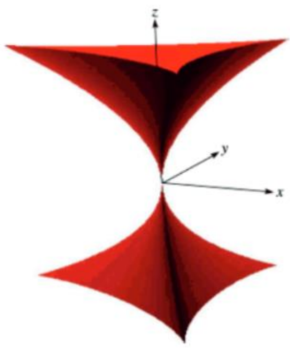
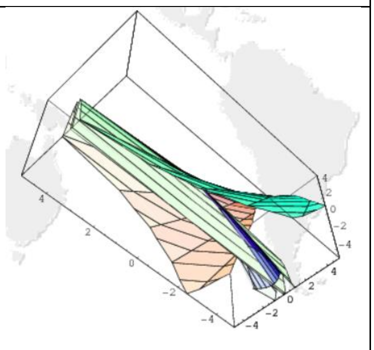
Катастрофа – стрибкоподібна зміна, що виникає у вигляді раптового відгуку системи на плавну зміну зовнішніх умов, тобто різка якісна зміна об'єкта при плавному кількісному зміненні параметрів, від яких залежить об’єкт. При катастрофі під дією керуючих параметрів змінюється стаціонарний стан системи, тобто вона переходить із одного стаціонарного стану до іншого. Як проходить перехідний процес для теорії катастроф, по суті, неважливо. Стани можуть бути як нерухомими, так і рухомими. Р. Том довів важливу теорему в теорії катастроф, яка допомогла класифікувати катастрофи і які носять назву елементарні чи канонічні катастрофи (таблиця 1).

Таблиця 1.

Типи елементарних катастроф

№ з/п	Тип катастрофи	Канонічна форма	Ілюстрація
1	Складка – руйнування центру притягання і поглинання його центром притягання з меншим потенціалом.	$Y_1^3 + UY_1$	
2	Збірка – поділ центру притягання на два окремих центри.	$\pm\left(Y_1^4 + U_1\frac{Y_1^2}{2} + U_1Y_1\right)$	

ISSN 2663 - 4023

№ з/п	Тип катастрофи	Канонічна форма	Ілюстрація
3	Хвіст ластівки – поверхня фронту хвилі утворює борону, дном якої служить ударна хвиля.	$Y^5+U_1Y^3+U_2Y^3+U_3Y$	
4	Метелик – виникає в результаті розшарування набухання ударної хвилі із вільною границею	$\pm(Y^6+U_1Y^4+U_2Y^3+U_3Y^2+U_4Y)$	
5	Гіперболічна омбілічна точка представляє собою гребінь хвилі, що розпадається	$Y_1^2Y_2+Y_2^3+U_1Y_1^2+U_2Y_1+U_3Y_2$	
6	Еліптична омбілічна точка представляє собою кінчик шипа типу загостреної піраміди з трикутною основою	$Y_1^2Y_2-Y_2^3+U_1Y_1^2+U_2Y_1+U_3Y_2$	
7	Параболічна омбілічна точка – структура, перехідна між гіперболічним і еліптичним типами, що має форму гриба, утвореного потоком	$\pm(Y_1^2Y_2+Y_2^4+U_1Y_1^2+U_2Y_2^2+U_3Y_1$ $+U_4Y_2)$	

Рівняння системи задається у загальному вигляді так:

$$\frac{dx}{dt} = F(x, \lambda)$$

або в координатному виді

$$\frac{dx_i}{dt} = F_i(x, \lambda), \qquad i = \underline{1, n}\,,$$

де $F(x, \lambda)$ – нелінійна векторзначна функція, x – вектор стану, λ – вектор керуючих параметрів мірності k.

Том Р. розглядав градієнтні системи, тобто такі, для яких виконується умова $\frac{dx}{dt} = -\frac{\partial E}{\partial x}$. Цей вираз пояснюється наступним чином. В правій частині міститься частинна похідна від потенціальної функції $E = E(x, \lambda)$ системи по вектору станів, тобто антиградієнт (з-за знаку «–») потенціальної функції. Для технічних систем потенціальна функція ототожнюється з потенціальною енергією. Антиградієнт напрямлений у бік зменшення потенціальної функції, а його довжина визначає швидкість цього зменшення. В лівій частині міститься похідна за часом від координат системи, тобто швидкість їх зміни в часі. Функціонування градієнтних систем є досягнення максимуму потенціальної функції (енергії). У стаціонарних точках похідна $\frac{dx}{dt}$ дорівнює нулю, отже, градієнт потенціальної функції також дорівнює нулю, а це є необхідною умовою мінімуму потенціальної функції.

Для мінімізації потенціальної функції є k одиниць керуючих параметрів $\lambda_1, \lambda_2, \ldots, \lambda_k$. Змінюючи їх так, щоб потенціальна функція мала мінімум, система приводиться у стан рівноваги.

Очевидно, що існує множина (нескінченна) таких градієнтних систем. Між іншим, якщо ввести, потрібні перетворення координат векторів x і λ, то багато з цих систем виявляться ідентичними, близькими за поведінкою.

Теорема Тома дозволяє класифікувати всі гладкі потенціальні функції. Найбільш важливою властивістю цієї класифікації є те, що вона залежить тільки від числа k керуючих параметрів, яке вважається скінченним.

Отже, нехай у деякій задачі функція $E(x, \lambda)$ невідома, тобто не існує математичної моделі системи, але припускається, що $E(x, \lambda)$ існує. Завдяки класифікації (таблиця 1) створюється модель системи, використовуючи невеликий набір скінченного числа елементарних потенціальних функцій, припускаючи, що від реальної системи модель буде відрізнятися тільки перетворенням координат. Крім того, теорема Тома гарантує структурну стійкість канонічної моделі. Отже, модель повинна проявляти ті самі властивості топологічного характеру, що й канонічна модель. Цим підтверджується важливість теореми Тома і її застосування у різних сферах.

Загалом, теорія катастроф застосовується до систем, які можуть реагувати на безперервні зміни керуючих змінних переривчастою зміною від одного стану рівноваги до іншого.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

На сучасному етапі, коли ймовірнісні підходи до оцінювання інформаційних ризиків не спрацьовують, а обсяг статистичних даних щодо інцидентів у системах безпеки не достатньо великий для доведення гіпотез, вчені пропонують розробляти динамічні моделі на основі теорії катастроф.

Як свідчить аналіз відповідної літератури науковці з безпеки вбачають застосування даної теорії у процесі виявлення мережевих аномалій, зокрема у хмарному середовищі.

Аномалії мережі можна класифікувати на два види [27]. Перший тип — це проблеми безпеки, які включають UDP-флуд, ping-todeath і TCP SYN-атаку. Їх функція – затоплення жертви високошвидкісним потоком, запитами, захват ресурсів інформаційної системи. Другий тип — це збої мережі, які включають збої файлового сервера, широкомовні шторми та тимчасові перевантаження. У дослідженні [22] авторам вдалося підійти до процесу виявлення вторгнень внаслідок застосування теорії катастроф. Завдяки спостереженням і аналізу мережевих даних, вони припускають, що катастрофа на вершині є найкращою для опису аномальної поведінки мережі. Модель катастрофи на вершині включає три поверхні: верхню поверхню, середню поверхню та нижню поверхню. Верхня поверхня представляє ненормальний стан мережі, нижня поверхня представляє нормальний стан мережі, а середня поверхня представляє нееквіпотенціальний стан мережі. Експеримент показав позитивні результати.

У роботах [23; 24] було запропоновано дві моделі виявлення аномалій на основі теорії катастроф у мережевому трафіку. Результати експерименту показали, що підхід може ефективно виявляти аномалії мережі та досягати високої ймовірності виявлення та низького рівня помилкових тривог.

У науковій розробці [25] було запропоновано ідею мережевого виявлення вторгнень у хмарному середовищі. На думку авторів, проблемою у виявленні аномалій є застосування динамічної природи хмарного трафіку в його прогнозуванні при збереженні прийнятного рівня точності, окрім зменшення обчислювальних витрат. З іншого боку, щоб подолати проблему додаткового часу навчання, впровадження високошвидкісного алгоритму є важливим. Тому саме теорія катастроф є ефективним інструментарієм для опису процесів раптової зміни мережі через динамічну природу хмари. Експоненціальне ковзне середнє застосовується до змінної стану в ковзному вікні, щоб краще показати динаміку трафіку хмарної мережі. Ентропія використовується як одна з керуючих змінних у теорії катастроф для аналізу розподілу характеристик руху. Розроблено програмне забезпечення і експериментально було доведено, що даний підхід є більш ефективним, ніж у роботі [24].

Математичний інструментарій теорії катастроф – новий напрям для моделювання систем захисту у кібербезпеці. Потрібно відмітити, що її застосування лише починається, не завжди використання при моделюванні математичної теорії катастроф приводить до адекватного відображення процесів, що моделюються [28].

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Інтерес до теорії катастроф у системах інформаційної та кібернетичної безпеки з метою дослідження динамічних моделей захисту інформації є очевидним. Кризові явища у сучасному світі є характерними і для систем безпеки. Їх аналіз за допомогою математичного апарату катастроф дозволить знайти нові шляхи забезпечення захисту інформаційних активів.

Слід відмітити, що увага у даному дослідженні була зосереджена, насамперед, на пошук шляхів застосування теорії катастроф у системах безпеки, проведення глибшого аналізу планується в перспективі. Вочевидь, можливості теорії катастроф дозволять розглянути поведінку системи, пов’язану з інсайдерською діяльністю, змоделювати і оцінити ризики кібербезпеки.

Розглянуті підходи до застосування теорії катастроф в інформаційній та кібернетичній безпеці можуть бути використані при підготовці фахівців спеціальності 125 Кібербезпека у процесі науково-дослідної роботи.

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. *Cybersecurity: Education, Science, Technique*, (5), 31–39. https://doi.org/10.28925/2663-4023.2019.5.3139.

2 Шевченко, С.М., Жданова, Ю.Д., Складанний, П.М., Спасітєлєва, С.О. (2021). Математичні методи в кібербезпеці: графи та їх застосування в інформаційній та кібернетичній безпеці. *Кібербезпека: освіта, наука, техніка*, 1(13), 133-144.

3 Шевченко, С.М., Жданова, Ю.Д., Кравчук, К.В. (2021). Модель захисту інформації на основі оцінки ризиків інформаційної безпеки для малого та середнього бізнесу. *Кібербезпека: освіта, наука, техніка*, *2*(14), 158-175.

4 Shevchenko, H., Shevchenko, S., Zhdanova, Yu., Spasiteleva, S., Negodenko, O. (2021). Information Security Risk Analysis SWOT. *CEUR Workshop Proceedings*, 2923, 309-317.

5 Negodenko, O., Shevchenko, S., Trintina, N., Astapenya, V., Tereshchenko, O. (2021). Problematic Issues of Approximation and Interpolation in Signal Processing in Secure Information Systems. *CEUR Workshop Proceedings*, *3187*(1), 276-283.

6 Шевченко, С.М., Складанний, П.М., Негоденко, О.В., Негоденко, В.П. (2022). Дослідження прикладних аспектів теорії конфліктів у системах безпеки. *Кібербезпека: освіта, наука, техніка*, 2(18), 150-162.

7 Лисенко, Н. О., Мазуренко, В. Б,. Федорович, А. І., Астахов, Д. С., Стаценко, В. І. (2021). Огляд математичних методів у системах виявлення та попередження кіберзагроз. *Актуальні проблеми автоматизації та інформаційних технологій*, 25, 91-102.

8 Haken, H. (2009). Synergetics: Basic Concepts. У *Encyclopedia of Complexity and Systems Science* (с. 8926–8946). Springer New York. https://doi.org/10.1007/978-0-387-30440-3_533

9 Arnold, V. I. (2012). *Catastrophe Theory*. Springer, Berlin Heidelberg. https://doi.org/10.1007/978-3-642-96937-9

10 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

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

12 Robbin, J. W. (2013). *Tom's catastrophe theory and Zeeman's model of the stock market*. Chaos and Complexity Seminar.

13 Qin, S., Jimmy Jiao, J., Wang, S., & Long, H. (2001). A nonlinear catastrophe model of instability of planar-slip slope and chaotic dynamical mechanisms of its evolutionary process. *International Journal of Solids and Structures*, *38*(44-45), 8093–8109. https://doi.org/10.1016/s0020-7683(01)00060-9.

14 Zeeman, E. C. (1976). Catastrophe theory. *Scientifc American*, *234*(4), 65–83.

15 Wagenmakers, E.-J., Molenaar, P. C. M., Grasman, R. P. P. P., Hartelman, P. A. I., & van der Maas, H. L. J. (2005). Transformation invariant stochastic catastrophe theory. *Physica D: Nonlinear Phenomena*, *211*(3-4), 263–276. https://doi.org/10.1016/j.physd.2005.08.014

16 Angelis, V., Dimaki, K. (2012). A bank's attractiveness as described by a cusp catastrophe model. In *25th European Conference on Operational Research*. Vilnius. https://www.researchgate.net/publication/340941439_A_Bank's_Attractiveness_as_described_by_a_Cusp_Catastrophe_Model

17 Хлєстова, О.А., Єлістратова, Н.Ю., Кальянов, А.В., Волков, Д.В. (2020). Використання математичної теорії катастроф у промисловій екології. *Екологічні науки*, 3(30), 15-19. http://ecoj.dea.kiev.ua/30-2020

18 Коляда, М.Г. (2010). Використання теорії катастроф для визначення оптимальної кількості компетентностей майбутнього фахівця сфери інформаційної безпеки. *Науковий вісник Донбасу*, 1. http://nbuv.gov.ua/UJRN/nvd_2010_1_5

19 Stamovlasis, D. (2016). Catastrophe Theory: Methodology, Epistemology, and Applications in Learning Science. У *Complex Dynamical Systems in Education* (с. 141–175). Springer International Publishing. https://doi.org/10.1007/978-3-319-27577-2_9

20 Isnard, C. A., Zeeman, E. C. (2020). *Some models from catastrophe theory in the social sciences*. The Use Of Models in Social Sciences, Taylor & Francis.

21 Liu, J., Bao, J., Yin, Y., & Yang, S. (2015). Applications of Catastrophe Theory in Engineering: A Review. *Journal of Computational and Theoretical Nanoscience*, *12*(12), 5739–5744. https://doi.org/10.1166/jctn.2015.4710

22 Lin, J., Yang, X., Long, K., & Peng, Y. (2008). Catastrophe model construction and verification for network anomaly detection. У W. Hu, S.-K. Liu, K.-i. Sato & L. Wosinska (Ред.), *Asia Pacific Optical Communications*. SPIE. https://doi.org/10.1117/12.804305.

23 Xiong, W., Xiong, N., Yang, L. T., Vasilakos, A. V., Wang, Q., & Hu, H. (2010). Network traffic anomaly detection based on catastrophe theory. У *2010 Ieee Globecom Workshops*. IEEE. https://doi.org/10.1109/glocomw.2010.5700309.

24 Xiong, W., Xiong, N., Yang, L. T., Park, J. H., Hu, H., & Wang, Q. (2011). An anomaly-based detection in ubiquitous network using the equilibrium state of the catastrophe theory. *The Journal of Supercomputing*, *64*(2), 274–294. https://doi.org/10.1007/s11227-011-0644-y.

25 Khatibzadeh, L., Bornaee, Z., Bafgh, A.G. (2019). Applying Catastrophe Theory for Network Anomaly Detection in Cloud Computing Traffic. *Security and Communication Networks*. https://doi.org/10.1155/2019/5306395

26 Великий тлумачний словник (ВТС) сучасної української мови. http://slovopedia.org.ua/53/53410/363176.html

27 Millard, E. (2005). *Internet attacks increase in number, severity*. Top Tech News.

28 Мокін, Б. І., Войцеховська, О. О. (2022). Про деякі наслідки некоректного застосування в прикладних дослідженнях математичної теорії катастроф. У *Матеріали міжнародної науково-методичної Інтернет–конференції «Проблеми вищої математичної освіти: виклики сучасності»*, Вінниця, 2022. https://conferences.vntu.edu.ua/index.php/pmovc/pmovc22/paper/view/16291

Svitlana M. Shevchenko
PhD, Associate Professor,
Associate Professor of the Department of Information and Cyber Security
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID: 0000-0002-9736-8623
s.shevchenko@kubg.edu.ua

Yuliia D. Zhdanova
PhD, Associate Professor,
Associate Professor of the Department of Information and Cyber Security
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID: 0000-0002-9277-4972
y.zhdanova@kubg.edu.ua

Svitlana O. Spasiteleva
PhD, Associate Professor,
Associate Professor of the Department of Information and Cyber Security
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID: 0000-0003-4993-6355
s.spasitielieva@kubg.edu.ua

MATHEMATICAL METHODS IN CYBERSECURITY: CATASTROPHE THEORY

Abstract. The improvement of protection systems is based on the introduction and use of a mathematical apparatus. Ensuring the confidentiality, integrity and availability of information is an urgent and important problem in the modern world. Crisis processes are characteristic phenomena in security systems, so stochastic models cannot always describe their functioning and give a solution. An effective tool for solving this problem can be the use of dynamic models based on the provisions of catastrophe theory.
This study is devoted to the analysis of modern approaches to the use of the basic provisions of catastrophe theory in cybersecurity systems. The work presents a brief historical view of the development of this theory and highlights the main definitions: bifurcations, attractors, catastrophes. Elementary catastrophes, their forms and features are characterized. A review of the literary sources of the use of catastrophe theory in information and cyber security was carried out. The analysis made it possible to single out that this theory has not yet been widely implemented, but there are point scientific developments in the process of detecting network anomalies in the cloud environment.
The considered approaches to the application of catastrophe theory in information and cyber security can be used to train specialists in the specialty 125 Cybersecurity in the process of research.
Keywords: cybersecurity systems; information protection; dynamic models; mathematical methods; catastrophe theory; bifurcation; attractors; elementary catastrophes.

REFERENCES

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. Cybersecurity: Education, Science, Technique, (5), 31–39. https://doi.org/10.28925/2663-4023.2019.5.3139.
2 Shevchenko, S.M., Zhdanova, Yu.D., Skladannyi, P.M., Spasitielieva, S.O. (2021). Matematychni metody v kiberbezpetsi: hrafy ta yikh zastosuvannia v informatsiinii ta kibernetychnii bezpetsi. Kiberbezpeka: osvita, nauka, tekhnika, 1(13), 133-144.
3 Shevchenko, S.M., Zhdanova, Yu.D., Kravchuk, K.V. (2021). Model zakhystu informatsii na osnovi otsinky ryzykiv informatsiinoi bezpeky dlia maloho ta serednoho biznesu. Kiberbezpeka: osvita, nauka, tekhnika, 2(14), 158-175.

4 Shevchenko, H., Shevchenko, S., Zhdanova, Yu., Spasiteleva, S., Negodenko, O. (2021). Information Security Risk Analysis SWOT. CEUR Workshop Proceedings, 2923, 309-317.

5 Negodenko, O., Shevchenko, S., Trintina, N., Astapenya, V., Tereshchenko, O. (2021). Problematic Issues of Approximation and Interpolation in Signal Processing in Secure Information Systems. CEUR Workshop Proceedings, 3187(1), 276-283.

6 Shevchenko, S.M., Skladannyi, P.M., Nehodenko, O.V., Nehodenko, V.P. (2022). Doslidzhennia prykladnykh aspektiv teorii konfliktiv u systemakh bezpeky. Kiberbezpeka: osvita, nauka, tekhnika, 2(18), 150-162.

7 Lysenko, N. O., Mazurenko, V. B,. Fedorovych, A. I., Astakhov, D. S., Statsenko, V. I. (2021). Ohliad matematychnykh metodiv u systemakh vyiavlennia ta poperedzhennia kiberzahroz. Aktualni problemy avtomatyzatsii ta informatsiinykh tekhnolohii, 25, 91-102.

8 Haken, H. (2009). Synergetics: Basic Concepts. U Encyclopedia of Complexity and Systems Science (s. 8926–8946). Springer New York. https://doi.org/10.1007/978-0-387-30440-3_533

9 Arnold, V. I. (2012). Catastrophe Theory. Springer, Berlin Heidelberg. https://doi.org/10.1007/978-3-642-96937-9

10 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

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

12 Robbin, J. W. (2013). Toms catastrophe theory and Zeemans model of the stock market. Chaos and Complexity Seminar.

13 Qin, S., Jimmy Jiao, J., Wang, S., Long, H. (2001). A nonlinear catastrophe model of instability of planar-slip slope and chaotic dynamical mechanisms of its evolutionary process. International Journal of Solids and Structures, 38(44-45), 8093–8109. https://doi.org/10.1016/s0020-7683(01)00060-9.

14 Zeeman, E. C. (1976). Catastrophe theory. Scientifc American, 234(4), 65–83.

15 Wagenmakers, E.-J., Molenaar, P. C. M., Grasman, R. P. P. P., Hartelman, P. A. I., & van der Maas, H. L. J. (2005). Transformation invariant stochastic catastrophe theory. Physica D: Nonlinear Phenomena, 211(3-4), 263–276. https://doi.org/10.1016/j.physd.2005.08.014

16 Angelis, V., Dimaki, K. (2012). A banks attractiveness as described by a cusp catastrophe model. In 25th European Conference on Operational Research. Vilnius. https://www.researchgate.net/publication/340941439_A_Banks_Attractiveness_as_described_by_a_Cusp_Catastrophe_Model

17 Khliestova, O.A., Yelistratova, N.Iu., Kalianov, A.V., Volkov, D.V. (2020). Vykorystannia matematychnoi teorii katastrof u promyslovii ekolohii. Ekolohichni nauky, 3(30), 15-19. http://ecoj.dea.kiev.ua/30-2020

18 Koliada, M.H. (2010). Vykorystannia teorii katastrof dlia vyznachennia optymalnoi kilkosti kompetentnostei maibutnoho fakhivtsia sfery informatsiinoi bezpeky. Naukovyi visnyk Donbasu, 1. http://nbuv.gov.ua/UJRN/nvd_2010_1_5

19 Stamovlasis, D. (2016). Catastrophe Theory: Methodology, Epistemology, and Applications in Learning Science. U Complex Dynamical Systems in Education (s. 141–175). Springer International Publishing. https://doi.org/10.1007/978-3-319-27577-2_9

20 Isnard, C. A., Zeeman, E. C. (2020). Some models from catastrophe theory in the social sciences. The Use Of Models in Social Sciences, Taylor & Francis.

21 Liu, J., Bao, J., Yin, Y., & Yang, S. (2015). Applications of Catastrophe Theory in Engineering: A Review. Journal of Computational and Theoretical Nanoscience, 12(12), 5739–5744. https://doi.org/10.1166/jctn.2015.4710

22 Lin, J., Yang, X., Long, K., & Peng, Y. (2008). Catastrophe model construction and verification for network anomaly detection. U W. Hu, S.-K. Liu, K.-i. Sato & L. Wosinska (Red.), Asia Pacific Optical Communications. SPIE. https://doi.org/10.1117/12.804305.

23 Xiong, W., Xiong, N., Yang, L. T., Vasilakos, A. V., Wang, Q., & Hu, H. (2010). Network traffic anomaly detection based on catastrophe theory. U 2010 Ieee Globecom Workshops. IEEE. https://doi.org/10.1109/glocomw.2010.5700309.

24 Xiong, W., Xiong, N., Yang, L. T., Park, J. H., Hu, H., & Wang, Q. (2011). An anomaly-based detection in ubiquitous network using the equilibrium state of the catastrophe theory. The Journal of Supercomputing, 64(2), 274–294. https://doi.org/10.1007/s11227-011-0644-y.

25 Khatibzadeh, L., Bornaee, Z., Bafgh, A.G. (2019). Applying Catastrophe Theory for Network Anomaly Detection in Cloud Computing Traffic. Security and Communication Networks. https://doi.org/10.1155/2019/5306395

ISSN 2663 - 4023
26 Velykyi tlumachnyi slovnyk (VTS) suchasnoi ukrainskoi movy. http://slovopedia.org.ua/53/53410/363176.html
27 Millard, E. (2005). Internet attacks increase in number, severity. Top Tech News.
28 Mokin, B. I., Voitsekhovska, O. O. (2022). Pro deiaki naslidky nekorektnoho zastosuvannia v prykladnykh doslidzhenniakh matematychnoi teorii katastrof. U Materialy mizhnarodnoi naukovo-metodychnoi Internet–konferentsii «Problemy vyshchoi matematychnoi osvity: vyklyky suchasnosti», Vinnytsia, 2022. https://conferences.vntu.edu.ua/index.php/pmovc/pmovc22/paper/view/16291