КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.26.707
УДК 004.94:519.21

Шевченко Світлана Миколаївна
к.п.н., доцент, доцент кафедри інформаційної та
кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0002-9736-8623
s.shevchenko@kubg.edu.ua

Жданова Юлія Дмитрівна
к.ф.-м.н доцент, доцент кафедри інформаційної та
кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0002-9277-4972
y.zhdanova@kubg.edu.ua

Складанний Павло Миколайович
к.т.н., доцент, доцент кафедри інформаційної та
кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Петренко Тарас Юрійович
студент Факультету інформаційних технологій та математики
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID ID: 0009-0000-9192-8629
typetrenko.fitm23m@kubg.edu.ua

НЕЧІТКІ КОГНІТИВНІ КАРТИ ЯК ІНСТРУМЕНТ ВІЗУАЛІЗАЦІЇ СЦЕНАРІЇВ РЕАГУВАННЯ НА ІНЦИДЕНТИ В СИСТЕМАХ БЕЗПЕКИ

Анотація. Кіберзагрози стають все більш складними та різноманітними. Існуючі методи аналізу та прийняття рішень не завжди дозволяють адекватно оцінити невизначеність та неоднозначність ситуації, реагуючи на кіберінциденти після їхнього настання. Ефективнішим є впровадження проактивних заходів кібербезпеки, що ґрунтуються на постійному аналізі та прогнозуванні потенційних загроз. Такий підхід дозволяє виявити слабкі місця в системі безпеки та вжити превентивних заходів, мінімізуючи ризик успішних кібератак. У даному дослідженні пропонується використовувати нечіткі когнітивні карти (НКК) як ефективний інструмент для візуалізації та аналізу сценаріїв реагування на інциденти. На основі аналізу наукових джерел висвітлені основні дефініції дослідження, зокрема, поняття когнітивного моделювання, нечіткої когнітивної карти, яка представлена у вигляді зваженого орієнтованого графа і когнітивної матриці, та етапи її створення. Сформульовані основні положення щодо сценарного підходу у кібербезпеці. Внаслідок проведеного SWOT-аналізу було ідентифіковано ключові концепти, включаючи ризики, атаки, засоби захисту, що формують основу системи. Оцінка зв'язків між концептами дозволила створити модель, яка відображає причинно-наслідкові взаємозв'язки між елементами системи безпеки мобільної мережі. Досліджено показники моделі: консонанс та дисонанс, які показали, що найбільшу загрозу для системи становлять APT (Advanced persistent threat), фішинг та програми-вимагачі, які мають найвищий рівень взаємозв'язків з іншими елементами системи, а DDoS-атаки, навпаки, мають найменший вплив у контексті побудованої моделі. За допомогою програмного засобу Mental Modeler були розроблені сценарії реагування на інциденти в системі безпеки мережі. Виділені недоліки когнітивного

моделювання та сценарного підходу. Їх обмеженість пов'язана з якістю експертних знань та складністю побудови моделей для великих систем. Перспективними напрямками подальших досліджень є розробка адаптивних моделей, здатних самонавчатися на нових даних за допомогою штучного інтелекту. Результати дослідження можуть бути використані в якості навчального матеріалу для студентів спеціальності 125 Кібербезпека та захист інформації.

Ключові слова: інформаційна безпека; нечіткі когнітивні карти; когнітивна матриця; концепти; моделювання сценаріїв; інциденти; загрози; прогнозування.

ВСТУП

Постановка проблеми. Система інформаційної безпеки — це складна взаємопов'язана мережа елементів, кожен з яких може мати свої особливості та уразливості. Через цю складність передбачити всі можливі сценарії атак та їхні наслідки є надзвичайно складним завданням. Саме тому моделювання різних ситуацій стає незамінним інструментом для аналізу потенційних загроз та розробки ефективних стратегій захисту.У цьому контексті надзвичайно важливо знайти такі рішення, які пропонують більш візуальний і інтуїтивно зрозумілий результат. Одним із таких підходів є когнітивне моделювання, яке є корисним інструментом для виявлення уразливих місць в системах безпеки та оцінювання ефективних заходів для їх усунення, надає відповідальним особам інструмент для аналізу різних сценаріїв та обґрунтованого прийняття рішень, а візуалізація цього процесу здійснюється за допомогою нечітких когнітивних карт.

Аналіз останніх досліджень і публікацій. Цифровізація суспільства сприяла розвитку теорії інформаційної безпеки. Забезпечення цілісності, доступності та конфіденційності інформації для кожної компанії стало пріоритетним завданням. Одним із підходів для вирішення питань із захистом інформації науковці та практики вбачають когнітивне моделювання, організацію когнітивних ігор, створення когнітивних карт та матриць і на їх основі розробку сценаріїв [1] — [8].

У дослідженні [1] описано когнітивну модель, яка дозволяє дослідити вплив потенційних загроз на рівень захищеності об'єкта критичної інфраструктури, і проведено сценарне моделювання цього впливу.

Управління ризиками інформаційної безпеки за допомогою когнітивних карт пропонується у роботах [2], [3], де в орієнтованому графі множина вагів дуг (сила впливу) є число $w_i = r_i = p_i q_i$, $0 \le w_i \le 1$, де r_i — ступінь ризику, p_i — ймовірність реалізації кожної загрози; q_i — ймовірність відповідних збитків; дані значення розраховуються на основі експертного оцінювання та за допомогою SWOT-аналізу.

Створення симуляцій та експериментів на основі моделей когнітивних процесів дає можливість досліджувати різні сценарії кібератак та оцінювати ефективність різних стратегій захисту, що сприяє підвищенню рівня безпеки інформаційних систем. Так вважають автори проєкту «Освоєння кіберпотужності: когнітивні науки та людський фактор у цивільній та військовій кібербезпеці», які представили дев'ять теоретичних та практичних досліджень з цієї проблеми [4], [5].

Для створення ефективної моделі захисту інформації, на думку науковців [6], є розвинуті когнітивні навички інженерів безпеки. Когнітивна безпека враховує чотири компоненти: процеси, знання, технології та когнітивні здібності для створення

ментальних карт, комплексного об'єднання даних, обробки масивних даних і підтримки знань. Щоб керувати операціями безпеки, потрібно зосередитися на чотирьох макропроцесах: обізнаність про ситуацію з кібербезпекою, атаки та загрози кібербезпеки, реагування на інциденти кібербезпеки та навички аналітиків безпеки [6].

Нетривіальність та комплексність досліджуваної проблеми є вагомим аргументом на користь подальших досліджень у сфері застосування когнітивного моделювання в нових контекстах кібербезпеки.

Метою статті є розширення можливостей застосування нечітких когнітивних карт з подальшою розробкою сценаріїв реагування на інциденти в системах безпеки.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Когнітивне моделювання: нечітка когнітивна карта та етапи виконання

«Когнітивний підхід полягає у прагненні зрозуміти, яким чином людина розшифровує інформацію про дійсність і організовує її, щоб приймати рішення або вирішувати насущні завдання» [9]. Когнітивне моделювання базується на побудові нечіткої когнітивної карти, тобто орієнтованого графа, вершини (концепти) якого представляють системні змінні, а зважені дуги відображають силу впливу одного концепта на інший [10]. Нечіткі когнітивні карти використовують концепції когнітивного картографування та нечіткої логіки для моделювання складних систем. Вони дозволяють аналізувати системи, де взаємозв'язки між елементами можуть бути нечіткими, динамічними та змінюватися в часі. Як відомо, нечітка когнітивна карта Kosko — це зважений орієнтований граф, де на дугах відмічають їх вагу: значення в межах [–1; 1], визначаючи таким чином рівень впливу одного фактора на інший, які називаються концептами. За допомогою когнітивної карти проводять статичний та динамічний аналіз (табл. 1).

Таблиця 1

Можливості використання когнітивної карти

У статиці	У динаміці
1. Оцінка впливу одних факторів на інші. 2. Стійкість ситуації загалом. 3. Пошук структурних змін для отримання стійких структур.	1. Генерація сценаріїв розвитку ситуації у часі. 2. Аналіз сценаріїв розвитку ситуації у часі. 3. Наслідки впливу на елементи системи або зміни характеру зв'язку.

У науковій літературі пропонуються різні етапи, схеми, механізми моделювання проблемної ситуації на основі когнітивного підходу. Нам імпонує процес побудови, запропонований у дослідженні [11] і представлений на рис. 1.

ISSN 2663 - 4023

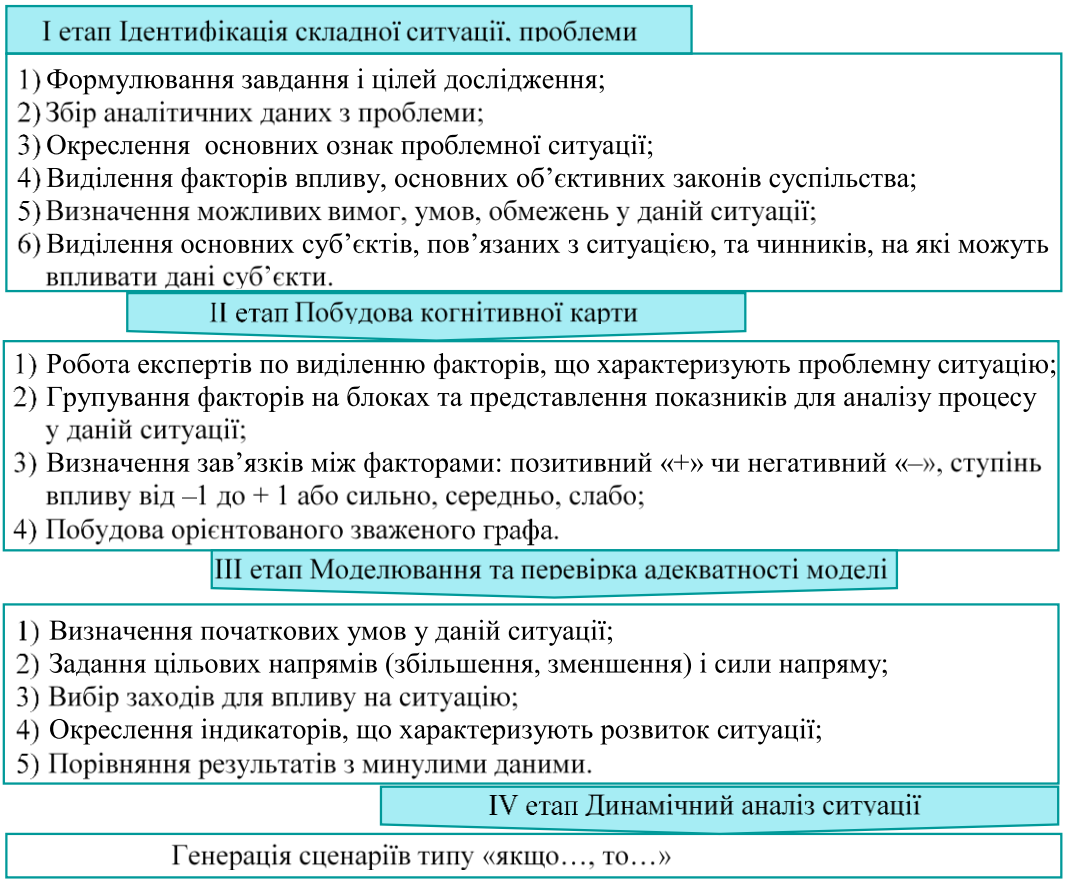

Рис. 1. Етапи моделювання на основі когнітивного підходу

Сценарний підхід у кібербезпеці

Сценарний підхід у кібербезпеці дозволяє моделювати різноманітні ситуації, починаючи від простих до надзвичайно складних. Він допомагає візуалізувати загрози; ідентифікувати уразливості; розробити ефективні заходи захисту; провести навчання персоналу; оцінити готовність до інцидентів; прогнозувати наслідки.

Сценарне планування — це дисциплінований метод уявлення можливого майбутнього, який компанії застосовують до широкого кола питань. Кожен сценарій розповідає про те, як різні елементи можуть взаємодіяти за певних умов. Коли зв'язки між елементами можна формалізувати, компанія може розробити кількісні моделі. Хоча межі сценарію іноді можуть бути нечіткими, детальний і реалістичний наратив може спрямувати увагу на аспекти, які раніше не помітили [12]. Сценарії дослідження припускають комплексну оцінку взаємодії різних факторів невизначеності, які розглядаються як рівноправні компоненти системи.

Серед переваг сценарного підходу виділяють:

– гнучкість — сценарії можна адаптувати до будь-якої частини інформаційної безпеки;
– ефективність — дозволяє швидко ідентифікувати потенційні загрози, а отже і заходи протидії;
– візуалізація — сценарії можна представити у вигляді діаграм, що дозволяє передачу абстрактної інформації побачити в інтуїтивно зрозумілій формі.

Хоча сценарний підхід є одним із найпоширеніших інструментів у кібербезпеці, він має свої обмеження:

- суб'єктивність — сценарії зазвичай створюються експертами, тому різні експерти можуть розробити різні сценарії для однієї й тієї ж ситуації;
- складність прогнозування — витікає із суб'єктивності;
- матеріальні та нематеріальні витрати — розробка та аналіз сценаріїв можуть бути трудомісткими процесами, особливо для великих та складних систем.

Для того, щоб мінімізувати ці недоліки, рекомендується комбінувати сценарний підхід з іншими методами.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

У даному досліджені, у якості зразка, розглянемо побудову нечіткої когнітивної карти і на її основі розробку сценаріїв реагування на інциденти в системі безпеки мобільної мережі. Оскільки на сучасному етапі здатність громадян залишатися на зв'язку є життєво важливою, особливо під час евакуації, пошуку допомоги або повідомлення про загрози. Крім того, мобільний зв'язок є ключовим інструментом для екстрених служб, які координують рятувальні операції, а також для військових, які захищають країну. У цьому контексті особливу увагу слід приділяти захисту інфраструктури мобільних операторів від кіберзагроз. Атаки на мережеве обладнання, кібератаки на системи зв'язку або вихід з ладу ключових вузлів можуть призвести до масштабних перебоїв, що значно ускладнить ситуацію для цивільного населення.

Опис структури нечіткої когнітивної карти

Позначимо через $\bar{G} = \{C, \bar{E}, W\}$ орієнтований граф, де $C = \{C_i\}$ — множина факторів (концептів), $\bar{E} = \{e_i\}$ — множина дуг, що відображають причинно-наслідкові зв'язки між факторами; $W = \{w_i\}$ — множина вагів дуг (сила впливу).

Для визначення множини факторів (концептів) та множини дуг (сили впливу) було здійснено SWOT-аналіз та експертне оцінювання. Найвагоміші, з точки зору вивчення даної проблеми, загрози мобільної мережі склали множину концептів:

C_1 — Програми-вимагачі (Ransomware),
C_2 — Компрометація ділової електронної пошти (Business Email Compromise),
C_3 — DDoS,
C_4 — Крадіжка даних (Data Theft),
C_5 — Фішинг (Phishing),
C_6 — APT (Advanced persistent threat),
C_7 — Інші атаки (Other attacks),
C_8 — Антивірус (Antivirus),
C_9 — Брандмауер (Firewall),
C_{10} — Інформування про безпеку (Security awareness),
C_{11} — Мережева безпека та стабільність (Network Security and Stability).

Мережева безпека сама по собі не впливає на інші концепти в моделі, оскільки вона є фундаментальною властивістю безпеки, які є результатом взаємодії інших елементів системи. Проте на неї суттєво впливають інші елементи. Зокрема, такі атаки, як DDoS, фішинг, компрометація ділової електронної пошти або програми-вимагачі негативно впливають на цей концепт, знижуючи загальний рівень безпеки та стійкості мережі.

У той же час, засоби захисту, такі як антивірусне програмне забезпечення, брандмауери і заходи з підвищення обізнаності про безпеку, позитивно впливають на безпеку і стабільність мережі, допомагаючи нейтралізувати загрози, зменшити їх вплив і підтримувати відмовостійкість системи. Таким чином, ця концепція є інтегративним показником, який відображає загальний стан мережевої безпеки з урахуванням впливу атак і захисних заходів.

Для оцінки сили впливу між кожною парою концептів використано нечітку лінгвістичну шкалу: {Не впливає; Дуже слабка; Слабка; Помірна; Сильна; Дуже сильна}. Кожному значенню нечіткої лінгвістичної шкали буде відповідати певний числовий діапазон, який визначає силу впливу концептів у моделі. Для додатних зв'язків використовуватиметься відрізок **[0, 1]**, а для від'ємних зв'язків — відрізок **[–1, 0]**. Такий підхід дозволяє кількісно відобразити різний ступінь впливу концептів залежно від їхнього характеру (табл. 2).

Таблиця 2

Відповідність лінгвістичних значень числовим діапазонам

Лінгвістичне значення	Числовий діапазон (додатні зв'язки)	Числовий діапазон (від'ємні зв'язки)
Не впливає	0	0
Дуже слабка	(0, 0.2]	[–0.2, 0)
Слабка	(0.2, 0.4]	[–0.4, –0.2)
Помірна	(0.4, 0.6]	[–0.6, –0.4)
Сильна	(0.6, 0.8]	[–0.8, –0.6)
Дуже сильна	(0.8, 1]	[–1, –0.8)

На основі представлених вище даних формуємо когнітивну матрицю (рис. 2) та нечітку когнітивну карту (рис. 3). Для цього використаємо програмне забезпечення Mental Modeler [13].

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11
C1				0.6							-0.46
C2							0.19				
C3											-0.08
C4					0.7						-0.07
C5		0.7		0.7							
C6	0.8			0.6							-0.8
C7											-0.1
C8	-0.7					-0.7					0.5
C9			-0.6								0.5
C10					-0.6						0.5
C11											

Рис. 2. Когнітивна матриця взаємовпливів концептів

ISSN 2663 - 4023

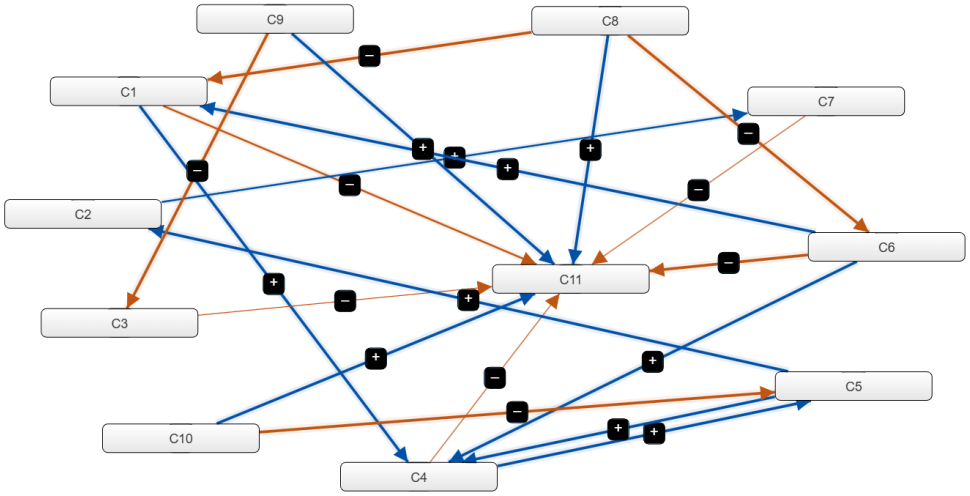

Рис. 3. Нечітка когнітивна карта дослідження стану мережевої безпеки

Щільність зв'язків для нечіткої когнітивної карти (НКК) визначається за формулою:

$$d = \frac{m}{n(n-1)},$$

де: d — щільність зв'язків, m — загальна кількість зв'язків між концептами, n — загальна кількість концептів у моделі.

Ця формула дозволяє оцінити відносну складність НКК, показуючи, яку частину від максимально можливої кількості зв'язків займають фактичні зв'язки між концептами.

Щільність може варіюватися від 0 (відсутність зв'язків) до 1 (максимальна кількість зв'язків, коли кожен концепт пов'язаний із кожним іншим). Це значення є ключовим показником для аналізу складності та взаємозв'язків у моделі.

У створеному випадку маємо 19 зв'язків, 11 концептів. Таким чином, щільність зв'язків створеної когнітивної карти:

$$d = \frac{19}{11(11-1)} = 0{,}1727\ .$$

Маємо оптимальну щільність зв'язків.

Структура НКК передбачає різні типи концептів залежно від характеру їхньої взаємодії (рис. 4).

Total Components	11
Total Connections	19
Density	0.1727272727
Connections per Component	1.7272727273
Number of Driver Components	3
Number of Receiver Components	1
Number of Ordinary Components	7
Complexity Score	0.3333333333

Component	Indegree	Outdegree	Centrality	Preferred State	Type
C1	1.5	1.06	2.56		ordinary
C2	0.7	0.19	0.8899999999999999		ordinary
C3	0.6	0.08	0.6799999999999999		ordinary
C4	1.9	0.77	2.67		ordinary
C5	1.2999999999999998	1.4	2.6999999999999997		ordinary
C6	0.7	2.2	2.9000000000000004		ordinary
C7	0.19	0.1	0.29000000000000004		ordinary
C8	0	1.9	1.9		driver
C9	0	1.1	1.1		driver
C10	0	1.1	1.1		driver
C11	3.0100000000000002	0	3.0100000000000002		receiver

Рис. 4. Основні показники нечіткої когнітивної карти

Маємо три концепти типу «Driver». Ці концепти впливають на інші елементи системи, але самі залишаються незалежними, тобто на них не впливає жоден інший концепт. Вони є ключовими рушіями змін у системі, формуючи вихідну точку для аналізу причинно-наслідкових зв'язків. Концептами типу «Driver» є засоби захисту.

У НКК є один концепт типу «Receiver». Концептом типу «Receiver» є захищеність системи. Це кінцевий концепт, який перебуває під впливом інших елементів системи, але сам не впливає на жоден із них. Він відображає інтегрований результат дії всіх інших концептів у системі.

Інші сім — концепти типу «Ordinary». Це проміжні концепти, які є як джерелами впливу на інші елементи системи, так і об'єктами впливу з боку інших концептів. Вони виступають посередниками, що забезпечують передачу впливу в межах системи. Концептами типу «Ordinary» є атаки. Вони взаємодіють із засобами захисту, перебуваючи під їхнім впливом, і водночас впливають на кінцевий концепт «Захищеність системи». Ці концепти відіграють роль посередників у динаміці системи, відображаючи взаємодію між ризиками та заходами безпеки.

Такий розподіл концептів дозволяє чітко визначити їхню функцію в моделі та краще зрозуміти динаміку системи. НКК надає можливість аналізувати як вплив окремих концептів, так і їхній внесок у загальну картину захищеності мережі, забезпечуючи системний підхід до моделювання.

Моделювання сценаріїв

Сценарій 1. Розглянемо, як зміниться стан інформаційної системи, якщо збільшимо вплив найвпливовішої загрози C_6 (APT-Advanced persistent threat) на 0,82. Із гістограми (рис. 5) випливає, що інші загрози: програми-вимагачі (Ransomware), крадіжка даних (Data Theft), фішинг (Phishing) збільшили свій вплив відповідно на 0,08; 0,06 та 0,01, а стан мережевої безпеки погіршиться на 0,09.

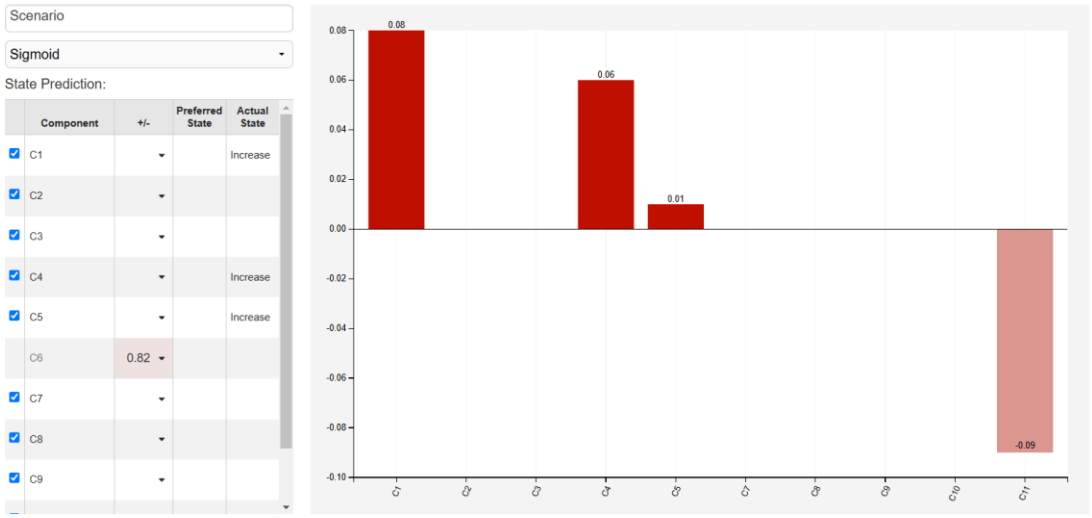

Рис. 5. Результати сценарію 1

Загроза APT (Розширена постійна загроза) — противник зі складним рівнем досвіду та значними ресурсами, що дозволяє йому за допомогою багатьох різних векторів атак (наприклад, кібер-, фізичних та обманних) створювати можливості для досягнення своїх цілей, які зазвичай полягають у встановленні та розширенні своєї присутності в межах інфраструктура інформаційних технологій організацій з метою

постійного викрадання інформації та/або для підриву чи перешкоджання критичним аспектам місії, програми чи організації, або для надання можливості робити це в майбутньому [14]. Як свідчать практики, єдиний спосіб протистояти ризикам, пов'язаних з APT, — це створити багаторівневий захист:

– навчання персоналу з питань інформаційної безпеки;
– традиційні механізми захисту (антивіруси та брандмауери);
– розширене виявлення шкідливих програм;
– виявлення аномалій подій.

У дослідженні [15] для забезпечення захисту інформації від загрози APT пропонують розроблене програмне забезпечення Decepticon (протидія на основі обману), структурою якого є модель Маркова, де індикатори компромісу (IoC) використовуються як спостережувані ознаки для допомоги у виявленні.

Сценарій 2. На рисунку 6 представлено результат сценарію, у якому збільшуємо вплив на систему двох загроз одночасно: компрометація ділової електронної пошти (Business Email Compromise) та APT (Advanced persistent threat) на 0,45. У такому випадку мінімізується стан мережевої безпеки 0,01, проте активізуються програми-вимагачі (Ransomware) та DDoS-атаки (на 0,01 відповідно кожна).

Компрометація бізнес-електронної пошти (BEC) — це різновид кіберзлочинності, коли шахрай використовує електронну пошту, щоб оманою змусити когось надіслати гроші або розкрити конфіденційну інформацію про компанію. Зловмисник видає себе за довірену особу, а потім просить сплатити фальшивий рахунок або конфіденційні дані, які вони можуть використати в іншому шахрайстві [16].

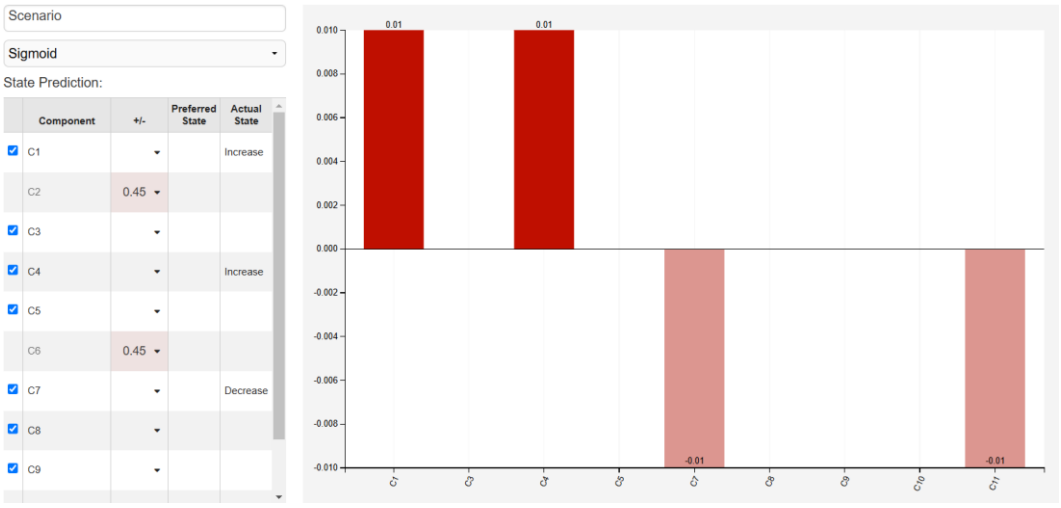

Рис. 6. Результати сценарію 2

Щоб запобігти вище названим інцидентам пропонується:

1) виконати поради для сценарію 1, оскільки збільшується у цій ситуації вплив і загрози APT;
2) використати безпечне рішення електронної пошти, наприклад, Microsoft Defender For Office 365 P1/P2 (типи ліцензій); налаштувати багатофакторну автентифікацію (MFA); застосувати засоби автентифікації електронної пошти, наприклад, Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) і Domain-based Message Authentication, Reporting, and Conformance (DMARC).

Сценарій 3. Спробуємо уявити, що захист інформаційної системи, а саме антивірус (Antivirus) та брандмауер (Firewall) максимально послабили (рис. 7).

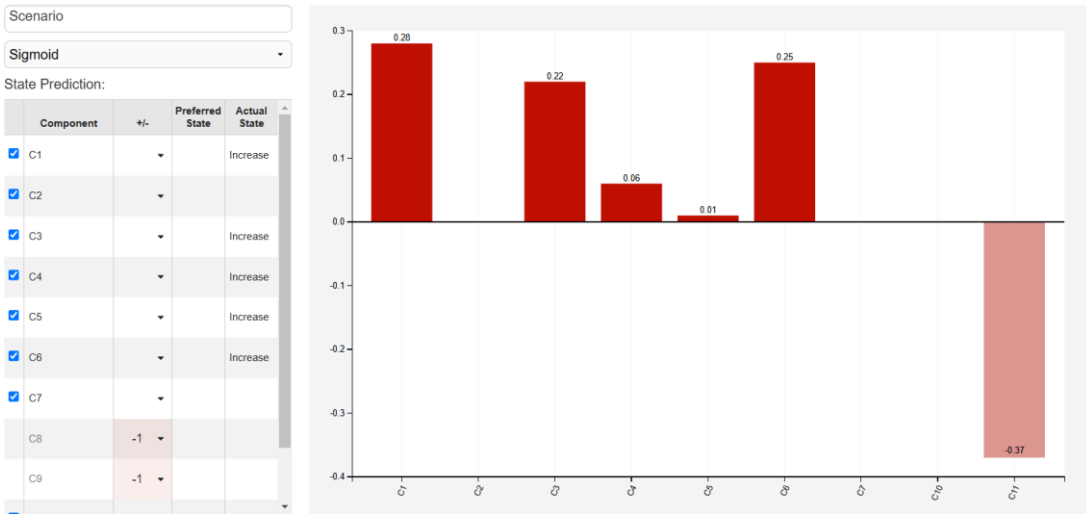

Рис. 7. Результати сценарію 3

Внаслідок взаємодії загроз: програм-вимагачів (Ransomware), DDoS-атак, крадіжки даних (Data Theft), фішингу (Phishing) та APT, які зросли на 0,28; 0,22; 0,06; 0,01; 0,25 відповідно, загальний стан інформаційної системи, а саме, мережева безпека та стабільність погіршилися майже у три рази (0,37). Реалізований сценарій наочно продемонстрував критичну роль антивірусних програм та брандмауерів у забезпеченні інформаційної безпеки, підтвердивши їх ефективність у виявленні та нейтралізації кіберзагроз.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Когнітивне моделювання є одним із перспективних напрямів у системах безпеки. За допомогою когнітивного підходу є можливість створити детальну модель системи безпеки, яка показує, як всі її елементи пов’язані між собою, як вони впливають один на одного та які наслідки можуть виникнути в результаті різних подій. Ця модель допомагає передбачити, а отже розробити ефективні стратегії для запобігання кіберзагрозам та вирішення проблем, які можуть виникнути. Когнітивна модель — це інтелектуальний помічник експерта, який допомагає йому орієнтуватися в складному інформаційному просторі, будувати причинно-наслідкові зв’язки та приймати оптимальні рішення в умовах обмеженого часу та ресурсів.

Проте виділення концептів та визначення сили впливу між ними можуть бути чутливими до якості експертних знань, що може призвести до невірних результатів. Також треба відзначити, що для великих моделей потрібні значні обчислювальні ресурси для обробки даних. Тому перспективними напрямками подальших досліджень є розробка адаптивних моделей, здатних самонавчатися на нових даних, а також інтеграція нечітких когнітивних карт з іншими методами штучного інтелекту [17].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Salieva, O. V., & Yaremchuk,, Y. E. (202.) Cognitive model for studying the level of security of a critical infrastructure facility. *Information Security, 26(2),* 64–73.
2. Shevchenko, S., Zhdanova, Y., Shevchenko, H., Nehodenko, O., & Spasiteleva, S. (2023). Information Security Risk Management using Cognitive Modeling. In: *Cybersecurity Providing in Information and Telecommunication Systems, Vol. 3550,* 297–305.
3. Shevchenko, S., Zhdanova, Y., Kryvytska, O., Shevchenko, H., & Spasiteleva, S. (2024). Fuzzy cognitive mapping as a scenario approach for information security risk analysis. In: *Cybersecurity Providing in Information and Telecommunication Systems II, Vol. 3826*, 356–362.
4. Veksler, V. D., Buchler, N., Hoffman, B. E., Cassenti, D. N., Sample, C., & Sugrim, S. (2018). Simulations in Cyber-Security: A Review of Cognitive Modeling of Network Attackers, Defenders, and Users. *Frontiers in Psychology, 9.* https://doi.org/10.3389/fpsyg.2018.00691
5. Veksler, V. D., Buchler, N., LaFleur, C. G., Yu Michael, S., Lebiere, C., & Gonzalez, C. (2020). Cognitive Models in Cybersecurity: Learning From Expert Analysts and Predicting Attacker Behavior. *Frontiers in Psychology, 11*.
6. Andrade, R. O., & Yoo, S. G. (2019). Cognitive security: A comprehensive study of cognitive science in cybersecurity. *Journal of Information Security and Applications, 48.* https://doi.org/10.1016/j.jisa.2019.06.008
7. Krichene, J., & Boudriga. N. (2008). Incident response probabilistic cognitive maps. *IEEE international symposium on parallel and distributed processing with applications*, 689–94. doi:10.1109/ISPA.2008.33
8. Andrade, R., Torres, J., & Flores, P. (2018). Management of information security indicators under a cognitive security model. *IEEE 8th annual computing and communication workshop and conference (CCWC),* 478–83. doi:10.1109/CCWC.2018.8301745
9. Shapar, V. B. (2007). *Modern explanatory psychological dictionary.* Kharkiv.: Prapor.
10. Kosko, B. (1986). Fuzzy Cognitive Maps. *International Journal of Man-Machine Studies, 24*, 65–75.
11. Miliavskyi, Y. L.(2021). Identification and control of complex systems based on cognitive maps impulse processes models. *Thesis for doctoral degree National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute»*.
12. Schoemaker, P. J. H. (1995). *Planning: A Tool for Strategic Thinking*. Reprint #3622.
13. *MentalModeler.* (n. d.). https://dev.mentalmodeler.com/
14. *Glossary. NIST SP 800-30 Rev. 1.* (n. d.). https://csrc.nist.gov/glossary/term/apt
15. Baksi, R. & Upadhyaya, S. (2021). Decepticon: a Theoretical Framework to Counter Advanced Persistent Threats. *Information Systems Frontiers, 23,* 1–17. https://doi.org/10.1007/s10796-020-10087-4
16. *Microsoft Security.* (n. d.). https://www.microsoft.com/en-us/security/business/security-101/what-is-business-email-compromise-bec
17. Apostolopoulos, I. D., & Groumpos, P. P. (2023). Fuzzy Cognitive Maps: Their Role in Explainable Artificial Intelligence. *Applied Sciences, 13(6),* 3412. https://doi.org/10.3390/app13063412
18. 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.

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

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

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

Pavlo Skladannyi
PhD, Associate Professor,
Head of the Department of Information and Cybersecurity
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Taras Petrenko
Student of the Faculty of Information Technologies and Mathematics
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID ID: 0009-0000-9192-8629
typetrenko.fitm23m@kubg.edu.ua

FUZZY COGNITIVE MAPS AS A TOOL FOR VISUALIZING INCIDENT RESPONSE SCENARIOS IN SECURITY SYSTEMS

Abstract. Cyber threats are becoming increasingly complex and diverse. Existing methods of analysis and decision-making do not always allow us to adequately assess the uncertainty and ambiguity of the situation, responding to cyber incidents after they occur. It is more effective to implement proactive cybersecurity measures based on constant analysis and forecasting of potential threats. This approach allows us to identify weaknesses in the security system and take preventive measures, minimizing the risk of successful cyber attacks. This study proposes the use of fuzzy cognitive maps (FCMs) as an effective tool for visualization and analysis of incident response scenarios. Based on the analysis of scientific sources, the main definitions of the study are highlighted, in particular, the concepts of cognitive modeling, a fuzzy cognitive map, which is presented in the form of a weighted directed graph and a cognitive matrix, and the stages of its creation. The main provisions regarding the scenario approach in cybersecurity are formulated. As a result of the SWOT analysis, key concepts were identified, including risks, attacks, and defenses that form the basis of the system. The assessment of the relationships between concepts allowed us to create a model that reflects the cause-and-effect relationships between the elements of the mobile network security system. The model indicators were studied: consonance and dissonance, which showed that the greatest threat to the system is posed by APT (Advanced persistent threat), phishing, and ransomware, which have the highest level of relationships with other elements of the system, and DDoS attacks, on the contrary, have the least impact in the context of the constructed model. Scenarios for responding to incidents in the network security system were developed using the Mental Modeler software tool. Disadvantages of cognitive modeling and the scenario approach are identified. Their limitations are associated with the quality of expert knowledge and the complexity of building models for large systems. Promising areas of further research are the development of adaptive models capable of self-learning on new data using artificial intelligence. The results of the study can be used as educational material for students of specialty 125 Cybersecurity and Information Protection.

Keywords: Information security; fuzzy cognitive maps; cognitive matrix; concepts; scenario modeling; incidents; threats; forecasting.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Salieva, O. V., & Yaremchuk,, Y. E. (202.) Cognitive model for studying the level of security of a critical infrastructure facility. *Information Security, 26(2)*, 64–73.
2. Shevchenko, S., Zhdanova, Y., Shevchenko, H., Nehodenko, O., & Spasiteleva, S. (2023). Information Security Risk Management using Cognitive Modeling. In: *Cybersecurity Providing in Information and Telecommunication Systems, Vol. 3550*, 297–305.
3. Shevchenko, S., Zhdanova, Y., Kryvytska, O., Shevchenko, H., & Spasiteleva, S. (2024). Fuzzy cognitive mapping as a scenario approach for information security risk analysis. In: *Cybersecurity Providing in Information and Telecommunication Systems II, Vol. 3826*, 356–362.
4. Veksler, V. D., Buchler, N., Hoffman, B. E., Cassenti, D. N., Sample, C., & Sugrim, S. (2018). Simulations in Cyber-Security: A Review of Cognitive Modeling of Network Attackers, Defenders, and Users. *Frontiers in Psychology, 9*. https://doi.org/10.3389/fpsyg.2018.00691
5. Veksler, V. D., Buchler, N., LaFleur, C. G., Yu Michael, S., Lebiere, C., & Gonzalez, C. (2020). Cognitive Models in Cybersecurity: Learning From Expert Analysts and Predicting Attacker Behavior. *Frontiers in Psychology, 11*.
6. Andrade, R. O., & Yoo, S. G. (2019). Cognitive security: A comprehensive study of cognitive science in cybersecurity. *Journal of Information Security and Applications, 48.* https://doi.org/10.1016/j.jisa.2019.06.008
7. Krichene, J., & Boudriga. N. (2008). Incident response probabilistic cognitive maps. *IEEE international symposium on parallel and distributed processing with applications*, 689–94. doi:10.1109/ISPA.2008.33
8. Andrade, R., Torres, J., & Flores, P. (2018). Management of information security indicators under a cognitive security model. *IEEE 8th annual computing and communication workshop and conference (CCWC),* 478–83. doi:10.1109/CCWC.2018.8301745
9. Shapar, V. B. (2007). *Modern explanatory psychological dictionary.* Kharkiv.: Prapor.
10. Kosko, B. (1986). Fuzzy Cognitive Maps. *International Journal of Man-Machine Studies, 24*, 65–75.
11. Miliavskyi, Y. L.(2021). Identification and control of complex systems based on cognitive maps impulse processes models. *Thesis for doctoral degree National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute»*.
12. Schoemaker, P. J. H. (1995). *Planning: A Tool for Strategic Thinking*. Reprint #3622.
13. *MentalModeler.* (n. d.). https://dev.mentalmodeler.com/
14. *Glossary. NIST SP 800-30 Rev. 1.* (n. d.). https://csrc.nist.gov/glossary/term/apt
15. Baksi, R. & Upadhyaya, S. (2021). Decepticon: a Theoretical Framework to Counter Advanced Persistent Threats. *Information Systems Frontiers, 23,* 1–17. https://doi.org/10.1007/s10796-020-10087-4
16. *Microsoft Security.* (n. d.). https://www.microsoft.com/en-us/security/business/security-101/what-is-business-email-compromise-bec
17. Apostolopoulos, I. D., & Groumpos, P. P. (2023). Fuzzy Cognitive Maps: Their Role in Explainable Artificial Intelligence. *Applied Sciences, 13(6),* 3412. https://doi.org/10.3390/app13063412
18. 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.