SECTION 7. CYBERSECURITY AND INFORMATION PROTECTION

DOI: 10.46299/ISG.2025.MONO.TECH.3.7.1

7.1 Когнітивне моделювання сценаріїв для прогнозування кіберризиків

Сучасний ландшафт кібербезпеки характеризується зростанням інтенсивності та глобальним розширенням кіберзагроз. Цифрова трансформація, зокрема, розгортання фізичних пристроїв Інтернет речей, хмарні рішення, віддалена робота, значно розширила периметр атаки. Складні фінансовані деякими державами хакер-групи, інноваційне застосування штучного інтелекту для прискорення злочинної діяльності та часті важковиявлені експлойти «нульового дня» ускладнюють протистояння, підривають ефективність традиційних механізмів захисту інформаційної системи. При цьому, слід зауважити, крім технологічних проблем у сфері кібербезпеки, залишається найбільш експлуатованим вектором компрометації людський фактор (соціальна інженерія, недостатня кібергігієна, інсайдерська діяльність). Середні світові витрати на витік даних перевищили 4,88 мільйонів доларів США у 2024 році, цей показник збільшиться до 23 трильйонів доларів США у 2027 році [143]. Крім фінансових збитків, компанії несуть репутаційні, втрачаючи довіру клієнтів. Для подолання цих викликів усім установам та урядам критично важливо перейти від простого реагування на інциденти до проактивної стратегії з метою прогнозування та завчасної побудови захисту для забезпечення конфіденційності, цілісності та доступності інформації.

За результатами Міжнародного аналітичного дослідження довіри до цифрових технологій 2025 [144] для бізнесу кібербезпека є пріоритетним завданням, однак лише 2% організацій впровадили заходи забезпечення кіберстійкості на усіх рівнях. Існують проблеми з кількісною оцінкою кіберризиків: надійність і достовірність результатів такої оцінки непокоїть 47% опитаних респондентів, а невизначеність оцінки – 39% [144].

Вище перераховані методологічні та емпіричні обмеження, недостатня гнучкість традиційних підходів вимагає удосконалення системи управління кіберризиками на основі впровадження математичних методів для якісного та кількісного підходу в оцінці цих ризиків з метою виявлення можливих інцидентів до їх прояву.

7.1.1 Понятійний апарат дослідження

7.1.1.1 Кіберризик

Аналіз наукових джерел дозволив визначити, що системний розгляд даної дефініції є актуальним та важливим в контексті управління ризиками та забезпечення кібербезпеки на всіх рівнях [145-151].

Вважають, що кіберризик – ризик, який виникає внаслідок використання інформаційно-комунікаційних технологій та загрожує конфіденційності, доступності та цілісності даних чи послуг [145].

У дослідженні [146] автором було проаналізовано 200 статей (з 2000 до 2028 року) з метою сформувати онтологічну метамодель концепції кіберризику. Як з'ясувалося лише 20 з них мають оригінальне визначення даного поняття, інші – опосередковано застосовують. На думку науковця, дане поняття включає знання двох областей: реальна сфера, яка містить організацію та її активи, та абстрактна сфера, яка охоплює такі поняття, як ризик, уразливість, ймовірність, загроза. Запропоноване дослідником визначення кіберризику висвітлює найважливіші його особливості:

- кіберризик знаходиться в області операційних ризиків;
- об'єкти, які зазначають втрат, спричинених кіберризиками, – це інформаційні активи, ресурси ІКТ, технологічні активи;
- кіберризик може виникати як в окремому комп'ютерному пристрої, так і у взаємопов'язаних ІТ-системах;
- потенційний вплив кіберризиків є триєдиним і охоплює: пошкодження активів (включаючи зобов'язання перед третіми особами та втрату прибутку), порушення операційної діяльності, шкода репутації.

Пізніше, застосовуючи дану методологію, науковці [147] підтвердили, що запропоноване автором визначення кіберризику залишається актуальним. При цьому автори проаналізували 474 праці з 2019 до 2021 року.

Слід відзначити дослідження [148], результати якого були визначені на основі 13805 публікацій, у яких одним з ключових слів є кіберризик, з 2004 до 2024 року. Їх визначення кіберризику відповідає попереднім твердженням: кіберризик поєднує ймовірність несприятливих подій та їхні наслідки з урахуванням організаційних цілей і невизначеностей, у кіберпросторі виникає внаслідок навмисних чи ненавмисних кіберзагроз, виходячи за рамки технічних недоліків і охоплюючи ширші суспільні, економічні та психологічні виміри.

Автори дослідження [149] пропонують поняття «ризик інформаційної безпеки» – це числова (словесна) функція, яка описує ймовірність втілення загроз інформаційної безпеки (ІБ) та величини збитку від їх реалізації внаслідок використання цими загрозами уразливостей активів з метою нанесення шкоди організації. Поняття «ризик ІБ» є комбінованим, який поєднує в собі інші ключові поняття: активи, уразливості, загрози, збиток.

Ми згодні з автором [150], що кіберризик слід розглядати як правову категорію. Проте в законодавстві України відсутнє визначення даного поняття. Зустрічається лише в Постановах Національного банку України. Так, в інструкції від 05.04.2024 №38 стверджується, що «кіберризик – це ризик реалізації кіберзагроз щодо інформаційних ресурсів та/або інформаційної інфраструктури, а також наслідків таких подій» [151].

Вважаємо наступне визначення, представлене у дослідженні [150], вичерпно характеризує всі особливості поняття «кіберризик» та охоплює усі дотичні сфери, надаючи комплексне та цілісне розуміння цього явища. «Кіберризик – існуюча ймовірність настання негативних наслідків для суб’єктів кібербезпеки, національної безпеки, суспільства та держави, що виникає внаслідок наявності потенційних кіберзагроз та/або уразливостей в інформаційних, комунікаційних та інформаційно-комунікаційних системах, а також недоліків у їх захисті, що можуть призвести до порушення

конфіденційності, цілісності, доступності інформаційних ресурсів, порушення сталого та надійного функціонування зазначених систем, завдання шкоди законним інтересам фізичних та юридичних осіб, майну, критичній інфраструктурі» [150].

Таким чином, кіберризик може мати природне походження або, частіше, техногенне, яке включає людський фактор, кіберзлочинність, кібервійну та кібертероризм. Його унікальність як ризикової категорії полягає у високому ступені взаємозалежності систем; існуванні потенційних подій з екстремальними наслідками; методологічними невизначеностями, пов’язаними з доступністю та якістю даних, які необхідні для моделювання; адекватністю самих підходів до моделювання; постійною динамікою технологічного ландшафту [145].

7.1.1.2 Сценарний підхід в кібербезпеці

Проактивна стратегія організацій у сфері кіберзахисту передбачає перехід від реагування на інциденти до їх прогнозування. Сценарний підхід є тієї методологією, яка базується на розробці та аналізу ймовірних, але відмінних один від одного, деталізованих варіантів розвитку подій (сценаріїв) у майбутньому. Він допомагає візуалізувати загрози; ідентифікувати уразливості; розробити ефективні заходи захисту; провести навчання персоналу; оцінити готовність до інцидентів; прогнозувати наслідки [152].

Кіберсценарій – це структурований наратив, який досліджує потенційне майбутнє, поєднуючи різні фактори кіберризику, такі як уразливості, суб'єкти та об’єкти загроз та вплив на бізнес. Сценарії не є прогнозами, це правдоподібні наративи про можливі події, які використовуються організаціями для концептуалізації загроз, підготовки до різноманітних результатів та пошуку відповідей на питання: «Що, якщо?» [153].

У дослідженні [154] автори запропонували автоматизовану структуру для симуляцій кіберінцидентів та детального профілювання атак, розширюючи прогнозування через інтеграцію структурованих/неструктурованих журналів, і пропонуючи нову методологію інтеграції застарілих систем із сучасними

платформами розвідки загроз для оптимізації проактивного управління безпекою.

Практичні навчання вимагають чітких сценаріїв атак та відповідних стратегій захисту. Так вважають дослідники [155] і пропонують свої розробки в середовищі системи промислового управління.

Науковці у роботі [156] пропонують структуровану операційну основу для навчання кібербезпеці космічних систем, створюючи реалістичні, технічно відтворювані сценарії атак (включаючи компрометацію наземного сегмента, DDoS-атаки та захоплення прошивки), що дозволяє оцінювати стратегії виявлення і реагування з урахуванням обмежень супутникового зв'язку.

Аналіз сценаріїв може допомогти установам зрозуміти потенційні ризики, як вони можуть передаватися, куди потрібно робити інвестиції та як найкраще реагувати на порушення системи [157]. Відправною точкою для створення сценаріїв є ретельна оцінка ризиків за допомогою експертної оцінки. Зазвичай будується декілька сценаріїв:

- оптимістичний – найкращий можливий сценарій;
- песимістичний – найгірший можливий сценарій;
- найбільш ймовірний (реалістичний) – сценарій, який має найбільші шанси на реалізацію.

Приклади застосування сценарного підходу можна побачити в роботах [152, 157].

Кіберризик можна визначити як функцію: $R = \{s_i, p_i, x_i\},\ i = 1,2, \dots n,$

де R – ризики; s_i – опис небажаного сценарію; p_i – ймовірність цього сценарію; x_i – міра наслідків або збитків, спричинених сценарієм, що стався; та n – кількість можливих сценаріїв, які можуть завдати шкоди системі [158].

Існує декілька типів сценарного підходу в кібербезпеці. Вони поділяються залежно від мети, об’єкта тестування, глибини симуляції (таблиця 1).

Таблиця 1. Типи сценарного підходу в кібербезпеці

Тип сценарію		Опис сценарію	Фокус
1. Тестування на проникнення (Penetration Testing)	Black-Box (Чорний ящик)	Attacker не має жодної попередньої інформації про систему. Сценарій імітує зовнішнього зловмисника.	Виявлення зовнішніх уразливостей, налаштувань мережі та вебзастосувань.
	White-Box (Білий ящик)	Attacker має повний доступ до вихідного коду, архітектури та конфігурацій. Сценарій імітує інсайдера або розробника.	Глибокий аудит коду та конфігурацій, пошук логічних помилок.
	Grey-Box (Сірий ящик)	Attacker має обмежену інформацію (наприклад, облікові дані користувача). Сценарій імітує внутрішнього користувача з низькими привілеями, що намагається підвищити їх.	Перевірка контролю доступу та сегментації мережі.
2. Командні навчання	Red Team (Червона команда)	Імітує дії реального зловмисника, використовуючи найновіші тактики, техніки та процедури (TTP).	Досягнення конкретної бізнес-цілі (наприклад, крадіжка даних клієнтів
	Blue Team (Синя команда)	Команда внутрішньої безпеки, яка повинна виявити, стримати та відновити систему після атаки Red Team.	Перевірка часу реагування та ефективність процесів.
	Purple Team (Фіолетова команда)	Об'єднує Red та Blue команди для постійного зворотного зв'язку	Навчальний— атака виконується, і Blue Team спостерігає, як спрацьовують їхні засоби захисту.

Продовження таблиці 1.

3. Соціальна інженерія	Фішинг (Phishing) / Спірфішинг (Spear Phishing)	Сценарій імітує розсилку електронних листів для виманювання облікових даних або встановлення шкідливого програмного забезпечення.	Перевірка людського фактору, який є найслабшою ланкою в ланцюгу безпеки.
	Вішинг (Vishing)	Сценарій імітує телефонні дзвінки, спрямовані на обман співробітників з метою отримання конфіденційної інформації.	
	Фізичне проникнення	Сценарій імітує спробу несанкціонованого фізичного доступу до офісу, серверної кімнати або закритої зони.	
4. Моделювання загроз (Threat Modeling)	DREAD або STRIDE (Фреймворки, що використовуються для структурування сценаріїв загроз для програмного забезпечення.)	Сценарій може бути: «Якщо користувач зможе підробити (Spoofing) свою ідентифікацію, які дані будуть скомпрометовані?»	Систематична ідентифікація ризиків на основі дизайну системи
5. Реагування на інциденти та відновлення (BDR/IR)	Витік даних (Data Breach Scenario)	Перевірка повного процесу — від виявлення до повідомлення регуляторів і громадськості.	Перевірка, що відбувається після успішної атаки або катастрофи.
	Викуп (Ransomware Scenario)	Перевірка процедури відновлення бізнесу з резервних копій, комунікації з кризовим менеджментом та ізоляції скомпрометованих систем.	

Незважаючи на свою поширеність, сценарний підхід у кібербезпеці має обмеження, включаючи суб'єктивність та складність прогнозування через залежність від експертної думки, а також значні матеріальні та трудові витрати, що вимагає його комбінування з іншими методами для мінімізації недоліків.

7.1.1.3 Когнітивне моделювання в кібербезпеці

Сценарії в кібербезпеці можна розробляти за допомогою когнітивного моделювання. «Когнітивне моделювання — це моделювання процесів людського мислення в обчислювальній моделі, яка є поєднанням різних дисциплін. Воно є важливим, оскільки дає знання про процеси мозку, такі як сприйняття, пам'ять та прийняття рішень; отже, його використовують для оцінки та розуміння поведінки людей у різних ситуаціях» [159]. У науковій роботі [160] був здійснений аналіз типів когнітивного моделювання та можливості його застосування в кібербезпеці.

1. Символічне моделювання (на основі правил) створює моделі, що імітують людське мислення та когнітивні функції, використовуючи чітко визначені правила та символи («Що, якщо»).

2. Моделювання на основі мереж (нейронні мережі) застосовує штучні нейронні мережі — об'єднані вузли (нейрони), які можуть навчатися та адаптуватися до нової інформації. Цей метод дозволяє моделювати процеси навчання та розпізнавання образів.

3. Баєсові моделі (ймовірнісне моделювання) використовує теорію ймовірностей для моделювання процесів прийняття рішень та прогнозування на основі апріорних знаннях.

4. Моделювання на основі агентів (симуляційне) створює віртуальне середовище, в якому автономні гравці (агенти) взаємодіють між собою та з оточенням, що дозволяє симулювати різні поведінкові дії та їхній колективний вплив.

Існують і гібридні моделі, які об’єднують вище перераховані. До таких моделей відносять нечіткі когнітивні карти (НКК). НКК – математична модель,

представлена у вигляді зваженого орієнтованого графа. Вузли графа – концепти (ключові фактори), зважені дуги – зв'язки між концептами з напрямом впливу та вагою в межах від – 1 до +1.

Нагадаємо побудову нечіткої когнітивної карти [152].

Крок 1. Ідентифікація складної ситуації, проблеми.

1.1 Формулювання завдання і цілей дослідження;

1.2 Збір аналітичних даних з проблеми;

1.3 Окреслення основних ознак проблемної ситуації;

1.4 Виділення факторів впливу, основних об'єктивних законів суспільства;

1.5 Визначення можливих вимог, умов, обмежень у даній ситуації;

1.6 Виділення основних суб'єктів, пов'язаних з ситуацією, та чинників, на які можуть впливати дані суб'єкти.

Крок 2. Побудова когнітивної карти.

1.1 Робота експертів по виділенню факторів, що характеризують проблемну ситуацію;

1.2 Групування факторів на блоках та представлення показників для аналізу процесу у даній ситуації;

1.3 Визначення зав'язків між факторами: позитивний «+» чи негативний «–», ступінь впливу від –1 до + 1 або сильно, середньо, слабо;

1.4 Побудова орієнтованого зваженого графа.

Крок 3. Моделювання та перевірка адекватності моделі.

3.1 Визначення початкових умов у даній ситуації;

3.2 Задання цільових напрямів (збільшення, зменшення) і сили напряму;

3.3 Вибір заходів для впливу на ситуацію;

3.4 Окреслення індикаторів, що характеризують розвиток ситуації;

3.5 Порівняння результатів з минулими даними

Крок 4. Динамічний аналіз ситуації: генерація сценаріїв типу «якщо…, то…».

НКК — це гібридна, причинно-наслідкова модель, яка поєднує структурну наочність із гнучкістю нечіткої логіки, що робить її високоефективним

інструментом когнітивного моделювання для кібербезпеки, що доведено у дослідженнях [152, 161-163].

7.1.1.4 Взаємозв’язок понять «кіберризик», «сценарний підхід», «когнітивне моделювання»

Взаємозв'язок між цими поняттями є циклічним та синергетичним, оскільки вони всі слугують одній меті: ефективному управлінню кіберризиками (таблиця 2).

Кіберризик є об'єктом управління, який необхідно оцінити та мінімізувати.

Сценарний підхід є методологічною рамкою для виявлення та деталізації того, як саме цей ризик може бути реалізований.

Когнітивне моделювання є інструментом для аналізу та візуалізації складної структури сценаріїв, допомагаючи зрозуміти, які фактори є найбільш критичними та як вони взаємодіють.

Таблиця 2. Порівняння ролей сценарного підходу та когнітивного моделювання в управлінні кіберризиком

Етап управління ризиком	Роль сценарного підходу	Роль когнітивного моделювання
Ідентифікація ризику	Визначає конкретні шляхи (сценарії) реалізації кіберризику	Допомагає виявити приховані або неочевидні взаємозв'язки між факторами в межах сценарію
Оцінка ризику	Надає вхідні дані (наслідки сценарію) для кількісної або якісної оцінки кіберризику.	Використовується для прогнозування динаміки та оцінки ймовірності розвитку подій за певним сценарієм, а також сили впливу факторів на кінцевий результат.
Обробка ризику	Тестує ефективність заходів захисту та планів реагування в умовах імітації (навчання на сценаріях).	Дозволяє експериментувати для даного випадку із різними стратегіями реагування (зміна ваги факторів) для вибору оптимального рішення.

Таким чином, когнітивне моделювання, застосоване до сценарного підходу, дозволяє не просто описати, а зрозуміти та кількісно оцінити складні, багатофакторні кіберризики, підвищуючи обґрунтованість рішень у сфері кібербезпеки.

Використання когнітивних сценаріїв є потужним інструментом для команд SOC (Security Operations Center) та CERT (Computer Emergency Response Team), що дозволяє значно підвищити ефективність реагування на кіберінциденти, особливо ті, що пов'язані з людським фактором. Ця інтеграція реалізується на кількох взаємопов'язаних рівнях.

По-перше, когнітивні моделі застосовуються для пріоритезації інцидентів. Завдяки оцінці впливу різних факторів на успішність атаки, таких як поєднання високої довіри користувача та складності атаки, моделі допомагають виокремити події з найбільшим потенціалом ескалації.

По-друге, впровадження передбачає формування автоматизованих когнітивних профілів користувачів і типових моделей поведінки. На основі когнітивних карт SOC/CERT можуть створювати поведінкові карти ризиків, ідентифікуючи, наприклад, співробітників, більш вразливих до соціальної інженерії. Це дає змогу генерувати сценарії, що показують, як низька обізнаність чи висока довіра можуть вплинути на можливість компрометації, і таким чином формувати персоналізований підхід до управління ризиками.

Третій рівень — це застосування когнітивних сценаріїв для сценарного прогнозування. SOC та CERT використовують результати симуляцій для побудови «Що, якщо» моделей, які тестують стратегії реагування на різні тактики зловмисників. У випадку фішингової кампанії модель допомагає оцінити, як зміна інтенсивності чи складності атак вплине на користувачів, дозволяючи вибудовувати стратегії випереджувального реагування, а не лише постфактумної реакції.

Особливо важливою є підтримка прийняття рішень у реальному часі. На основі когнітивної карти можна налаштувати автоматичні тригери, які попереджатимуть аналітиків SOC про можливу ескалацію інциденту ще до того,

як технічна компрометація стане очевидною. Наприклад, виявлення поведінки, типової для користувача з високою ймовірністю довіри до підозрілих листів, може автоматично підвищити критичність інциденту. Такі ранні індикатори значно прискорюють реакцію та мінімізують наслідки.

Крім того, когнітивні сценарії інтегруються в навчальні програми та тренінги для SOC/CERT. Результати моделювання дають змогу адаптувати навчання під реалістичні сценарії, що враховують не лише технічні прояви, але й реальну поведінку людей та типові тактики зловмисників. Це робить тренувальні симуляції значно ефективнішими, цілеспрямовано працюючи з людським фактором.

У результаті, таке комплексне впровадження створює багаторівневу систему оцінки ризиків, де технічні індикатори доповнюються когнітивними сигналами. Реакція системи ґрунтується на поведінкових патернах, підтверджених моделюванням. Це дає SOC та CERT можливість оперативніше виявляти загрози, точніше прогнозувати розвиток інцидентів та ефективніше управляти ризиками, пов’язаними як з фішинговими, так і з іншими соціально-інженерними загрозами.

7.1.2 Практична реалізація формування сценаріїв кіберінцидентів на основі когнітивних моделей

Практична реалізація формування сценаріїв кіберінцидентів на основі когнітивних моделей у цій роботі була здійснена з застосуванням нечітких когнітивних карт (НКК) для моделювання сценарію використання організаціями слабких паролів.

1. Визначаємо концепти:

C1. Складність пароля. Рівень довжини, різноманітності символів та його унікальності;

C2. Повторне використання паролів. Використання одного пароля для багатьох сервісів;

С3. Обізнаність користувачів щодо безпеки паролів. Знання принципів створення безпечних паролів та наслідків компрометації;

С4. Використання менеджерів паролів. Впровадження інструментів для генерації й зберігання паролів;

С5. Ймовірність компрометації облікових даних. Ймовірність зламу пароля, його перебору або витоку;

С6. Успішність атаки типу Brute Force. Ефективність атаки, спрямованої на підбір або перевірку паролів;

С7. Рівень доступу зловмисника після компрометації. Наскільки критичний доступ може отримати цей зловмисник;

С8. Захист облікових даних. MFA, моніторинг, блокування підбору;

С9. Ризик масштабного інциденту. Ланцюгова компрометація, доступ до критичних систем;

С10. Політика паролів в організації. Регламенти, наприклад, мінімальна довжина, заборона повторень, періодична зміна пароля тощо.

2. Визначимо значення ваг для нашої НКК:

С3→С1, вага +0,7 (сильний позитивний вплив), адже чим вища обізнаність, тим складніші паролі створює користувач;

С3→С2, вага -0,6 (помірний негативний вплив), адже обізнаний користувач рідше повторює вже створений пароль;

С4→С1, вага +0,9 (сильний позитивний вплив), адже менеджери паролів генерують складніші паролі;

С4→С2, вага -0,8 (сильний негативний вплив), адже менеджери паролів усувають проблему повторного використання, бо зберігають унікальні паролі;

С10→С1, вага +0,8 (сильний позитивний вплив), адже політика паролів компанії напряму формує вимоги до складності паролів;

С10→С2, вага -0,7 (сильний негативний вплив), адже політика паролів може забороняти повторне використання паролів;

C1→C5, вага -0,7 (сильний негативний вплив), адже чим складніший пароль, тим менша ймовірність його компрометації;

C1→C6, вага -0,6 (помірний негативний вплив), адже сильні паролі складніше підібрати, що знижує успішність атаки Brute Force;

C5→C7, вага +0,9 (сильний позитивний вплив), адже компрометація часто дає значний рівень доступу;

C7→C9, вага +0,9 (сильний позитивний вплив), адже якщо зловмисник отримав високий доступ, то високий ризик масштабу інциденту;

C8→C5, вага -0,8 (сильний негативний вплив), адже MFA та інші засоби знижують ймовірність успішної компрометації;

C3→C4, вага +0,5 (помірний позитивний вплив), адже обізнані користувачі частіше встановлюють менеджери паролів;

C10→C8, вага +0,5 (помірний позитивний вплив), адже політика безпеки часто включає обов’язкове використання MFA.

3. Будуємо матрицю зв’язків ваг (таблиця 3).

Таблиця 3. Матриця зв’язків ваг

	C1	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**	**C8**	**C9**	**C10**
C1	0	0	0	0	–0,7	–0,6	0	0	0	0
C2	0	0	0	0	0	0	0	0	0	0
C3	0,7	–0,6	0	0,5	0	0	0	0	0	0
C4	0,9	–0,8	0	0	0	0	0	0	0	0
C5	0	0	0	0	0	0	0,9	0	0	0
C6	0	0	0	0	0	0	0	0	0	0
C7	0	0	0	0	0	0	0	0	0,9	0
C8	0	0	0	0	–0,8	0	0	0	0	0
C9	0	0	0	0	0	0	0	0	0	0
C10	0,8	–0,7	0	0	0	0	0	0,5	0	0

Задано попередні дані: $C(0) = [C1 = 0{,}4; C2 = 0{,}7; C3 = 0{,}4; C4 = 0{,}3; C5 = 0{,}6; C6 = 0{,}5;\ C7 = 0{,}6; C8 = 0{,}4; C9 = 0{,}5; C10 = 0{,}5)$. У сценаріях нижче будуть змінюватись компоненти, які розглядаються, а інші залишатись базовими.

4. Створюємо за заданими параметрами НКК (рис. 1):

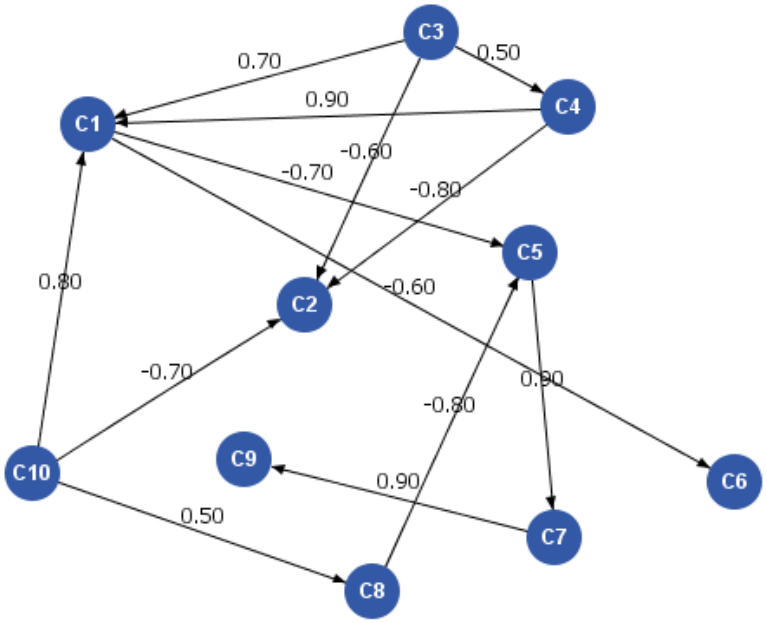

Рисунок 1. Нечітка когнітивна карта (початкова)[авторська розробка]

У роботі представлені розрахунки для ключових концептів, що формують траєкторію «C3 → C1/C2 → C5 → C6 → C7 → C9». Ця траєкторія дозволяє відобразити як обізнаність користувачів впливає на складність паролю та його повторне використання, як ці фактори впливають на ймовірність компрометації, і як успішний злам паролю може призвести до критичного доступу та масштабного інциденту.

5. Для моделювання і проведення симуляцій було використано програму FCM Expert. FCM Expert – це спеціалізоване програмне забезпечення призначене для створення та симуляцій нечітких когнітивних карт [164].

Запускаємо симуляцію на початковому етапі, не змінюючи нічого, отримуємо значення (рис. 2 та рис. 3):

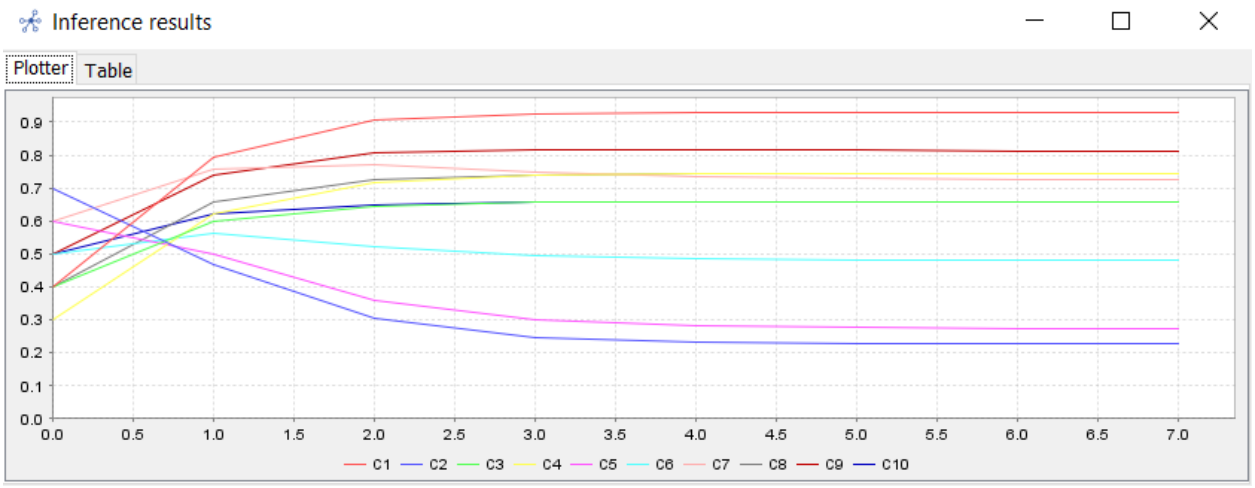

Рисунок 2. Початкова симуляція (графічне представлення) [авторська розробка]

Inference results

Plotter | Table

Step	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10
0	0.4	0.7	0.4	0.3	0.6	0.5	0.6	0.4	0.5	0.5
1	0.7941	0.4675	0.5987	0.6225	0.5	0.5646	0.7577	0.657	0.7389	0.6225
2	0.9065	0.3046	0.6454	0.7154	0.3586	0.522	0.7699	0.7248	0.8055	0.6508
3	0.9257	0.2478	0.656	0.7385	0.2982	0.4945	0.7489	0.7408	0.8173	0.6572
4	0.9293	0.2321	0.6584	0.7439	0.2804	0.4848	0.7344	0.7445	0.8163	0.6586
5	0.93	0.2281	0.6589	0.7452	0.2757	0.4818	0.7285	0.7453	0.8142	0.659
6	0.9302	0.2271	0.659	0.7455	0.2746	0.481	0.7264	0.7455	0.813	0.659
7	0.9302	0.2269	0.659	0.7455	0.2743	0.4807	0.7258	0.7456	0.8126	0.659

Рисунок 3. Початкова симуляція [авторська розробка]

У першій базовій симуляції, де параметри ще не змінювались, простежується, природня динаміка ланцюжка. При незмінних вхідних умовах обізнаність користувачів (C3) поступово підтягує складність паролів (C1) та знижує повторне використання (C2), що вже на початкових етапах веде до стабільного невеликого зменшення компрометації. Відповідно, зниження компрометація (C5) впливає на рівень успішності атаки типу Brute Force (C6) і на те, який доступ може отримати зловмисник після зламу (C7). У кінцевому підсумку, це має відбиток на показнику ризику масштабного інциденту (C9).

Для першого досліджуваного сценарію ми змінюємо концепт C3 (обізнаність користувачів щодо безпеки паролів), для того, щоб дослідити, як знання впливають на створення паролів і на подальшу безпеку їх використання. C3 стає з 0,9.

Результати симуляції зображені на рис. 4 та рис. 5.

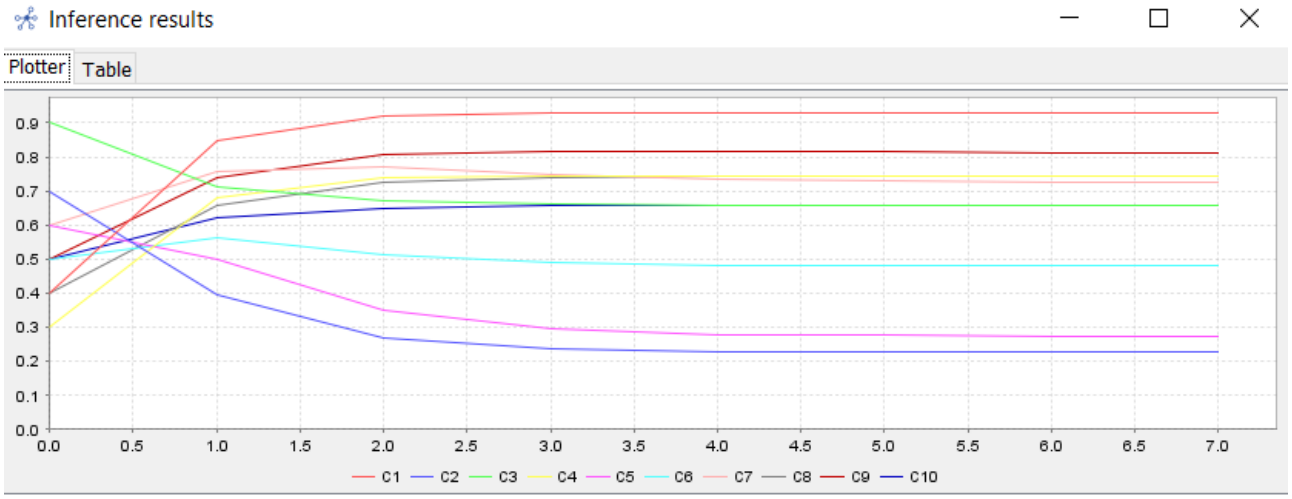

Рисунок 4. Друга симуляція (графічне представлення) [авторська розробка]

Inference results

Plotter | Table

Step	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10
0	0.4	0.7	0.9	0.3	0.6	0.5	0.6	0.4	0.5	0.5
1	0.8455	0.3941	0.7109	0.6792	0.5	0.5646	0.7577	0.657	0.7389	0.6225
2	0.9207	0.2667	0.6706	0.7378	0.3504	0.5143	0.7699	0.7248	0.8055	0.6508
3	0.9292	0.2348	0.6616	0.7452	0.2944	0.4905	0.7475	0.7408	0.8173	0.6572
4	0.9301	0.2282	0.6596	0.7457	0.2792	0.4832	0.7335	0.7445	0.8161	0.6586
5	0.9302	0.227	0.6592	0.7457	0.2754	0.4813	0.728	0.7453	0.814	0.659
6	0.9302	0.2268	0.6591	0.7456	0.2745	0.4808	0.7263	0.7455	0.8129	0.659
7	0.9302	0.2268	0.6591	0.7456	0.2743	0.4807	0.7258	0.7456	0.8125	0.659

Рисунок 5. Друга симуляція [авторська розробка]

Порівняння цієї симуляції з першою показує, як різке підвищення обізнаності користувачів змінює поведінку системи. З результатів видно, що C1 (складність паролю) зростає значно швидше та досягає вищих значень уже на першому кроці, а C2 (повторне використання паролів) навпаки знижується. Це очікуваний результат, адже підвищення обізнаності безпосередньо стимулює створення складніших паролів та зменшує повторне використання, що наочно було доведено результатами симуляції. Окрім цього, концепт C5 (ймовірність компрометації) у другій симуляції спадає до нижчого рівня, ніж у першій. Це також впливає і на C6 (успішність Brute Force атаки), який зменшується, на C7 (рівень доступу зловмисника після зламу) та не кардинально, але на C9 (ризик масштабного інциденту). Ці концепти стабілізуються на нижчих показниках

порівняно з першою симуляцією, що демонструє зниження загального ризику для системи.

У підсумку, підвищення концепту C3 привело систему до більш захищеного стану та забезпечило нижчу ймовірність масштабного інциденту, ніж у базовій симуляції без зміни параметрів.

У наступному сценарії залишаємо вже введені зміни, але також додаємо зміну концепту C8 (захист облікових даних). C8 = 0.8, результати симуляції зображені на рис. 6 та рис. 7.

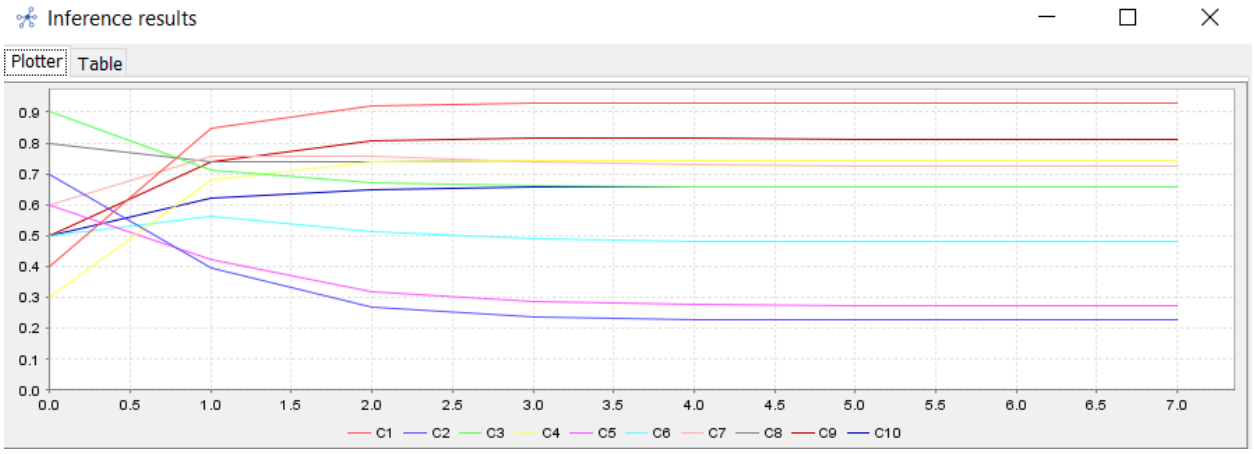

Рисунок 6. Третя симуляція (графічне представлення) [авторська розробка]

Inference results

Plotter | Table

Step	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10
0	0.4	0.7	0.9	0.3	0.6	0.5	0.6	0.8	0.5	0.5
1	0.8455	0.3941	0.7109	0.6792	0.4207	0.5646	0.7577	0.7408	0.7389	0.6225
2	0.9207	0.2667	0.6706	0.7378	0.3178	0.5143	0.757	0.7412	0.8055	0.6508
3	0.9292	0.2348	0.6616	0.7452	0.285	0.4905	0.7394	0.7439	0.8156	0.6572
4	0.9301	0.2282	0.6596	0.7457	0.2768	0.4832	0.7303	0.7451	0.8147	0.6586
5	0.9302	0.227	0.6592	0.7457	0.2748	0.4813	0.727	0.7454	0.8134	0.659
6	0.9302	0.2268	0.6591	0.7456	0.2743	0.4808	0.726	0.7455	0.8127	0.659
7	0.9302	0.2268	0.6591	0.7456	0.2742	0.4807	0.7257	0.7456	0.8125	0.659

Рисунок 7. Третя симуляція [авторська розробка]

З наведених результатів прослідковується вплив посилених механізмів захисту на загальну динаміку моделі. Порівняно з попередньою симуляцією, де підвищували лише концепт C3, і першою, де параметри були базовими, зміна C3 та C8 призводять до найбільш помітного зниження C5, що є очікуваним, адже MFA та інші засоби безпеки безпосередньо знижують доступ, навіть, у випадку

слабкого паролю. У результаті також зменшились і значення C7 та C9, хоча зміни тут менш різкі, бо вони залежать не лише від C8, а й від компрометації, що знижується поступово. Усі інші компоненти демонструють майже ідентичну поведінку до другої симуляції, що вказує на те, що посилення тільки захисту не змінює поведінку користувачів (наприклад, складність паролю, повторне його використання тощо), але впливає на кінцеві ризики.

Загалом третя симуляція показує, що навіть при високих значеннях C2 (повторне використання) та недостатньо високої складності паролів, сильні механізми захисту можуть стримувати розвиток атаки й знижувати критичні наслідки.

Таким чином, нечітка когнітивна карта дозволяє швидко проводити аналіз типу "Що, якщо" шляхом модифікації початкових умов; зміна значення лише одного концепту генерує нові сценарії розвитку подій і водночас демонструє ефективність застосованих захисних заходів.

Варто відзначити, що існуючі моделі прогнозування кіберризиків переважно використовують історичні дані, проте їхня валідність та прогностична спроможність ставляться під сумнів в умовах експоненційно швидкого розвитку та перманентної трансформації загрозливого кіберландшафту [146, с.6]. Створення надійних сценаріїв кіберризиків вимагає поєднання людського досвіду та штучного інтелекту, однак прийняття рішення залишається за людиною.