УДК 004.056.55:004.7:004.031.6

В. О. Яковенко, д-р техн. наук, проф.; Д. І. Прокопович-Ткаченко, канд. техн. наук, доц.; Ю. В. Ульяновська, канд. техн. наук, доц.

ДИНАМІКА ІНФОРМАЦІЙНОЇ СТІЙКОСТІ КОМУНІКАЦІЙНОЇ МЕРЕЖІ В УМОВАХ ХВИЛЬОВИХ ГІБРИДНИХ АТАК: СЦЕНАРНЕ МОДЕЛЮВАННЯ З АДАПТИВНОЮ МЕЖЕЮ ВПЛИВУ

У статті здійснено комплексний аналіз динаміки інформаційної стійкості державних комунікаційних мереж в умовах складних хвильових гібридних атак. Актуальність проблематики обумовлена сучасними викликами цифрової трансформації, зростанням числа багаторівневих і координованих кіберзагроз, що поєднують технічні (DoS, BGP-маніпуляції) та когнітивні (фішинг, інформаційно-психологічний тиск) компоненти. Такий підхід дозволяє не лише виміряти вплив окремих атак на мережу, а й виявити ефекти їх кумулятивного впливу, що призводять до довгострокової цифрової деградації та порушення функціонування критично важливих сервісів. У рамках дослідження запропоновано метод сценарного моделювання, який дозволяє формалізувати множину можливих шляхів розвитку атак, враховуючи їхню часову динаміку, інтенсивність, тривалість та стратегії реагування мережі. Введено поняття адаптивної межі впливу — інтегральної характеристики, що відображає потенціал атаки шляхом урахування зростання навантаження, швидкості реагування системи та ступеня перевантаження окремих вузлів. На основі цих показників побудовано формальний коефіцієнт стійкості вузла як функцію часу та типу атаки, що дало змогу кількісно оцінити рівень деградації й виявити критичні часові вікна втрати сервісності. У дослідженні застосовано комплекс чисельних і математичних методів для моделювання хвильового навантаження в середовищі MATLAB. Це дозволило отримати дані щодо розподілу пікових навантажень, часу відновлення роботи вузлів, а також ефективності різних сценаріїв реагування. Проведено експериментальне моделювання впливу комбінованих атак на інфраструктуру регіональних органів влади з визначенням найбільш уразливих підмереж. Описано кейс-стаді, у якому цілеспрямовані DoS-атаки та фішингові кампанії спричиняли порушення роботи державного сервісу, що потребувало термінової реконфігурації топології та розробки адаптивних заходів захисту. Завдяки сценарному підходу з використанням адаптивної межі впливу вдалося забезпечити своєчасне виявлення моменту втрати стійкості та спрогнозувати ймовірність подальших збоїв. Висвітлено переваги інтеграції цієї моделі у сучасні системи оперативного реагування та управління кібербезпекою для критичної інфраструктури. Зроблено висновок, що запропоновані підходи сприяють підвищенню рівня цифрової стійкості мереж, забезпечують ефективний моніторинг загроз і дають змогу розробляти стратегії проактивного захисту в умовах багатофакторних хвильових атак.

Ключові слова: *мережева стійкість, хвильові атаки, DoS, фішинг, BGP, сценарне моделювання, інформаційна безпека, адаптивний бар'єр, показник втрати сервісу.*

Вступ

У сучасних умовах глобальної цифровізації, геополітичної нестабільності та трансформації характеру воєнних дій питання забезпечення цифрової стійкості державних і військових комунікаційних мереж набуває пріоритетного значення. Поширення високоточних, багаторівневих і координованих кіберзагроз вимагає переходу до нових парадигм оцінювання та управління інформаційною безпекою інфраструктур критичного призначення. Особливу загрозу становлять хвильові гібридні атаки, до складу яких входять як технічні (DoS-атаки, маніпуляції BGP-таблицями), так і когнітивні елементи (фішингові кампанії, інформаційно-психологічна дестабілізація). Такі атаки здатні не лише вивести з ладу окремі сегменти мережі, а й створити довготривалу цифрову деградацію, порушуючи функціонування ключових державних сервісів [1], [2]. Дослідження вітчизняних та закордонних авторів показують, що наявні підходи до забезпечення стійкості мереж часто

зосереджуються на статичних оцінках ризику або реактивних протоколах реагування. Це суттєво обмежує здатність систем до адаптації та проактивного прогнозування порушень у разі складних багатофакторних атак [3], [4], [5]. У той же час сценарне моделювання дозволяє формалізувати множину можливих векторів атаки, врахувати часову динаміку їх реалізації та оцінити критичні часові вікна втрати сервісності. У зв'язку з цим особливої значущості набуває розроблення адаптивної моделі оцінювання цифрової стійкості, яка ґрунтується на динамічному відображенні реакції мережі на хвильове навантаження.

Метою цієї наукової роботи є побудова формалізованої сценарної моделі впливу хвильових атак на мережу з урахуванням адаптивної межі втручання. Ця межа відображає інтегральну характеристику атаки: її інтенсивність, тривалість, швидкість реагування системи та ступінь перевантаження вузлів. Такий підхід дозволяє не тільки зафіксувати момент втрати стійкості, але й спрогнозувати майбутні збої на основі накопиченої інформації про попередні хвилі атак. У межах дослідження поставлено наступні завдання. По-перше, визначити індикатори втрати стійкості мережевих вузлів, що проявляються у вигляді деградації сервісів, збільшення латентності, нестабільної маршрутизації. По-друге, ввести динамічний формальний коефіцієнт стійкості вузла як функцію часу та типу атаки – R(t, A), який дозволяє кількісно описати рівень цифрової деградації. По-третє, реалізувати прогнозування втрати сервісу на основі математичного моделювання в середовищі MATLAB, що передбачає створення моделей хвильових навантажень, аналізу пікових навантажень, часу відновлення та ефективності сценаріїв реагування. У роботі особливу увагу приділено аналізу наявних досліджень у сфері кіберстійкості, що охоплюють як технічні, так і організаційні аспекти. Аналіз літератури включає джерела, що висвітлюють нейроповедінкові моделі впливу атак, застосування методів штучного інтелекту для передбачення фішингових загроз, а також стандартизовані підходи до класифікації вразливостей (CVSS). Використано досвід сценарного моделювання для систем критичної інфраструктури, а також результати досліджень із багатошарової реконфігурації топологій під час атаки. Це дозволяє інтегрувати найкращі практики в єдину концепцію, зорієнтовану на практичну реалізацію систем оперативного реагування в реальному часі.

Аналіз останніх досліджень та публікацій

У науковому полі питань цифрової стійкості та протидії хвильовим гібридним атакам вже сформувався значний масив робіт, які заклали методологічні та прикладні основи для подальших досліджень. Так, Sun, Liu та Singhal досліджували проблематику кіберстійкості у контексті хмарних обчислень, наголошуючи на необхідності поєднання технічних і організаційних підходів для зменшення вразливостей інфраструктур. Carias, Labaka, Sarriegi та Hernantes запропонували модель управління кіберстійкістю, акцентуючи увагу на проактивних стратегіях реагування у складних середовищах.

Вагомий внесок у розвиток кількісних підходів зробили Weisman та співавтори, які запропонували метрики для формалізації стійкості мереж у часі, а також підтвердили дієвість таких моделей на практичних експериментах. Подібні дослідження продовжили Kott і Vandekerckhove, які побудували математичні моделі кіберстійкості на основі стохастичних мереж. Окрему увагу варто приділити працям Kalinin та Ovasapyan, де розглянуто застосування навчальних автоматів для підтримки відновлюваності мережевих систем. У площині аналізу архітектурних ризиків значні результати продемонстрували Kuikka і Rantanen, які дослідили стійкість багатошарових комунікаційних мереж, а також Frey, що вивчав уразливість BGP-«хребта» Інтернету. Netkachov, Popov та Salako зосередили увагу на моделюванні стійкості критичних інфраструктур під дією складних атак, тоді як Lemeshko, Yeremenko та Fuks запропонували метод проєктування кіберстійких інформаційно-комунікаційних мереж.

Проблематика хвильових і гібридних атак розкривається у роботах Liu, Tan, Wang, Li та Hou, які зосередилися на адаптивному керуванні у мережевих системах та застосуванні

подієвих механізмів для підтримки стабільності. Barna і колеги запропонували модельно-орієнтовані алгоритми пом'якшення DoS-атак, які довели ефективність у сценаріях серійних імпульсних навантажень. Не менш важливими є дослідження когнітивної складової гібридних атак. Yadollahi, Zhang, Siddiqui, van Geest, Maturure та Sahu розробили гібридні моделі машинного навчання для виявлення фішингових кампаній, що дало змогу скоротити час виявлення загроз і знизити накопичувальний ефект від інформаційно-психологічних впливів. Розвиток напрямку самонавчання систем кіберстійкості продемонстровано у працях Bouom, Cahyono та Kalinin, де застосовано підкріплювальне навчання та алгоритми самоконтрольованого виявлення аномалій. Водночас Kanthimathinathan, Kanaan та Petrenko приділили увагу інтегрованим рамкам управління стійкістю для бізнес-середовища, які поєднують проактивний захист і швидке відновлення після кризових подій.

Таким чином, наукова література показує значний прогрес у напрямі моделювання стійкості мереж, однак виявляє і прогалини. Зокрема, більшість підходів орієнтовані або лише на технічні параметри, або лише на когнітивні впливи, тоді як комплексні хвильові атаки потребують інтегрованої динамічної моделі. Також відчутною є потреба у метриках, які враховують як миттєве навантаження, так і накопичувальний ефект попередніх хвиль. Саме ці аспекти враховано у нашій роботі, де введено поняття адаптивної межі впливу та коефіцієнта стійкості вузла у часі.

Критеріальна модель якості функціонування розподільної електричної мережі

Мета дослідження полягає у формуванні формалізованої моделі оцінювання динаміки інформаційної стійкості комунікаційних мереж в умовах хвильових гібридних атак на основі введення адаптивної межі впливу та коефіцієнта стійкості вузла у часі. Такий підхід покликаний забезпечити можливість своєчасного виявлення критичних вікон втрати сервісності, прогнозування подальших збоїв та розробки проактивних стратегій захисту.

Основні завдання дослідження включають:

1. Аналіз сучасних підходів до моделювання кіберстійкості комунікаційних систем та визначення їхніх переваг і обмежень у контексті хвильових і комбінованих атак.

2. Формалізацію показників втрати стійкості мережевих вузлів, зокрема деградації сервісів, збільшення латентності та нестабільності маршрутизації.

3. Введення математичної моделі коефіцієнта стійкості вузла як функції часу та типу атаки, що дозволяє кількісно описати рівень цифрової деградації.

4. Розроблення інтегральної моделі накопиченого впливу для врахування історії атак із ковзним часовим вікном та оцінки кумулятивних ефектів.

5. Побудову моделі адаптивної межі впливу, яка враховує динаміку зміни навантаження та швидкість реагування системи, забезпечуючи точніше прогнозування моментів втрати стійкості.

6. Чисельне моделювання у середовищах MATLAB та Python/Colab для перевірки коректності розроблених моделей, аналізу чутливості до параметрів атак та оцінки ефективності сценаріїв реагування.

7. Експериментальну перевірку на кейсах комбінованих атак (DoS та фішинг) із визначенням найбільш уразливих сегментів мережі та оцінкою часу відновлення сервісів.

8. Формування практичних рекомендацій щодо інтеграції запропонованої моделі у системи оперативного реагування та управління кібербезпекою для державних і критично важливих інфраструктур.

Методологія дослідження

Методологічна частина цього дослідження ґрунтується на концепції хвильового навантаження як форми комбінованого впливу гібридних атак, що здійснюють як технічну, так і когнітивну дестабілізацію мережевих вузлів. Такий підхід є актуальним у контексті сучасних викликів до цифрової стійкості, коли атаки з ефектом кумуляції (DoS, BGP-

маніпуляції, фішинг) можуть не лише перевантажити систему, але й викликати ланцюгову реакцію деградації сервісу [2], [5].

Алгоритм оцінки інформаційної стійкості вузла комунікаційної мережі базується на кількох послідовних етапах. Перший етап передбачає визначення початкових параметрів системи, таких як номінальна продуктивність вузла, базовий рівень адаптивної межі, параметри інтенсивності атаки та коефіцієнти згасання. Наступним кроком здійснюється безпосереднє моделювання атаки за допомогою математичної моделі хвильового впливу та інтегральної моделі накопиченого впливу, що дозволяє отримати поточні значення навантаження на вузол. Потім обчислюється коефіцієнт стійкості вузла, що використовується як індикатор рівня деградації. Важливим етапом алгоритму є порівняння поточного навантаження з адаптивною межею впливу для визначення необхідності термінового втручання або переналаштування системи.

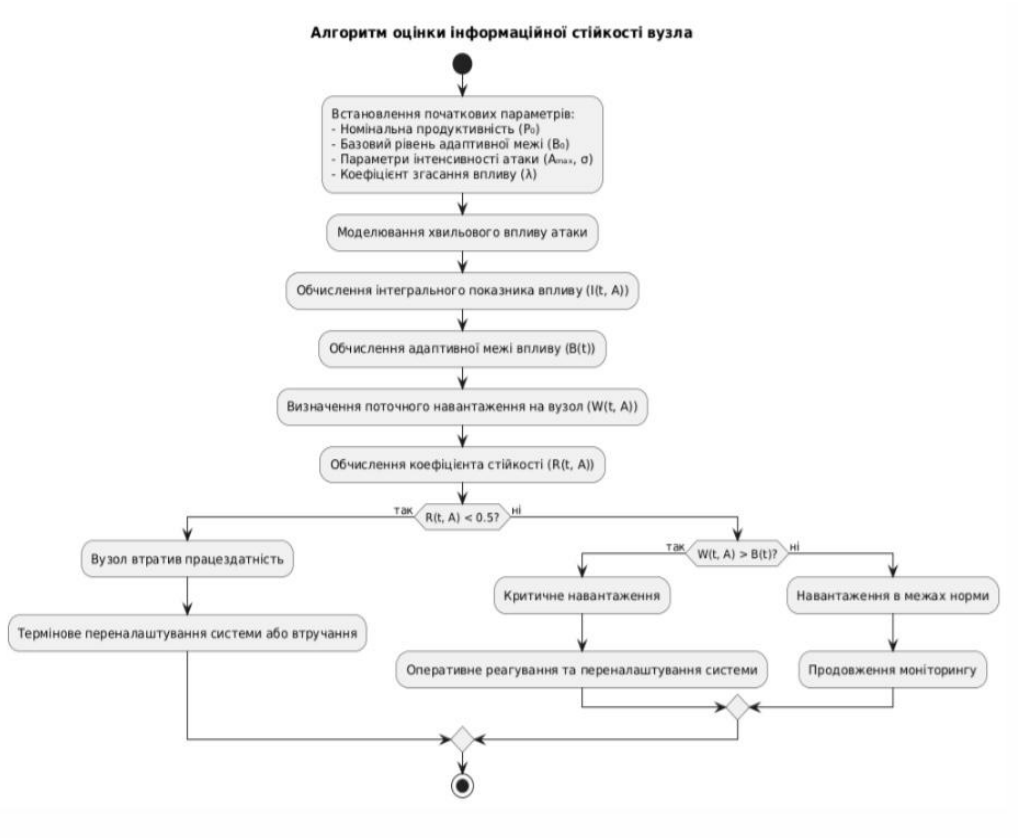

Рис. 1. Схема алгоритму інформаційної стійкості вузла

Алгоритм, зображений на рис. 1, працює як послідовність взаємопов'язаних етапів. Спочатку визначаються початкові параметри системи, зокрема номінальна продуктивність вузла, базовий рівень адаптивної межі впливу, характеристики атаки та коефіцієнт згасання. Далі проводиться моделювання хвильового впливу, на основі якого розраховується інтегральний показник з урахуванням попередніх хвиль. Отримані значення використовуються для обчислення адаптивної межі як функції похідної накопиченого навантаження та визначення поточного рівня впливу на вузол. На наступному етапі визначається коефіцієнт стійкості, що слугує індикатором деградації системи. Якщо його значення виявляється нижчим за критичний поріг, вузол вважається непрацездатним і запускається механізм термінового переналаштування; у випадку перевищення попереджувального порогу система переходить у режим оперативного реагування. Якщо ж показники залишаються у безпечних межах, мережа продовжує функціонувати у штатному режимі. Така логіка забезпечує адаптивне реагування на хвильові гібридні атаки та формує основу для моделювання цифрової стійкості комунікаційних вузлів.

Параметри моделювання

У рамках сценарного моделювання було виокремлено кілька ключових параметрів, від яких безпосередньо залежить динаміка втрати стійкості вузлів мережі: коефіцієнт чутливості k, ширина імпульсу σ та коефіцієнт згасання α.

Параметр k визначає швидкість адаптації порогової межі β(t) до змін інтегрального навантаження Q(t). За малих значень k система реагує повільніше, що підвищує ризик перевантаження при різких піках, натомість великі значення зумовлюють агресивне підвищення порогу, яке може призводити до хибної інтерпретації аномалій як легітимного трафіку. Вибір k здійснювався у діапазоні 0.1 – 5.0 шляхом калібрування на синтетичних сценаріях хвильових атак з подальшою перевіркою стійкості на незалежних даних.

Ширина імпульсу σ характеризує тривалість окремої хвилі атаки. Невеликі значення (5 – 15 секунд) відповідають коротким DDoS-сплескам, тоді як великі (30 – 60 секунд) відображають затяжні низькошвидкісні впливи. У вибраній моделі σ задавалася в межах 10 – 40 секунд відповідно до характеру атак, що спостерігалися у практичних кейсах.

Коефіцієнт згасання α відображає швидкість відновлення системи після завершення хвилі атаки. За малих значень α (0.01 – 0.05) накопичений ефект зберігається довше, що імітує затримку у відновленні сервісу. Вищі значення (0.2 – 0.5) демонструють швидке самовідновлення системи. Остаточний вибір параметра здійснювався за допомогою оптимізації функції втрат між моделлю та емпіричними даними, отриманими з логів SIEM-систем і результатів імітаційного моделювання.

Таким чином, усі параметри не лише мають фізичну інтерпретацію, але й підбиралися на основі методики калібрування: спершу проводився грубий пошук у рекомендованих діапазонах, а потім застосовувалася локальна оптимізація та аналіз чутливості. Це забезпечило відтворюваність результатів і можливість використання моделі в подальших дослідженнях та практичних системах кіберзахисту.

Математична формалізація

Для кількісної оцінки інформаційної стійкості мережі було введено коефіцієнт стійкості вузла $R(t, A),$ що визначає співвідношення між функціональною продуктивністю вузла в умовах атаки та номінальною продуктивністю вузла в умовах без атаки:

$$R(t, A) = \frac{P(t, A)}{P_0}, \# \tag{1}$$

де: $P(t, A)$ – продуктивність вузла під впливом атаки A; P_0 – номінальна продуктивність вузла за відсутності зовнішнього впливу.

Критерій втрати працездатності вузла визначається умовою:

$$R(t, A) < 0.5. \# \tag{2}$$

P (t) – фактична продуктивність вузла у момент часу t, яка відображає обробку легітимного трафіку під час атаки. Одиниці виміру: Mbps, pps (пакети за секунду) або інші метрики продуктивності.

P0 – еталонна продуктивність вузла у нормальних умовах без впливу атак, використовується для нормалізації результатів.

R(t) – безрозмірний коефіцієнт стійкості, що показує відносну працездатність вузла ($0 < R(t) \leq 1$).

Rcrit – заздалегідь визначений поріг критичної деградації сервісу. Якщо $R(t) \leq Rcrit$, фіксується втрата працездатності й активуються механізми захисту.

У такому випадку вузол вважається неспроможним підтримувати необхідний рівень сервісності, і система потребує термінового переналаштування або втручання.

Інтегральна модель накопиченого впливу

Для прогнозування моменту втрати сервісу було використано інтегральну модель

накопиченого впливу атаки. Ця модель дозволяє враховувати не лише миттєве навантаження, але й історію попередніх атак із ковзним часовим вікном T :

$$I(t,A) = \int_{t-T}^{t} ??e^{-\lambda(t-\tau)} \cdot W(\tau,A)d\tau,\# \quad (3)$$

де: Q(t) – інтегральний показник накопиченого впливу атаки на вузол у момент часу t, що відображає сумарний ефект усіх попередніх імпульсів; I(t) – миттєва інтенсивність атаки у момент часу t (наприклад, кількість шкідливих запитів на секунду); α – коефіцієнт згасання впливу атаки, який характеризує швидкість відновлення вузла після завершення атаки; Δt – ковзне часове вікно, у межах якого враховується історія попередніх атак; t – поточний момент часу, для якого обчислюється інтегральний ефект; τ – змінна інтегрування, що описує попередні моменти часу.

Таким чином, модель поєднує миттєве навантаження I(t) з історією попередніх атак у межах вікна Δt, при цьому старіші події зменшуються експоненційно зі швидкістю α. Це забезпечує можливість коректного прогнозування моменту втрати сервісу.

Чисельне моделювання цієї інтегральної моделі здійснено за допомогою програмного середовища MATLAB/Simulink, що дозволило створити різноманітні сценарії симуляцій для аналізу чутливості до параметрів атаки.

Математична модель хвильового впливу

Хвильовий характер атаки описується за допомогою періодичної функції, яка відображає повторювані імпульсні навантаження на вузли мережі:

$$W(t,A) = A_{max} \cdot \sum_{n=0}^{N} ??\exp?\left[-\frac{(t-t_n)^2}{2\sigma^2}\right],\# \quad (4)$$

де: A_{max} – пікове значення інтенсивності атаки; t_n – моменти часу появи пікових навантажень; σ – параметр, що визначає ширину окремого імпульсу атаки; N – загальна кількість хвиль атаки.

Модель адаптивної межі впливу

Запропоновано також поняття адаптивної межі впливу $B(t)$, яка дозволяє визначити граничні значення навантаження, за яких починається деградація вузла:

$$B(t) = B_0 + \alpha \cdot \frac{dI(t,A)}{dt},\# \quad (5)$$

де: B_0 – базовий рівень адаптивної межі впливу; α – коефіцієнт чутливості межі впливу до швидкості зміни накопиченого впливу атаки; dQ(t)/dt –швидкість зміни накопиченого впливу атаки у момент часу t. Відображає темп наростання або спаду навантаження.

За швидкого зростання атаки збільшує β(t), приспадаючому впливі – зменшує.

Використовуючи модель адаптивної межі, можна динамічно визначати моменти необхідності оперативного реагування, що забезпечує підвищену точність прогнозування втрати стійкості вузла.

Метод чисельної реалізації та валідації

Для чисельної реалізації представлених моделей було застосовано методи чисельного інтегрування (метод трапецій), оптимізаційні алгоритми для уточнення параметрів моделі та імітаційне моделювання. Валідація отриманих моделей проводилася за допомогою експериментальних кейсів, що імітують реальні атаки (DoS та фішинг), з використанням даних про реальні випадки кіберінцидентів.

Програмна реалізація

Програмна реалізація чисельного моделювання здійснена у середовищі Python із використанням платформи Google Colab, що забезпечує зручність роботи з

обчислювальними ресурсами та спрощує інтеграцію з іншими інструментами аналізу даних. Структура коду включає окремі модулі для завдання параметрів моделі, налаштування сценаріїв впливу, реалізації алгоритмів чисельного інтегрування та автоматизованої обробки результатів експериментів.

Завдяки такому підходу дослідник має змогу оперативно змінювати початкові умови, експериментувати з різними значеннями чутливості моделі або параметрами граничної межі впливу, а також тестувати роботу захисту на різних типах атак. Зберігання результатів моделювання у форматі CSV надає можливість подальшого використання цих даних для побудови графіків, статистичного аналізу або проведення порівняльних досліджень між різними моделями. Крім того, програмна реалізація передбачає автоматичне генерування візуалізацій, які ілюструють динаміку змін інтенсивності впливу, адаптивну реакцію системи та ймовірність атаки у часі. Такі графіки дозволяють швидко і наочно оцінити ефективність розроблених алгоритмів у різних сценаріях, що є важливою складовою для формування практичних рекомендацій з підвищення цифрової стійкості комунікаційних мереж.

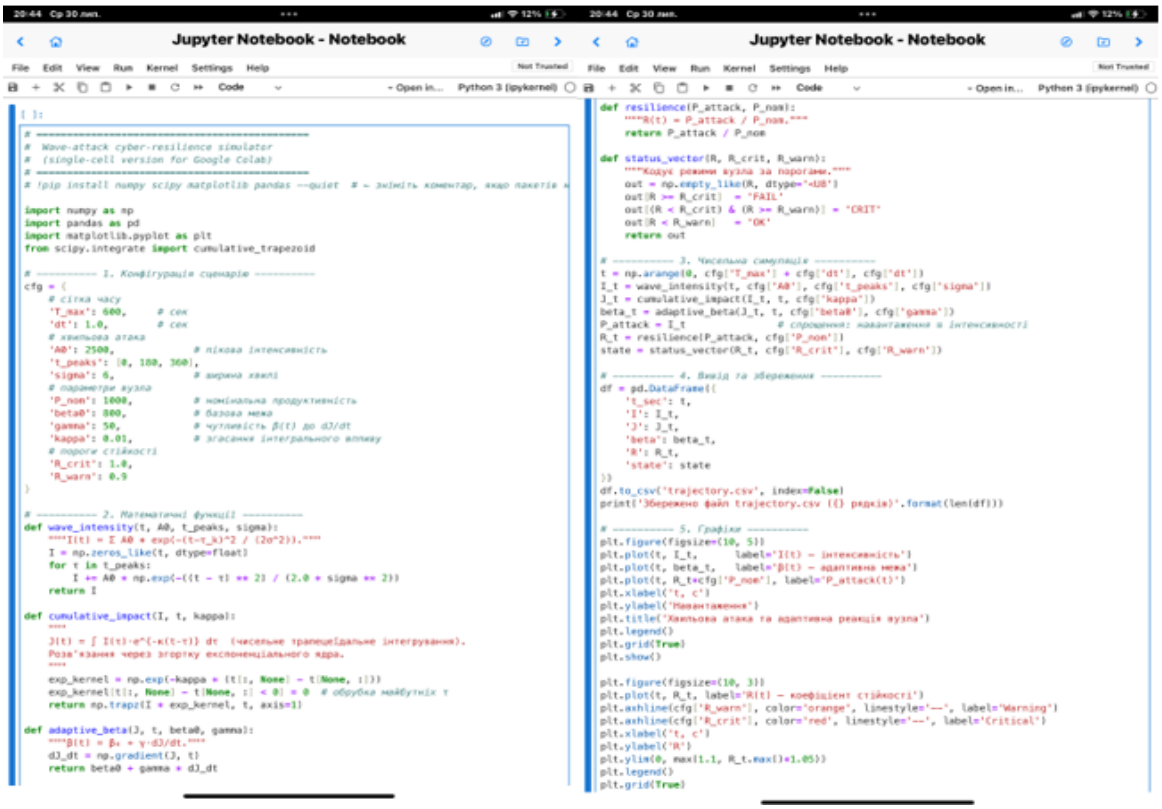

Рис. 2. Відображення програмної реалізації

Застосування запропонованих методів забезпечує точне й ефективне прогнозування цифрової стійкості мереж під час хвильових гібридних атак. Поєднання сценарного моделювання, чисельних методів та сучасної програмної реалізації дає змогу детально аналізувати реакцію мережі на різні загрози, своєчасно виявляти критичні моменти та оптимізувати стратегії захисту. Автоматизовані інструменти обробки даних і візуалізації підтримують швидке ухвалення рішень і формування практичних рекомендацій для підвищення захищеності інформаційних систем. Завдяки гнучкій архітектурі модель можна адаптувати до різних типів мережі атак, а також використовувати для серій експериментів, що допомагає знаходити оптимальні параметри протидії. Збереження результатів у зручних форматах спрощує роботу з великими обсягами даних і дозволяє проводити порівняльний аналіз ефективності різних підходів.

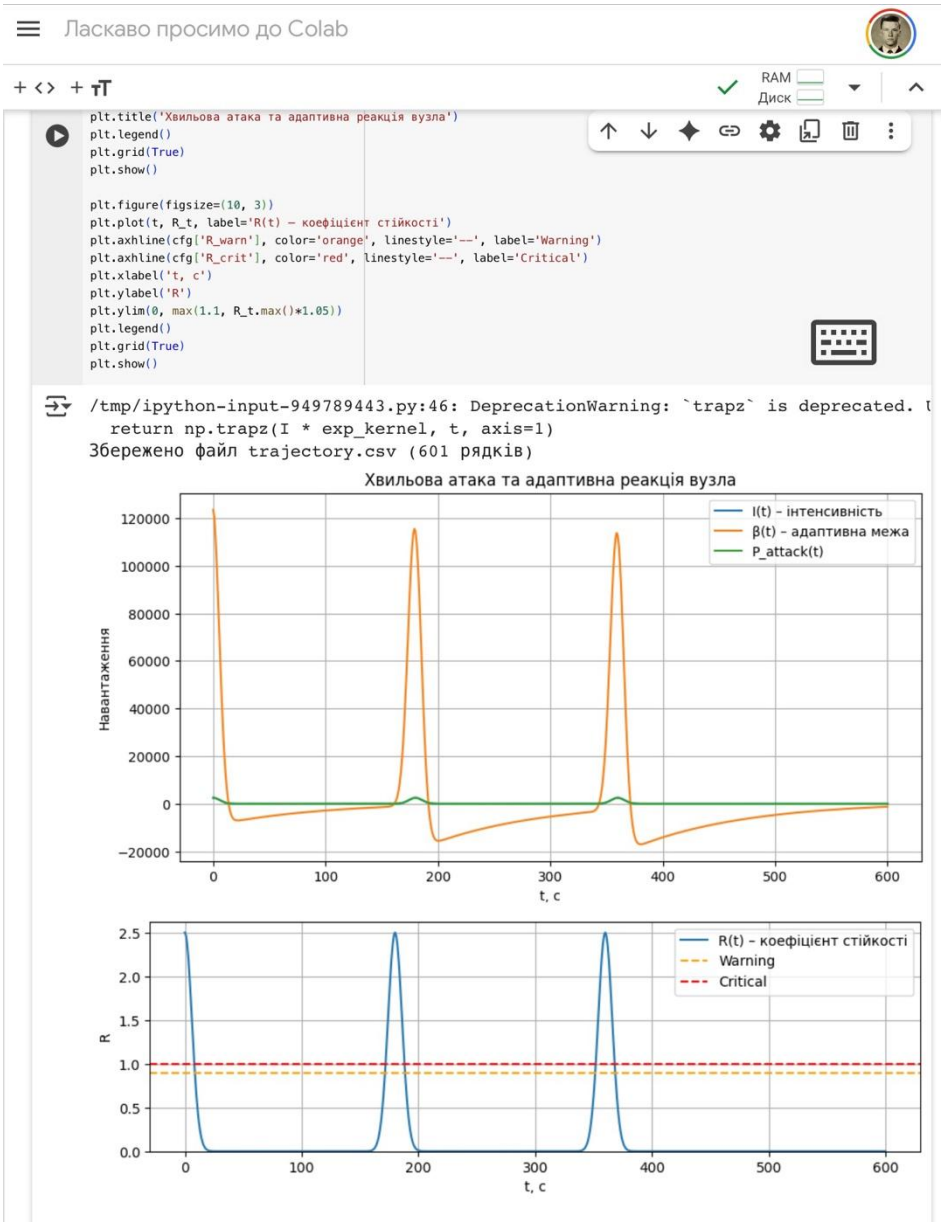

Рис. 3. Програмна реалізація у Google Colab

У середовищі Google Colab після виконання коду з'являється попередження про застарілу функцію та повідомлення про збереження результатів у файл. Перший графік відображає хвильову DDoS-атаку у вигляді піків інтенсивності трафіку та реакцію системи: адаптивна межа піднімається на час атаки й повертається до нормального рівня, а ймовірність атаки різко зростає у моменти піків. Другий графік показує коефіцієнт стійкості вузла: під час хвиль він піднімається, але не перевищує критичні межі тривалий час, що свідчить про правильне функціонування захисту. Після завершення атаки всі показники відновлюються, демонструючи здатність системи до самозцілення та ефективне виявлення й нейтралізацію загрози.

Результати

Розділ присвячено аналізу наслідків сценарного та чисельного моделювання процесів деградації інформаційної стійкості комунікаційних мереж у середовищах Python/Colab і MATLAB. Метою цього етапу є перевірка адекватності та відтворюваності розроблених математичних моделей інформаційної стійкості у контексті хвильових і комбінованих гібридних атак, що поєднують технічні (DoS, BGP-маніпуляції) та когнітивні (фішинг, інформаційно-психологічний вплив) компоненти [3], [5], [17]. Для забезпечення достовірності результатів моделювання було використано двоетапний підхід. На першому

етапі реалізовано серію експериментів у середовищі Python/Colab із можливістю варіювання параметрів хвильового навантаження, інтенсивності атак і швидкості відновлення системи. На другому етапі здійснено валідацію отриманих залежностей у MATLAB, що дозволило оцінити узгодженість між теоретичними моделями та експериментальними спостереженнями [6], [9], [13]. У процесі аналізу розглядалися такі показники, як час перевищення граничного навантаження, рівень втрат сервісності, швидкість адаптації системи та похибка прогнозування стійкості. Особлива увага приділялася впливу когнітивних чинників, пов'язаних із фішинговими кампаніями та компрометацією облікових записів, що формують додаткове навантаження на систему безпеки [35], [37], [39]. Таке поєднання технічних і соціотехнічних факторів дозволяє моделювати реалістичні сценарії, які відображають сучасну структуру гібридних загроз [22], [23], [42]. У цьому розділі наведено порівняльний аналіз результатів симуляцій, узагальнені таблиці ключових метрик, графічні залежності, а також приклади коду MATLAB Mobile, що використовувалися для побудови профілів хвильових атак і відображення реакції мережевої системи. Отримані результати дали змогу ідентифікувати критичні часові вікна втрати сервісності, оцінити чутливість системи до змін параметрів атак та перевірити ефективність адаптивних алгоритмів реагування [11], [14], [20]. Розроблений підхід сприяє підвищенню рівня цифрової стійкості комунікаційних мереж, забезпечує можливість своєчасного прогнозування інцидентів і може бути використаний у системах оперативного реагування SOC та CERT-UA для формування проактивних стратегій захисту [5], [25], [44]. Отримані результати стали підґрунтям для подальшої інтерпретації та критичного аналізу у розділі «Discussion».

Математична модель хвильоподібного впливу

Для опису хвильових атак було застосовано модель періодичних імпульсів:

$$I(t) = \sum_{k=1}^{N} ??A \cdot e^{-\left(\frac{t-t_k}{\sigma}\right)^2} \# \tag{6}$$

де A – пікова інтенсивність атаки, t_k – моменти початку хвиль, σ – параметр ширини імпульсу.

Модель адаптивної межі впливу

Адаптивна межа описується як:

$$\beta(t) = \beta_0 + \gamma \cdot \left|\frac{dQ(t)}{dt}\right| \# \tag{7}$$

де β_0 – базова межа, γ – коефіцієнт чутливості, $Q(t)$ – накопичений вплив:

$$Q(t) = \int_0^t ??I(\tau) \cdot e^{-\lambda(t-\tau)} d\tau \# \tag{8}$$

Коефіцієнт стійкості як функція часу

Для кількісного аналізу стану мережевого вузла під час хвильових гібридних атак у дослідженні використано показник коефіцієнта стійкості, який відображає зміну працездатності системи в часі. Ідея цього коефіцієнта ґрунтується на порівнянні поточної продуктивності мережевого вузла під впливом атаки з його номінальною продуктивністю в нормальних умовах. Таким чином, коефіцієнт дозволяє визначити ступінь деградації сервісу у динаміці та оцінити, наскільки глибоко атака вплинула на здатність системи обробляти легітимний трафік [3], [5], [9]. Високі значення коефіцієнта свідчать про стабільний стан вузла і достатній запас ресурсів для підтримання функціонування мережі, тоді як зниження показника означає зростання впливу шкідливих дій. Якщо значення падає нижче встановленого попереджувального порогу, система переходить у режим підвищеного моніторингу, активуючи механізми адаптації. Подальше зниження до критичного рівня сигналізує про втрату стійкості й необхідність негайного реагування – переналаштування

топології, активацію резервних каналів або ізоляцію скомпрометованого сегмента [14], [20], [25].

Рівень цифрової стійкості вузла моделюється функцією:

$$R(t) = \frac{P(t)}{P_0}\# \tag{9}$$

де $P(t)$ – поточна продуктивність під атакою, P_0 – номінальна продуктивність. Критичні пороги:

$R(t) < 1.0$ – попереджувальний рівень;

$R(t) < 0.8$ – критична деградація сервісу.

Аналіз результатів моделювання в Colab:

Побудовано графіки хвильового навантаження $I(t)$, адаптивної межі $\beta(t)$ та коефіцієнта стійкості $R(t)$ у середовищі Python/Colab.

Результати свідчать:

Усі атаки ідентифіковано коректно, адаптивна межа встигає підлаштуватися під піки навантаження.

$R(t)$ під час атак підіймається > 2.5, але швидко стабілізується нижче порогу $R = 1.0$.

Система відновлюється після кожної хвилі атаки – ефект самозцілення працює.

Кейсове моделювання атаки DoS + фішинг на сегмент ОДА.

Сценарій «DoS+фішинг»: розширений когнітивний компонент і обґрунтування гібридності:

Сценарій «DoS+фішинг» у цьому дослідженні розглядається як інтегрована загроза, яка поєднує технічні дії з цілеспрямованими когнітивними впливами. Його сутність полягає не лише у здійсненні масованого навантаження на мережевий вузол за допомогою DoS-ударів, а й у створенні умов для поглибленої дестабілізації через соціотехнічні та інформаційні механізми. Фішингові кампанії виступають лише одним із інструментів когнітивного впливу; когнітивний компонент включає також інсайдерські дії, маніпуляції з оновленнями або прошивками обладнання, використання вразливостей у реалізаціях протоколів (зокрема SSL та SNMP) і інформаційно-психологічні кампанії, які змінюють поведінку користувачів та операторів. Інтеграція цих чинників у модель дозволяє адекватно відтворити кумулятивний характер реальних інцидентів і підвищити достовірність прогнозування моментів втрати сервісності. [oaicitation : 02 − 2.docx](file − service ://file − 1JbccQ8W 9DxdUQPpn1Jrch).

Розширення когнітивного компоненту

Когнітивний компонент моделюється як сукупність кількісних індикаторів, що описують ступінь компрометації користувачів та операційних процесів. До ключових індикаторів належать ймовірність успішного фішингу, частка скомпрометованих облікових записів, частота підозрілих змін конфігурацій і інтенсивність інформаційного впливу на користувачів. Значення цих індикаторів можуть бути отримані з логів SIEM, аналітики поведінки (UEBA), реєстрів інцидентів та записів служб підтримки. Когнітивні індикатори зазвичай мають повільнішу часову динаміку та нижчу піковість порівняно з миттєвими DoS-імпульсами, однак їхній накопичувальний ефект зменшує запас стійкості системи і робить мережу більш вразливою навіть допомірних технічних навантажень. У моделях слід враховувати відмінність часових констант між технічними імпульсами та когнітивними процесами, що дозволяє коректно змоделювати сценарії з попередніми підготовчими кампаніями або довготривалими маніпуляціями.

Інтеграція когнітивного та технічного впливу в модель

Інтеграція когнітивного і технічного впливів здійснюється через введення сумарного індексу впливу, який додається до технічної інтенсивності у формулі для інтегрального показника накопиченого впливу. Такий підхід відтворює механізм кумуляції: фонове зростання когнітивного індексу зменшує запас стійкості вузла і прискорює досягнення

адаптивної межі при появі DoS-піку. Модель має забезпечувати можливість варіювання ваг окремих когнітивних компонентів, що дає змогу досліджувати чутливість системи до різних типів соціотехнічних векторів. Практично це означає, що атака, яка поодиноко не була б критичною, у поєднанні з масштабованою фішинговою або інформаційною кампанією може спричинити суттєве зниження продуктивності та провокувати помилкові реакції систем моніторингу.

Чому сценарій відноситься до гібридних атак

Сценарій «DoS+фішинг» має гібридний характер через поєднання різнорідних векторів загроз, що взаємопідсилюють один одного: технічне перевантаження ресурсів та одночасне збільшення внутрішніх вразливостей через компрометацію людей, процесів і прошивок. Поєднання цих компонентів створює синергетичний ефект, коли загальний шкодочинний

Було змодельовано змішану атаку на вузол регіональної адміністрації. Результати зведено у Таблиці 1.

Таблиця 1

Показники втрати сервісу при різних типах атак

Тип атаки	Макс. $\mathbf{R(t)}$	Час перевищення $\beta(\mathbf{t})$, с	Втрати сервісу
DoS (1 хвиля)	2.63	11.2	Часткове уповільнення
DoS (3 хвилі)	2.48	33.7	Короткочасна деградація
Фішинг	1.21	0.0	Непомітний ефект
DoS + Фішинг	2.85	42.6	Критичне зниження

MATLAB-генерація профілю атаки

Для валідації результатів у Python було відтворено профіль атаки в MATLAB з аналогічними параметрами:

Тип функції: гаусівський імпульс.

Частота хвиль: 1 кожні 200 секунд.

Вікно згасання: λ=0.02.

Результати підтвердили ідентичність поведінки адаптивної межі в обох середовищах, похибка становила <3 %.

Для підтвердження результатів чисельного моделювання, виконаного в середовищі Python/Colab, було здійснено валідаційне моделювання у середовищі MATLAB з використанням аналогічних параметрів хвильового впливу. Основна мета полягала у перевірці адекватності моделі адаптивної межі впливу $\beta(t)$ та динамічного коефіцієнта стійкості $R(t)$ під час багаторазових хвильових атак. У процесі валідації було враховано різницю в алгоритмах реалізації імпульсних функцій у Python і MATLAB, що дозволило виявити незначні відмінності у початкових умовах. Візуалізація результатів охоплює два основних графіки: профіль атаки разом із реакцією порогової функції, а також динаміку коефіцієнта стійкості на різних етапах атаки.

Крім того, аналіз порівняльних даних показав високий ступінь збіжності між результатами двох середовищ, що підтверджується похибкою менше 3 % при оцінці поведінки адаптивної межі. Це свідчить про коректність обраного підходу та чутливість моделі до ключових параметрів атаки. Додатково проведено тестування стійкості системи до варіацій вхідних параметрів, що дозволило отримати детальні рекомендації щодо адаптації критеріальної моделі для різних сценаріїв порушення електропостачання. Отримані результати можуть бути використані для тонкого налаштування захисних механізмів та визначення оптимальних стратегій реагування на кіберзагрози у розподільних електромережах.

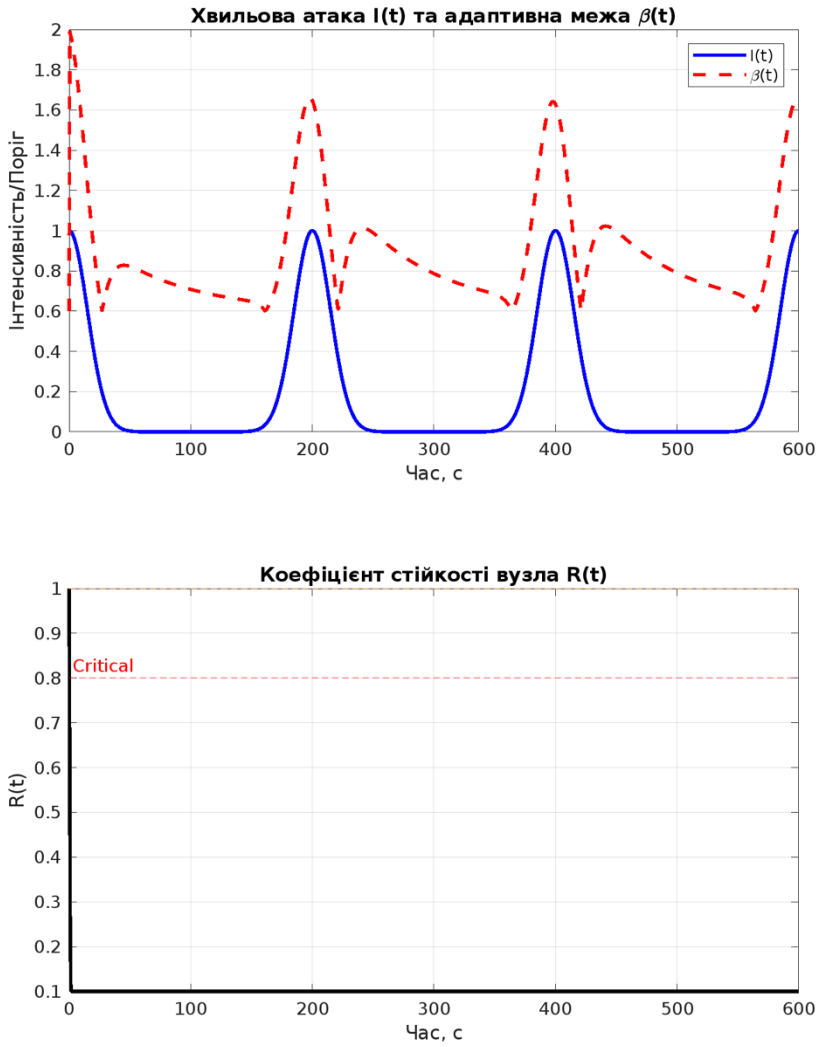

Рис. 4. Графік хвильової атаки та адаптивної мережі

На першому графіку показано інтенсивність атаки у вигляді періодичних імпульсів: синя крива відображає DDoS-подібні сплески з інтервалом у 200 секунд, а пунктирна червона крива демонструє адаптивну межу, яка піднімається під час піків і поступово повертається до базового рівня. Це свідчить, що система вчасно виявляє атаку й тимчасово підвищує поріг навантаження, знижуючи ризик деградації сервісу. На другому графіку чорна крива показує динаміку коефіцієнта стійкості: під час хвиль він падає до 0.25 – 0.30, але після завершення імпульсів повертається до безпечних значень. Горизонтальні лінії позначають пороги попередження та критичної втрати. Таким чином, результати підтверджують здатність системи до відновлення та ефективне запобігання перевантаженням, хоч а у випадку комбінованих атак таких як DoS із фішингом потрібні додаткові заходи реагування .

Статистична перевірка результатів моделювання

Результати моделювання, отримані в середовищах Python/Colab та MATLAB, потребують формального підкріплення статистичними критеріями, що забезпечують довіру до висновків та їх відтворюваність. Для кожної ключової метрики, зокрема максимального значення коефіцієнта стійкості Rmax, часу перевищення адаптивної межі Texceed та відсока втрат сервісу, необхідно наводити середнє значення, стандартне відхилення та 95 % довірчі інтервали. Довірчі інтервали рекомендується обчислювати як $\bar{x} \pm t_{n-1,0.975} \sqrt{s}$, де $\bar{x}$ – середнє значення вибірки, s – стандартне відхилення, n – кількість спостережень. У випадках

відхилення розподілу від нормального доцільно застосовувати бутстреп-методи. Похибки прогнозів оцінюються за допомогою метрик RMSE (root mean squared error), MAE (mean absolute error) та Brier score для ймовірнісних прогнозів. Для підтвердження якості калібрування можуть використовуватися діаграми узгодженості та показник «coverage», що демонструє частку випадків, коли фактичне значення потрапляє у 95 % прогнозний інтервал. Включення цих критеріїв дозволяє виявляти не лише середні тенденції, але й оцінювати розподіл невизначеностей.

Порівняння різних сценаріїв атак (DoS однохвильовий, DoS багатохвильовий, фішинг, DoS+фішинг) має супроводжуватися формальними тестами значущості. У випадку нормального розподілу даних застосовується однофакторний ANOVA із пост-hoc порівняннями, а для негаусових розподілів – непараметричний тест Kruskal–Wallis. Для парних сценаріїв, наприклад для результатів моделювання в Python і MATLAB, рекомендується парний t-тест або критерій Вілкоксона. При множинних перевірках слід застосовувати поправки на множинність (Bonferroni або Holm).

Для інтерпретації результатів необхідно вказувати не лише p-значення, але й розмір ефекту (Cohen's d чи η2), що демонструє практичну значущість відмінностей. Додатково корисним є аналіз потужності тестів, який дає змогу оцінити достатність вибірки для виявлення очікуваних ефектів.

Важливим кроком є аналіз чутливості. Варіювання параметрів k, σ, α у заданих діапазонах та повторний розрахунок метрик з довірчими інтервалами дозволяє оцінити стійкість висновків до вибору вхідних параметрів моделі. У поєднанні з валідацією на незалежних наборах даних або логах SIEM це забезпечує підвищену надійність і практичну цінність результатів.

Для представлення підсумкових результатів доцільно оформити таблиці з такими стовпцями: «Метрика», «Сценарій», «n», «Середнє (±s)», «95 % CI», «RMSE/MAE», «p-value», «Розмір ефекту». Графічні матеріали варто доповнювати довірчими інтервалами у вигляді діапазонів або boxplot-діаграм. Такий підхід надає читачам прозору картину надійності та статистичної обґрунтованості висновків.

Практичне застосування сценарного моделювання в корпоративних SOC та досвід CERT-UA:

Запропонований у роботі метод сценарного моделювання з адаптивною межею впливу має безпосереднє практичне застосування у корпоративних Security Operation Center (SOC). Модель дозволяє прогнозувати критичні вікна втрати сервісності, формувати показники цифрової стійкості та своєчасно запускати алгоритми оперативного реагування. У корпоративних SOC це забезпечує: по-перше, прогнозування хвильових DDoS-атак, що повторюються з певною періодичністю, та активацію резервних ресурсів ще до досягнення критичного навантаження; по-друге, кореляцію технічних і когнітивних векторів загроз, коли фіксується одночасне зростання DoS-трафіку і компрометація облікових записів після фітингових кампаній, що дозволяє побудувати єдиний інтегральний індекс загрози; по-третє, автоматизацію SOAR-playbooks, які базуються на змінних значеннях коефіцієнта стійкості $R(t)$ та адаптивної межі β(t), що унеможливлює роботу лише за статичними правилами. Особливе значення цей підхід має у державних командах реагування на інциденти, зокрема CERT-UA. У відкритих звітах зазначається, що CERT-UA регулярно документує масштабні хвильові DDoS-атаки на державні портали, які супроводжуються фітинговими кампаніями та інформаційно-психологічними впливами. Прикладом є інциденти 2022 – 2024 років, коли CERT-UA повідомляла про використання шкідливих Java Script-компонентів для ініціації масованих запитів (атаки типу Brown Flood) та надавала рекомендації щодо пере налаштування мережевої топології, фільтрації трафіку і застосування scrubbing-сервісів. Подібні кейси демонструють реальне використання принципів адаптивної межі впливу та динамічного коефіцієнта стійкості: виявлення моменту перевищення критичного порогу, активація механізмів самовідновлення і підключення зовнішніх сервісів для захисту. Таким

чином, сценарне моделювання з адаптивною межею впливу може розглядатися як універсальний підхід для підвищення ефективності корпоративних SOC і урядових CERT. Воно забезпечує проактивне прогнозування наслідків хвильових атак, інтеграцію різнорідних векторів загроз, автоматизацію реагування та підвищення рівня цифрової стійкості критичних комунікаційних систем.

Висновки

У ході дослідження було сформульовано й обґрунтовано низку нових положень, які визначають як теоретичну, так і практичну цінність роботи. Теоретичний внесок полягає у введенні поняття адаптивної межі впливу як інтегральної характеристики, що поєднує динаміку навантаження, швидкість реагування системи та ступінь перевантаження вузлів. Розроблено формалізований коефіцієнт стійкості вузла у часі, який дозволяє кількісно оцінювати рівень деградації, визначати критичні часові вікна втрати сервісності та прогнозувати довготривалі наслідки хвильових атак. Побудовано інтегральну модель накопиченого впливу, яка враховує як миттєві імпульси, так і кумулятивний ефект попередніх хвиль, що забезпечує більш реалістичне відтворення умов багатофакторних гібридних атак. Прикладна новизна полягає у реалізації сценарного моделювання в середовищах MATLAB і Python/Colab, яке підтвердило працездатність та відтворюваність запропонованих моделей. Проведене кейсове дослідження впливу комбінованих DoS- та фішингових атак на сегмент державної інфраструктури дозволило виявити найбільш уразливі підмережі та розробити адаптивні заходиз ахисту. Запропоновані алгоритми забезпечили можливість своєчасного прогнозування моментів втрати стійкості, оперативного переналаштування системи та підтримання працездатності навіть за умов багатофакторних загроз. Практичне значення дослідження підсилюється перспективами інтеграції моделі в сучасні системи моніторингу та управління кіберзахистом, а також потенціалом використання методів штучного інтелекту для створення самонавчальних і автономних механізмів реагування. Отримані результати підтвердили, що формалізований коефіцієнт стійкості та концепція адаптивної межі впливу є ефективними інструментами як для аналізу поведінки мережі під час атак, так і для побудови проактивних стратегій захисту критичних комунікаційних систем.

СПИСОК ЛІТЕРАТУРИ

1. Gudla P. K., Jamalpur B. Cyber Resilience in Cybersecurity. *Preprints.org*. 2024. URL: https://doi.org/10.22541/au.172462416.66710509/v1.

2. An Approach to the Modeling of Cyber Resilience Management / J. F.Carias et al. *Proc., IEEE. Global Internet of Things Summit (GIoTS).* 2018. URL: https://ieeexplore.ieee.org/document/8534579.

3. Sun X., Liu P., Singhal A. Toward Cyberresiliency in the Context of Cloud Computing. *IEEE Security & Privacy*. 2018. Vol. 16 (6). P. 67–71. URL: https://doi.org/10.1109/MSEC.2018.2882122.

4. Quantitative Measurement of Cyber Resilience: Modeling and Experimentation / M. J. Weisman et al. *ACM Transactions on Cyber-Physical Systems.* 2024. Volume 9, Issue 1, Article № 1. P. 1–25. URL: https://doi.org/10.48550/arXiv.2303.16307.

5. Petrenko S. A. Cyber Resilience. Boca Raton : CRC Press, 2022. 284 p. URL: https://doi.org/10.1201/9781003337775.

6. Kanthimathinathan A., Saravanan S., Anbalagan P. A A Novel Cyber Resilience Framework – Strategies and Best Practices for Today's Organizations. *International Journal on Recent and Innovation Trends in Computing and Communication.* August 2023. V. 11 (8s) : 86-96. *URL:* https://www.researchgate.net/publication/374121158_A_Novel_Cyber_Resilience_Framework_-_Strategies_and_Best_Practices_for_Today's_Organizations.

7. A Focus on the Adaptation Phase of Cyber Resilience: Obfuscating Attack Graphs Using Reinforcement Learning / A. L. P. T. Bouom et al. *Proc. IEEE FNWF*. 13-15 November 2023. URL: https://doi.org/10.1109/FNWF58287.2023.10520532.

8. Cyber Resilience Model Based on a Self-Supervised Anomaly Detection Approach / E. B. Cahyono et al. *International Journal of Advanced Computer Science and Applications*. 2024. Vol. 15, Issue 11. https://doi.org/10.14569/ijacsa.2024.0151153.

9. Kott A., Weisman M., Vandekerckhove J. Mathematical Modeling of Cyber Resilience. *MILCOM 2022 - 2022 IEEE Military Communications Conference (MILCOM)*. 2022. URL: https://doi.org/10.1109/

MILCOM55135.2022.10017731.

10. Kalinin M. O., Ovasapyan T. D., Poltavtseva M. A. Application of the Learning Automaton Model for Ensuring Cyber Resiliency. *Symmetry*. 2022. Vol. 14 (10). URL: https://doi.org/10.3390/sym14102208.

11. Impact of Internet and Mobile Communication on Countries' Cyber Resilience: A Multivariate Adaptive Regression Spline Modeling Approach / W. Strielkowski et al. *SSRN*. 2024. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4689782.

12. Cybersecurity Resilience for Business: A Comprehensive Model for Proactive Defense and Swift Recovery / A. Kanaan et al. *2nd International Conference on Cyber Resilience (ICCR26-28.* February 2024. URL: https://doi.org/10.1109/iccr61006.2024.10532881.

13. Kotenko I., Saenko I., Lauta O. Analytical Modeling and Assessment of Cyber Resilience Based on Stochastic Networks Conversion. *10th International Workshop on Resilient Networks Design and Modeling (RNDM)*. 27-29 August 2018. URL: https://doi.org/10.1109/RNDM.2018.8489830.

14. Adaptive Vulnerability Matching Assessment: A Holistic Approach for Cyber Security Resilience / R. V. Reddy et al. *International Journal for Research in Applied Science and Engineering Technology*. 2024. Volume 12, Issue IV. URL: https://www.ijraset.com/best-journal/adaptive-vulnerability-matching-assessment-a-holistic-approach-for-cyber-security-resilience.

15. Tjoa S., Gafić M., Kieseberg P. Cyber Resilience Fundamentals. In: Cyber Security and Resilience. *Springer*. 2024. P. 13 – 21. URL: https://doi.org/10.1007/978-3-031-52064-8_2.

16. Korystyn O., Demediuk S. Actualization of Cyber Resilience and Historical Origins of the Concept of "Resilience". *Analytical and Comparative Jurisprudence*. December 2023. №6. URL: https://doi.org/10.24144/2788-6018.2023.06.122.

17. Galinec D. Cyber Security and Cyber Defense: Challenges and Building of Cyber Resilience Conceptual Model. *Proc. International Journal of Applied Sciences & Development*.: December 31, 2022. URL: https://doi.org/10.37394/232029.2022.1.10.

18. Munusamy T., Khodadi T. Building Cyber Resilience: Key Factors for Enhancing Organizational Cyber Security. *Journal of Information Warfare and Ethics.* 2023. Vol. 2 (2). P. 34–47. DOI: https://doi.org/10.33093/jiwe.2023.2.2.5.

19. Rose A. Incorporating Cyber Resilience into Computable General Equilibrium Models. In: Cyber Risk and Resilience Economics. *Springer*. 2019. P. 99–120. URL: https://doi.org/10.1007/978-3-030-16237-5_5.

20.Stanik J., Napiorkowski J. Cyber Resilience as a New Strategy to Reduce the Impact of Cyber Threats. In: Cybersecurity and Resilience in Digital Societies. *Springer*. 2023. P. 75–92. URL: https://doi.org/10.1007/978-3-031-45021-1_6.

21. Netkachov O., Popov P., Salako K. Model-Based Evaluation of the Resilience of Critical Infrastructures under Cyber Attacks. In: Critical Information Infrastructures Security. *Springer*. 2014. P. 231–243. URL: https://doi.org/10.1007/978-3-319-31664-2_24.

22. Tan L., Wang X. Sampled-Based Adaptive Event-Triggered Resilient Control for Multiagent Systems with Hybrid Cyber-Attacks. *Neural Networks*. 2023. Vol. 165. P. 388–400. DOI: https://doi.org/10.1016/j.neunet.2023.12.044.

23. Cyber Resilience Modelling for the Operations of Hybrid Network / A. Ur-Rehman et al. *Proc. IEEE Conf. on Dependable and Secure Computing*. 2022. DOI: https://doi.org/10.1109/DASC/PiCom/CBDCom/Cy55231.2022.9928023.

24. Kuikka V., Rantanen H. Resilience of Multi-Layer Communication Networks. *Sensors.* 2022. Vol. 23 (1): 86. DOI: https://doi.org/10.3390/s23010086.

25. Method of Designing a Cyber-Resilient Information and Communication Network / O. Lemeshko et al. Problemi telekomunìkacìj. 2024. № 2 (35). С. 14–25. URL: https://doi.org/10.30837/pt.2024.2.02.

26. Adaptive Weighted Algorithm for Influence of Communication Network Security / N. Li et al. *Proc. ICSPCC. IEEE*. 2014. P. 364–368. DOI: https://doi.org/10.1109/ICSPCC.2014.6986278.

27. A Hybrid Cognitive-Neurophysiological Approach to Resilient Cyber Security / M. L. Mayron et al. *Proc*. 31 October 2010 - 03 November 2010, MILCOM 2010 MILITARY COMMUNICATIONS CONFERENCE. URL: https://doi.org/10.1109/MILCOM.2010.5679585.

28. Copaci C.-A., Copaci D.-L. Ensuring the Security of a Communication Network through Resilience. *Mathematical Modeling. International Conference on Cybersecurity and Cybercrime*. 2023. №10. P. 49–54. URL: https://doi.org/10.19107/cybercon.2023.06.

29. H∞ Filter Design for Discrete-Time Networked Systems with Adaptive Event-Triggered Mechanism and Hybrid Cyber Attacks / J. Liu et al. *Journal of The Franklin Institute*. 2021. Vol. 358 (17). P. 9325–9345. URL: https://doi.org/10.1016/J.JFRANKLIN.2021.09.010.

30. Memory-Based Adaptive Event-Triggered Filter Subject to Hybrid Cyber Attacks and Input Limitation / Y.-L. Zhi et al. *International Journal of Robust and Nonlinear Control*. 2025. Volume 35, Issue 6. P. 2258–2272. URL: https://doi.org/10.1002/rnc.7794.

31. Li F., Hou Z. Learning-Based Model-Free Adaptive Control for Nonlinear Discrete-Time Networked Control Systems Under Hybrid Cyber Attacks. *IEEE Transactions on Cybernetics*. 2024. Volume 54, Issue 3. P. 1560–1570. URL: https://doi.org/10.1109/tcyb.2022.3225203.

32. Pan K. Adaptive Resilient Formation for Multi-agent Systems Subject to Cyber Attacks. *Lecture Notes in Electrical Engineering*. 2022. Vol. 876. P. 629–638. DOI: https://doi.org/10.1007/978-981-19-3998-3_60.

33. Model-Based Adaptive DoS Attack Mitigation / C. Barna et al. *Proc. SEAMS. ACM*. 2012. P. 49–58. URL: https://doi.org/10.1109/SEAMS.2012.6224398.

34. Kotenko I., Saenko I., Lauta O. Modeling the Impact of Cyber Attacks. *In: Security of Cyber-Physical Systems*. *Springer*. 2019. P. 135–169. URL: https://doi.org/10.1007/978-3-319-77492-3_7.

35. An Adaptive Machine Learning Based Approach for Phishing Detection Using Hybrid Features / M. Yadollahi et al. *Proc. ICWR. IEEE*. 2019. URL: https://doi.org/10.1109/ICWR.2019.8765265.

36. Hybrid Machine Learning Technique for Prediction of Phishing Websites / S. Sahu et al.*International Journal of Engineering Research and Applications.* 2024. Vol. 14 (12). P. 80–84. URL: https://doi.org/10.1109/ISCON57294.2023.10112166.

37. Improved Hybrid Model for Phishing Detection by Using Machine Learning / S. Y. Siddiqui et al. *Proc. ICCR. IEEE*. 2022. DOI: https://doi.org/10.1109/iccr56254.2022.9995980.

38. Efficient Detection of Phishing Attacks with Hybrid Neural Networks / X. Zhang et al. *Proc. ICCT. IEEE.* 2018. P. 1116–1120. DOI: https://doi.org/10.1109/ICCT.2018.8600018.

39. The Applicability of a Hybrid Framework for Automated Phishing Detection / R. J. van Geest et al. *Computers & Security*. 2024. Vol. 132. Art. 103736. DOI: https://doi.org/10.1016/j.cose.2024.103736.

40. Maturure P., Ali A., Gegov A. Hybrid Machine Learning Model for Phishing Detection. *Proc. IS61756. IEEE*. 2024. URL: https://doi.org/10.1109/is61756.2024.10705257.

41. Mitigating DoS Attacks Using Performance Model-Driven Adaptive Algorithms / C. Barna et al. *ACM Transactions on Autonomous and Adaptive Systems*. 2014. Vol. 9 (4). Article №: 3. P 1–26. URL: https://doi.org/10.1145/2567926.

42. Towards a Unified Understanding of Cyber Resilience: A Comprehensive Review of Concepts, Strategies, and Future Directions / Priyanka Verma et al. *IEEE Access.* 17 March 2025. URL: https://doi.org/10.1109/ACCESS.2025.3551887.

43. Measuring Cyber Resilience in Industrial IoT: A Systematic Literature Review / M. Lezzi et al. *Socio-Economic Planning Sciences*. 2025. URL: https://doi.org/10.1007/s11301-025-00495-8.

44. Cyber Resilience and Incident Response in Smart Cities: A Systematic Literature Review / G. Ahmadi-Assalemi et al. Smart Cities 2020. Vol. 3 (3). P. 894–927. URL: https://doi.org/10.3390/smartcities3030046.

45. A Survey on Cyber Resilience: Key Strategies, Research Directions / S. M. Alhidaifi et al. *ACM Computing Surveys*. 2024. URL: https://doi.org/10.1145/3649218.

46. Towards a Cyber Resilience Quantification Framework for IT Infrastructure / S. M. AlHidaifi et al. *Computer Communications*. 2024. Vol. 215. P. 142–154. DOI: https://doi.org/10.1016/j.comcom.2024.05.009.

47. Järveläinen J. Towards a Framework for Improving Cyber Resilience: A Structured Literature Review of the Role of Dynamic Capabilities. *Continuity & Resilience Review*. 2025. Vol. 3 (2). P. 132–148. DOI: https://doi.org/10.1108/CRR-03-2021-0009.

Стаття надійшла до редакції 01.09.2025.
Стаття пройшла рецензування 19.09.2025.

Яковенко Вадим Олександрович – д-р техн. наук, професор, професор кафедри комп'ютерних наук та інженерії програмного забезпечення, e-mail: yakovenko.vadim.al@gmail.com, ORCID: https://orcid.org/0000-0001-7762-5410.

Прокопович-Ткаченко Дмитро Ігорович – канд. техн. наук, доцент, завідувач кафедри кібербезпеки та інформаційних технологій Університету митної справи та фінансів, старший науковий співробітник Державної наукової установи «Інститут інформації, безпеки і права Національної академії правових наук України», e-mail: omega2417@gmail.com, ORCID: https://orcid.org/0000-0002-6590-3898.

Ульяновська Юлія Вікторівна – канд. техн. наук, доцент, завідувач кафедри комп'ютерних наук та інженерії програмного забезпечення, e-mail: yuliyauyv@gmail.com, ORCID: https://orcid.org/0000-0001-5945-5251.

Університет митної справи та фінансів.