КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.29.884
УДК 303.732:004.056.5:004.02

Долгова Наталя Геннадіївна
к.т.н., доцент,
доцент кафедри кібербезпеки та інформаційних технологій
Харківський національний економічний університет імені Семена Кузнеця, Харків, Україна
ORCID ID: 0000-0002-8950-8200
natalya.dolgova@hneu.net

Шаповалова Олена Олександрівна
к.т.н., доцент,
доцент кафедри кібербезпеки та інформаційних технологій
Харківський національний економічний університет імені Семена Кузнеця, Харків, Україна
ORCID ID: 0000-0003-4566-6634
olena.shapovalova@hneu.net

Солодовник Ганна Валеріївна
к.т.н., доцент,
доцент кафедри кібербезпеки та інформаційних технологій
Харківський національний економічний університет імені Семена Кузнеця, Харків, Україна
ORCID ID: 0000-0001-6323-5083
ganna.solodovnyk@m.hneu.edu.ua

СИСТЕМА ПІДТРИМКИ РІШЕНЬ У ЗАВДАННЯХ ПРОЕКТУВАННЯ КІБЕРБЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. У статті розглянуто проблему прийняття обґрунтованих архітектурних рішень у сфері кіберзахисту об'єктів критичної інфраструктури в умовах зростаючих загроз, обмеженості ресурсів та складної міждисциплінарної структури систем. Проаналізовано сучасні підходи до побудови систем захисту, зокрема концепцію Zero Trust Architecture, методи Explainable AI та ризик-орієнтовані моделі, що застосовуються для виявлення та реагування на загрози у висококритичних середовищах. Визначено, що наявні рішення не забезпечують достатнього рівня адаптивності та не враховують сукупність взаємозалежних критеріїв, що впливають на ефективність архітектури системи захисту. Метою дослідження є створення інтегрованої системи підтримки прийняття рішень, яка враховує багатовимірний характер задачі кіберзахисту та дозволяє здійснювати вибір оптимальної архітектури з урахуванням технічних, організаційних та економічних факторів. Запропоновано багатокритеріальний підхід на основі MAI, доповнений модулем структурного аналізу впливів та механізмом динамічного оновлення ваг критеріїв відповідно до зміни ризиків і загроз. Формалізовано критерії оцінювання ефективності архітектур захисту (MTTD, MTTR, рівень виявлення загроз, автоматизація, вартість, відповідність політикам тощо) з урахуванням їх функціональних характеристик та типів функцій корисності. Практична реалізація СППР здійснена з використанням Python та бібліотеки Streamlit, що забезпечує інтерактивну взаємодію користувача, побудову матриць порівнянь, візуалізацію причинно-наслідкових зв'язків і генерацію ранжованих рішень у зручному форматі. У статті представлено архітектуру програмного модуля, приклад функціонування системи на базі трьох архітектурних моделей (класична, ZTA, хмарна) та обґрунтовано вибір альтернативи в контексті критичної інфраструктури. Запропонований підхід дозволяє підвищити обґрунтованість і прозорість рішень у сфері кіберзахисту, а також адаптувати систему до реального середовища функціонування, забезпечуючи стійкість до складних багатовекторних атак. Отримані результати можуть бути застосовані для автоматизованого проєктування архітектури безпеки об'єктів енергетики, транспорту, телекомунікацій та інших критичних секторів.

Ключові слова: система підтримки прийняття рішень; кіберзахист; критична інфраструктура; системний підхід, багатокритеріальний аналіз; Zero Trust; Explainable AI; Cross-Impact Matrix; MAI.

ВСТУП

На сучасному етапі розвитку інформаційного суспільства критично важлива інфраструктура все глибше інтегрується з цифровими технологіями, що, з одного боку, забезпечує підвищення ефективності та автоматизації виробничих і управлінських процесів, а з іншого — значно підвищує рівень її вразливості до різноманітних кіберзагроз. До об'єктів КВІ належать енергетичні системи, транспорт, медичні установи, системи водопостачання, зв'язку та державного управління, від яких безпосередньо залежить стабільне функціонування держави та добробут громадян. У контексті діджиталізації ці об'єкти дедалі частіше стають мішенню для цілеспрямованих атак з боку організованих кіберзлочинних груп, державних або воєнізованих хакерських підрозділів, з використанням новітніх засобів ураження.

Особливої актуальності проблема кіберзахисту КВІ набуває у воєнний час, коли об'єкти інфраструктури є цілями не лише фізичних, а й кібернетичних атак. Зростання складності кіберфізичних систем, що поєднують інформаційні та операційні технології (IT/OT), поширення багатовекторних атак типу APT (Advanced Persistent Threats), Zero-Day, атак через ланцюги постачання (Supply Chain Attacks) та інші — вимагає від захисних систем не лише виявлення інцидентів, а й гнучкої, адаптивної протидії в реальному часі. З огляду на високу ціну простою або виведення з ладу таких об'єктів, забезпечення їх надійного функціонування навіть за умов ворожого впливу є пріоритетним завданням державної безпеки.

Традиційні централізовані підходи до побудови архітектури кіберзахисту вже не відповідають вимогам часу. Вони часто не забезпечують необхідного рівня масштабованості, стійкості до складних сценаріїв атак і динамічного адаптування до змін зовнішнього середовища. Впровадження інноваційних рішень, таких як Zero Trust Architecture, системи з пояснюваним штучним інтелектом (Explainable AI), SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation and Response), вимагає комплексного системного підходу. Йдеться про проектування гнучких архітектур безпеки, які поєднують сучасні технології з урахуванням організаційної структури, наявних ресурсів, нормативних вимог та ризиків.

Постановка проблеми. У науковій та прикладній літературі спостерігається значний розрив між концептуальними підходами до проєктування систем кіберзахисту критичної інфраструктури та практичними інструментами підтримки рішень, які б дозволяли приймати ґрунтовні архітектурні рішення в умовах багатофакторності, невизначеності та динамічних змін середовища. Існуючі моделі здебільше фокусуються або на статичному аналізі ризиків, або на реалізації окремих технічних елементів захисту, але при цьому залишають без урахування цілісність міжкомпонентних взаємозв'язків. Відсутність формалізованих процедур, які б об'єднували знання про загрози, обмеження ресурсів, специфіку інфраструктури й очікувані сценарії атак, суттєво ускладнює завдання побудови ефективної та адаптивної системи захисту.

В умовах постійно зростаючої складності цифрового середовища особливе значення набуває розробка інструментів підтримки прийняття рішень для вибору найбільш ефективних архітектур кібербезпеки. Такі інструменти мають враховувати багатофакторність оцінювання, зокрема технічну ефективність, витрати на впровадження, оперативну адаптивність до загроз, відповідність галузевим стандартам і можливість масштабування. Найбільш перспективними виглядають моделі, побудовані на основі методів системного аналізу, багатокритеріальної оптимізації та використання штучного інтелекту — як для виявлення загроз, так і для синтезу стійких архітектур.

У зв'язку з цим постає завдання розробки спеціалізованої системи підтримки прийняття рішень, яка дозволяє здійснювати багатокритеріальну оцінку можливих архітектур і надавати допомогу у виборі кращого варіанта з урахуванням технічних характеристик, операційних ризиків, економічних обмежень і поточної кіберзагрозової ситуації. Така система повинна бути гнучкою, динамічно адаптивною та придатною до практичного застосування в умовах обмежених даних і високої критичності.

Таким чином, ефективне проєктування та впровадження архітектур кіберзахисту критичної інфраструктури вимагає міждисциплінарного підходу, що поєднує знання з інформаційної безпеки, системного аналізу, інженерії рішень та сучасних технологій обробки даних. У цьому контексті запропоноване дослідження спрямоване на розробку методології та прототипу системи підтримки прийняття рішень щодо вибору оптимальної архітектури кіберзахисту для об'єктів критичної інфраструктури на основі багатокритеріального аналізу, актуальних даних про кіберзагрози та наявні ресурси.

Аналіз останніх досліджень і публікацій. У наукових дослідженнях останніх років спостерігається зростання інтересу до трансформації архітектур кіберзахисту критичної інфраструктури відповідно до динамічного характеру загроз.

Одним із найбільш структурованих напрямів розвитку вважається Zero Trust Architecture (ZTA), що базується на постійному контролі та верифікації користувачів і пристроїв незалежно від їхнього місцезнаходження в мережі. У роботах [1], [2] розроблено відповідні фреймворки, які адаптують концепцію ZTA до середовищ із обмеженими ресурсами, що характерно для об'єктів енергетики, транспорту та інших сегментів критичної інфраструктури. При цьому окреслено ключові компоненти архітектури, а саме мікросегментацію, динамічне управління доступом, контекстну автентифікацію.

Паралельно, у системах виявлення вторгнень набуває розвитку інтеграція технологій Explainable AI (XAI). Як показано у [3], інтерпретованість рішень відіграє вирішальну роль у забезпеченні довіри до автоматизованих систем безпеки, особливо у висококритичних середовищах на кшталт SCADA або ICS.

У роботі [4] представлено реалізацію процесно-орієнтованої моделі XAI для OT/ICS-систем, що дозволяє суттєво підвищити ефективність детекції складних загроз типу APT завдяки врахуванню контексту фізичних процесів.

Разом з тим, критичний огляд актуальних реалізацій ZTA у контексті інфраструктури США [5] засвідчує низку обмежень: зокрема, надмірна зосередженість на контролі доступу без достатньої уваги до механізмів виявлення та реагування, що знижує стійкість до складних мультивекторних атак. Крім того, підкреслено обмежену адаптивність таких систем у динамічному середовищі.

Аналіз джерел також демонструє загальну відсутність формалізованих підходів до вибору архітектури захисту, які враховували б не лише концептуальну модель, але й реальні умови функціонування об'єкта — тип загроз, обмеження ресурсів, можливості інтеграції модулів, масштабованість. У [2] та [5] зазначено, що сучасні підходи практично не містять моделей підтримки прийняття архітектурних рішень, здатних забезпечити адаптацію до змін зовнішнього середовища.

На цьому тлі важливо виділити дослідження, що орієнтовані на урахування української специфіки. У [6] проведено аналіз специфічних загроз, з якими стикаються об'єкти критичної інфраструктури в умовах гібридної війни. Наголошено на необхідності поєднання технічних, організаційних і поведінкових компонентів у побудові архітектури захисту. У [7] запропоновано методику оцінювання кіберзахищеності з урахуванням особливостей об'єкта, топології та сценаріїв порушення функціонування, що дозволяє ідентифікувати вразливі елементи у поточних архітектурах.

Розвиток XAI-методів у сфері інтелектуального моніторингу розглянуто в [8], де підтверджено, що поєднання машинного навчання з інтерпретованими моделями забезпечує не лише високу точність, а й прозорість прийняття рішень у режимі реального часу — що особливо важливо для операторів критичних систем.

Водночас у [9] запропоновано математичну модель оцінки ризику функціонування об'єктів критичної інфраструктури на основі нечіткої логіки, що дозволяє враховувати невизначеність, властиву реальним сценаріям. У цьому ж дослідженні наголошено на потребі інтеграції ризик-орієнтованого аналізу, систем виявлення загроз (XAI-IDS) і принципів ZTA в єдину систему підтримки прийняття архітектурних рішень (СППР).

Таким чином, результати аналізу наявних досліджень свідчать про наявність зрілих концептуальних підходів до архітектури захисту (ZTA, XAI, OT-орієнтовані IDS), однак також фіксують істотний брак комплексної методології, яка б дозволила здійснювати адаптивний вибір архітектурного рішення з урахуванням множинних критеріїв. Відсутність інтегрованої СППР знижує ефективність реалізації політик безпеки, породжуючи ризики фрагментарності та несумісності окремих компонентів.

З вищенаведеного випливає доцільність застосування системного підходу до моделювання архітектури комбінованої системи кіберзахисту. Такий підхід має забезпечити узгодження моделей загроз, структури об'єкта, сценаріїв атак, ресурсних обмежень і функціональних вимог у межах єдиної багатоаспектної системи підтримки рішень. Це створює підґрунтя для формування надійних, адаптивних і практично застосовних архітектур захисту критичної інфраструктури.

Мета статті. Метою статті є розробка системного підходу до підтримки архітектурних рішень у сфері кіберзахисту об'єктів критичної інфраструктури шляхом створення інтегрованої системи підтримки прийняття рішень, яка враховує актуальні загрози, функціональні вимоги, обмеження ресурсів і специфіку інфраструктури.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Проблема вибору архітектури системи кіберзахисту об'єктів критичної інфраструктури формалізується як задача багатокритеріального вибору серед дискретного набору альтернатив.

Нехай $A = \{a_1, a_2, \dots, a_m\}$ — множина архітектурних альтернатив,

$F = \{f_1, f_2, \dots, f_n\}$ — сукупність цільових функцій (критеріїв), кожна з яких відображає один із аспектів ефективності рішення.

Узагальнена векторна модель прийняття рішень набуває вигляду:

$$a^* \in A : F(a) = (f_1(a), f_2(a) \dots, f_n(a)). \quad (1)$$

Для переходу до однозначного ранжування використовується агрегована функція корисності:

$$U(a_j) = \sum_{i=1}^{n} w_i * u_i(x_{ij}), \quad (2)$$

де x_{ij} — значення критерію *i* для альтернативи a_i;

$u_i(x_{ij})$ — нормалізована функція корисності;

$w_i \in [0,1]$ — ваговий коефіцієнт, що відображає пріоритетність критерію k_i, $\sum w_i = 1$.

Таким чином, потрібно знайти

$$a^* = arg \max_{a_j \in A} U(a_j) \quad (3)$$

У контексті прийняття рішень щодо архітектури кіберзахисту для об'єктів критичної інфраструктури доцільним є використання багатокритеріальних методів, що дозволяють формалізувати складні вимоги до системи. Вибір методу залежить від характеру критеріїв, доступності даних, рівня визначеності середовища та вимог до прозорості прийняття рішень.

Метод зваженої суми (WSM) [10] є одним з найпростіших та найбільш інтуїтивно зрозумілих; він часто використовується як базовий підхід у задачах з чітко визначеними, кількісними критеріями. Метод ґрунтується на лінійній агрегації нормалізованих значень. Його використання дозволяє швидко обчислити інтегральну оцінку шляхом лінійного поєднання нормалізованих значень за критеріями з урахуванням їхніх ваг.

Зокрема, модель не враховує взаємозалежності між критеріями, не відображає природи конфліктності та не дозволяє працювати з нечіткими чи лінгвістичними оцінками. У складних сценаріях, які вимагають адаптивності та гнучкості, доцільно звертатися до більш складних моделей, що враховують ці особливості.

Наприкалад, метод аналізу ієрархій (Analytic Hierarchy Process, MAI), який передбачає побудову ієрархічної моделі (мета — критерії — альтернативи) та попарне порівняння елементів на кожному рівні [11]. Визначення ваг базується на розрахунку власних векторів матриць порівняння

$$U(a_j) = \sum_{i=1}^{n} w_i * p_{ij}\,, \tag{4}$$

де p_{ij} — локальний пріоритет альтернативи щодо критерію.

На відміну від простої лінійної агрегації, MAI дозволяє гнучко структурувати задачу вибору, розкладаючи її на рівні цілей, критеріїв і підкритеріїв. Він забезпечує можливість порівнювати критерії попарно, що дозволяє глибше врахувати пріоритети в умовах складних взаємозв'язків. Разом із тим, з ростом кількості альтернатив і критеріїв метод стає обчислювально складним, а його результати можуть бути чутливими до суб'єктивності початкових оцінок. Ця обставина обмежує застосування MAI у сценаріях з великою кількістю змінних або нечіткими даними, характерними для динамічного середовища кіберзагроз.

У таких випадках доречним є застосування моделей, що оперують нечіткістю та дозволяють врахувати неоднозначність експертних оцінок, наприклад, нечіткі MCDM-моделі.

У нечітких багатокритеріальних моделях (Fuzzy MCDM) замість чітких (однозначних) чисел використовуються нечіткі числа, які відображають діапазон можливих значень. Найпоширенішим є трикутне нечітке число (TFN — Triangular Fuzzy Number), яке задається трійкою

$$\widetilde{x_{ij}} = x_{ij}^{L}, x_{ij}^{M}, x_{ij}^{U}\,, \tag{5}$$

де x_{ij}^{L} — нижня межа: найменше можливе значення оцінки;

x_{ij}^{M} — модальне значення (середина): найбільш імовірне або бажане значення;

x_{ij}^{U} — верхня межа: найбільше можливе значення оцінки.

Така форма дозволяє враховувати невизначеність або розбіжність експертних оцінок, які не можна подати у вигляді точного значення.

Застосування нечітких моделей [12] є надзвичайно ефективним у тих випадках, коли прийняття рішень супроводжується високим рівнем інформаційної невизначеності, що характерно для задач кібербезпеки в умовах обмежених або суперечливих даних. Основною перевагою цього підходу є здатність інтегрувати якісні, експертні оцінки у формалізовану математичну модель. Це забезпечує гнучкість у роботі з невизначеними

параметрами та дозволяє адаптувати модель до реальних умов функціонування критичної інфраструктури.

Разом з тим, застосування нечітких множин ускладнює розрахунки, оскільки потребує виконання спеціалізованих арифметичних операцій та процедури дефазифікації. Ще однією складністю є необхідність обґрунтованого вибору функцій належності, які безпосередньо впливають на точність і достовірність результатів моделі.

У випадках, коли оцінки за критеріями можуть бути суперечливими або конфліктними, доцільно розглянути інший клас методів — алгоритми наддомінування , зокрема ELECTRE та PROMETHEE. Ці підходи дозволяють здійснювати парні порівняння альтернатив і формувати відношення переваги, що є особливо корисним при вирішенні задач з високою критичністю вимог.

Ці методи оперують не глобальною функцією корисності, а відношенням переваг. Зокрема, у методі ELECTRE будується матриця переваг P_{ij}, на основі якої формується граф домінування. Альтернативи з мінімальним числом домінантів вважаються прийнятними.

Методи ELECTRE та PROMETHEE ефективно вирішують проблеми з конфліктними критеріями, оскільки порівнюють альтернативи попарно й формують відношення переваги, проте обидва припускають, що ваги критеріїв w_i залишаються статичними протягом усього аналізу.

У середовищі кіберзахисту критичної інфраструктури ситуаційні ризики змінюються динамічно (нова вразливість, підвищений пріоритет безперервності сервісу тощо). Це зумовлює потребу в адаптивному коригуванні ваг, коли значущість критеріїв оновлюється у реальному часі залежно від поточного профілю загроз та доступних ресурсів.

У динамічному середовищі можливо моделювання ваг критеріїв як функції від часу та зовнішніх змін:

$$w_i(t+1) = f\big(w_i(t), \Delta R_i(t), Z_i(t)\big), \quad (6)$$

де $\Delta R_i(t)$ — зміна ризику,

$Z_i(t)$ — вплив нових даних (інцидентів, загроз).

Це дозволяє формувати гнучку систему з підтримкою сценаріїв реактивного планування и дає змогу оперативно переорієнтовувати процес прийняття рішень і забезпечувати актуальність альтернативних виборів у швидкоплинних умовах.

Жоден метод не є універсальним — кожен має свої переваги й обмеження залежно від контексту задачі. У межах критичної інфраструктури доцільним є застосування гібридних підходів, які поєднують нечітке моделювання, ієрархічну структуру та адаптивне оновлення ваг.

В даній роботі було обрано гібридний підхід, що поєднує елементи системного аналізу (структурні залежності) з інструментами багатокритеріальної оптимізації.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Системний аналіз (СА) розглядає комплекс об’єктів, процесів та зв’язків як цілісну систему, що має вхідні та вихідні потоки, ієрархію підсистем та цільову функцію. У дослідженнях критичної інфраструктури (КІ) СА дозволяє формалізувати складні міждисциплінарні залежності між кібернетичними й фізичними компонентами та оцінити їх стійкість до загроз. У межах проєктування систем кіберзахисту (СКЗ) СА надає апарат для ідентифікації меж системи та її взаємодії з оточенням; декомпозиції на функціональні модулі та рівні захисту; формулювання багатокритеріальної задачі

оптимізації ресурсів кіберзахисту; аналізу ризиків і послідовного прийняття рішень (Decision Support).

Згідно зі ст. 1 Закону України № 2163-VIII «Про основні засади забезпечення кібербезпеки України» [13], СКЗ — це сукупність організаційно-технічних заходів, процесів, ресурсів та комп'ютерних систем, спрямованих на захист кіберпростору держави й об'єктів КІ від кіберзагроз. У стандартах ISO/IEC 27001:2022 та IEC 62443 СКЗ трактується як інформаційна система управління безпекою (ISMS), що охоплює політики, процедури, технічні та людські ресурси [14],[15]. Додатково, NIST SP 800-82 Rev. 3 для операційних технологій (ОТ) визначає СКЗ як комбінацію захисних механізмів, які реагують на зміни фізичного середовища та загроз кіберпростору [16].

Для КІ під СКЗ будемо розуміти ієрархічно організований комплекс апаратно-програмних засобів, процесів управління, персоналу та правових механізмів, що функціонує з метою забезпечення конфіденційності, цілісності, доступності та цілісності технологічних процесів, які мають критичне значення для суспільства.

Тоді система кіберзахисту критичної інфраструктури — це багаторівнева, модульна й динамічно адаптивна сукупність технічних, програмних та організаційних засобів, яка забезпечує безперервне виявлення, запобігання, реагування та відновлення у разі кіберінцидентів.

Функціональна структура системи кіберзахисту критичної інфраструктури відповідає концепції багаторівневої оборони (*defense-in-depth*) та демонструє узгоджену роботу різних модулів, інструментів і ролей персоналу на кожному рівні захисту від фізичного до хмарного (табл. 1).

Таблиця 1

Елементи функціональної структури СКЗ зі зв'язками між модулями та шарами

Рівень «defense-in-depth»	Ключові модулі	Типові інструменти	Ролі персоналу	Типові загрози
Фізичний рівень	Контроль доступу, безпека майданчика	СКУД, сенсори	Технічна охорона	Несанкціонований фізичний доступ, пошкодження обладнання
Мережевий (периметральний) рівень	Фаєрвол, IDS/IPS, проксі	Cisco, Fortinet, Snort, pfSense, Wazuh	Адміністратор мережі, фахівець IR	DDoS, MitM, Brute Force, Zero-day
Внутрішній рівень (IT-інфраструктура)	Сервери, AD, управління вразливостями	Windows/Linux Hardening, WSUS, DB Firewall	Системний адміністратор, DevOps	Insider Threat, Misconfiguration, Shadow IT
SOC-рівень (оперативне реагування)	Secure SDLC, криптографія, IAM/MFA	PKI, TLS, SAST/DAST, IAM-платформи	Розробник, архітектор безпеки	Malware, Credential stuffing, Social engineering
Організаційний рівень	SIEM, UEBA, SOAR, GRC	Splunk, Elastic, Open-SOAR, Archer	Аналітик SOC, CISO, аудитори	Недотримання політик, відсутність аудиту, помилки персоналу
Хмарна інфраструктура	Резервне копіювання, SaaS-інтеграції	AWS/Azure, API-шлюзи	Архітектор хмари, кінцевий користувач	Ransomware, витік даних через API, збій бекапу

Фізичний рівень є найнижчим рівнем, що охоплює фізичний захист IT-ресурсів, наприклад, серверних кімнат, дата-центрів, мережевих вузлів. Застосовуються системи

контролю доступу, відеонагляд, сенсори та охоронні механізми. Персонал відповідає за фізичну охорону й моніторинг доступу до критичних об'єктів.

Основна мета мережевого рівня полягає в відсіченні зовнішніх атак за допомогою фаєрволів, IDS/IPS-систем і проксі-серверів. Цей рівень реалізує базові фільтраційні функції, сегментацію трафіку й блокування аномальних з'єднань. Інструменти на кшталт Cisco, Fortinet, Snort або pfSense дозволяють ефективно реалізовувати ці задачі. Відповідальними особами є мережеві адміністратори та аналітики інцидентів.

Внутрішній рівень (IT-інфраструктура) охоплює сервери, маршрутизатори, бази даних, CRM/ERP-системи, а також активні дії користувачів. Ризики тут пов'язані з інсайдерами, помилками персоналу, помилковими конфігураціями. Застосовуються засоби централізованого керування, політики доступу, обліку змін та моніторинг активностей. Роль персоналу варіюється від адміністраторів до кінцевих користувачів.

Центральний елемент прийняття рішень у кіберзахисті це SOC-рівень. Він виконує безперервний моніторинг, аналіз поведінки користувачів (UEBA), реагування на інциденти за допомогою SIEM та EDR-платформ (Splunk, Wazuh, ArcSight тощо). Працюють аналітики безпеки, оператори SOC та CISO.

Організаційний рівень забезпечує стратегічне управління, аудит і відповідність регуляторним вимогам. Застосовуються GRC-системи для впровадження політик, процедур, контролів відповідності. Участь беруть регулятори, аудитори, менеджмент безпеки.

Хмарна інфраструктура інтегрує зовнішні сервіси (SaaS, API, хмарні платформи), резервне копіювання та взаємодію між платформами. Особливу роль відіграють архітектори безпеки, які відповідають за шифрування, контроль доступу, аудит API-запитів та відповідність вимогам постачальників.

Рівні функціонують у тісному зв'язку: між ними циркулюють інформаційні потоки, сигнали подій, логи, що у разі аномалії передаються в SOC для аналізу. Виявлення загрози на нижньому рівні (наприклад, фаєрволом) може автоматично ініціювати відповідь на вищому рівні (наприклад, блокування облікового запису через SOAR).

Різні типи загроз (APT, phishing, DDoS) можуть проникати в систему через інтернет, користувачів або хмарні канали, взаємодіяти з такими компонентами, як проксі, бази даних, користувачі та SOC-моніторинг (рис.1). Слабкі місця можуть бути спричинені як зовнішніми атаками, так і внутрішніми загрозами — від навмисних дій інсайдерів до помилок звичайних користувачів. Саме для цього кожен рівень має бути захищений та інтегрований у загальну архітектуру.

Проте побудова навіть найскладнішої системи не гарантує її ефективність без об'єктивного оцінювання. З цією метою доцільно використовувати систему критеріїв оцінювання (Evaluation Criteria System), яка дозволяє оцінити захист у семи ключових вимірах: від здатності протистояти поширеним і цілеспрямованим атакам (C1, C2), до витрат на впровадження (C3), простоти підтримки та обслуговування (C4), швидкості реагування (C5), відповідності стандартам (C6) та оцінки рівня кіберризику (C7).

З огляду на багатовимірний характер оцінювання кіберзахисту, важливо не лише перелічити критерії, а й визначити ступінь їхнього взаємного впливу. Для цього доцільно використати підхід структурного системного аналізу, викладений у роботі [17]. Ця методологія базується на побудові матриці крос-впливів (Cross-Impact Matrix), що дозволяє формалізувати взаємозв'язки між критеріями та ідентифікувати ключові драйвери, залежні фактори та критичні точки управління [18].

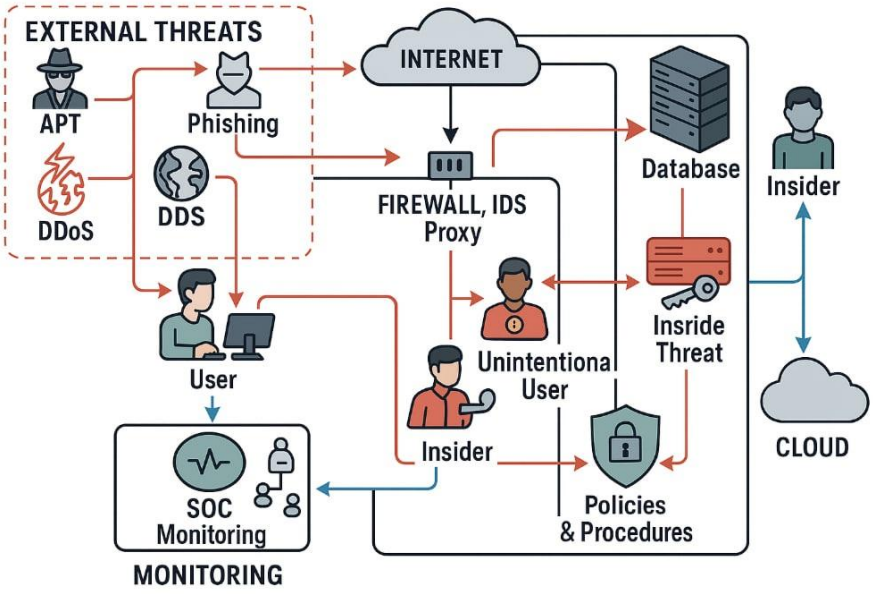


Рис. 1. Схема ймовірних шляхів реалізації кіберзагроз

Математична модель, яка реалізує цей підхід у контексті кіберзахисту критичної інфраструктури формулюється наступним чином.

Нехай є множина критеріїв оцінювання системи кіберзахисту:

$$C = \{C_1, C_2, \dots, C_n\},$$

де C_i — окремий критерій (в нашому випадку n = 7)

Далі формується квадратна матриця розміром n x n, де кожен елемент a_{ij} характеризує ступень впливу критерію C_i на C_j:

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{21} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix},$$

де $a_{ij} = 0$ — якщо немає впливу,

$a_{ij} \in \{1, 2, 3, 4\}$ — якщо є слабкий/помірний/ сильний/дуже сильний вплив.

Далі потрібно провести розрахунки показників впливу (Cause) та ефекту (Effect). Вплив критерію C_i визначається як сума впливів, які C_i чинить на інші фактори:

$$Cause_i = \sum_{j=1}^{n} a_{ij}.$$

Ефект впливу на критерій C_i визначається як сума впливів, що інші фактори чинять на нього:

$$Effect_i = \sum_{j=1}^{n} a_{ji}.$$

За результатами розрахунків векторів Cause/Effect можливо візуалізувати карту залежностей:

- критерії з високим Cause — активні драйвери;
- критерії з високим Effect — чутливі результати;
- високі обидва — ключові важелі;
- низькі обидва — нейтральні фактори.

У контексті захисту критичної інфраструктури зростає потреба у використанні різних архітектур безпеки, що враховують як фізичні обмеження, так і сучасні вектори атак. З метою обґрунтованого вибору оптимального рішення, було проведено аналіз трьох найбільш поширених моделей: класичної корпоративної моделі, Zero Trust архітектури та хмарної моделі.

Класична корпоративна модель базується на захисті мережевого периметра та централізованому адмініструванні внутрішніх ресурсів. Її архітектура орієнтована на забезпечення фізичної ізоляції, контроль доступу в межах корпоративної мережі та мінімізацію зовнішніх загроз за допомогою міжмережевих екранів, VPN та систем виявлення вторгнень. Проте такий підхід виявляється менш ефективним у сучасних умовах, де ключову роль відіграють гібридна робота, мобільні пристрої та хмарні сервіси.

Архітектура Zero Trust (ZTA) відмовляється від поняття довіри за географічною чи мережевою ознакою. Кожен запит щодо використання ресурсу розглядається як потенційно ворожий, незалежно від його походження. Безпека забезпечується шляхом застосування багаторівневої аутентифікації, сегментації доступу, аналізу поведінки та дотримання принципу мінімальних привілеїв. Такий підхід підвищує стійкість до складних, довготривалих атак та внутрішніх загроз, але вимагає ретельного налаштування та інтеграції контролю в кожному елементі системи.

Хмарна модель орієнтована на масштабованість, гнучкість і доступність. Вона передбачає делегування частини безпекових функцій провайдерам (IaaS, PaaS) та водночас зобов'язує користувачів забезпечити контроль за конфігурацією, шифруванням, автентифікацією та моніторингом. Цей підхід ідеально підходить для динамічного середовища, проте вразливий до помилок конфігурації, витоку через API та атак на ланцюг постачання (Supply Chain Attacks).

Зведені характеристики кожної моделі, їхні ключові компоненти, фокус захисту, типові обмеження, а також найбільш ймовірні вразливості та домінуючі кіберзагрози наведено у табл. 2.

Таблиця 2

Ключові властивості трьох моделей

Характеристика	Класична корпоративна модель (A1)	Zero Trust Architecture (A2)	Хмарна модель (A3)
1. Основні компоненти	Фаєрволи (Cisco ASA, Fortinet), IDS/IPS (Snort), VPN, AD, антивіруси. Орієнтована на апаратні компоненти та централізовану IT-інфраструктуру	IAM/MFA, мікросегментація, SDP, UEBA, SIEM (Splunk). Забезпечує детальний контроль доступу та контекстну перевірку	SaaS-сервіси, API-шлюзи, Cloud WAF, CASB, шифрування даних. Покладається на сервіси третьої сторони

2. Фокус безпеки	Захист мережевого периметра, централізований контроль доступу	Контроль доступу на основі контексту, перевірка кожної сесії	Безпека хмарної інфраструктури, аудит доступу, шифрування
3. Обмеження / Виклики	Обмежена масштабованість, складність оновлення, низька адаптивність до змін середовища	Складність впровадження, інтеграція з наявною інфраструктурою, потреба в чіткому адмініструванні	Залежність від провайдера, ризик неправильних конфігурацій, складність SLA-контролю
4. Вразливості	Внутрішня мережа, кінцеві пристрої, сервери AD	Контроль доступу, API шлюзи, хмарні ресурси	API-інтерфейси, хмарне зберігання, несанкціоновані додатки
5. Найнебезпечніші загрози	Phishing, Ransomware, Insider Threats, DoS	Credential Theft, Lateral Movement, APT, Zero-Day	Misconfiguration, Data Leakage, Supply Chain Attacks, DoS
6. Довіра за замовчуванням	Всередині мережі	Взагалі нікому	Частково делегована (залежно від моделі провайдера)
7. Точка контролю	Периметр	Кожен запит	Інтерфейси та політики
8. Середовище застосування	Стаціонарний офіс	Віддалена/гібридна робота	Динамічна інфраструктура, з частими змінами конфігурацій
9. Основний ризик	Інсайдери, APT	Недостатній моніторинг, складність	Помилки конфігурації, API вразливості

З огляду на проведене порівняння трьох основних архітектурних підходів до побудови систем кібербезпеки було виявлено низку ключових характеристик, що відрізняють ці альтернативи за принципами побудови, рівнем захищеності, типами загроз і специфікою середовища використання. Встановлено, що кожна модель має свої сильні сторони та обмеження, які необхідно враховувати під час вибору найбільш ефективної системи для конкретної критичної інфраструктури.

Для формалізованого порівняння альтернатив в дослідженні застосовано MAI, який дозволяє провести їх багатокритеріальну оцінку з урахуванням взаємної важливості критеріїв. Виходячи з технічних, організаційних та економічних аспектів, сформовано узагальнений перелік критеріїв оцінювання, що відображають як функціональні показники ефективності систем (наприклад, швидкість виявлення та реагування), так і показники надійності, автоматизації, витрат і відповідності політикам безпеки.

MAI передбачає побудову ієрархічної структури проблеми, що включає:

- мету оцінювання (вибір найкращої архітектури кібербезпеки);
- низку критеріїв ефективності, що характеризують технічні, організаційні та економічні аспекти,
- перелік альтернативних варіантів рішень.

В межах даного дослідження запропонована наступна система критеріїв, що характеризують різні аспекти безпеки та дозволяють оцінити її ефективність (табл. 3).

Таблиця 3

Система критеріїв для оцінки ефективності безпеки

C_i	Критерій	Опис критерію	Чому важливо
C1	Середній час виявлення (MTTD)	Середній час, який потрібен для виявлення кіберзагрози після її виникнення	Менший час виявлення знижує шкоду від атаки
C2	Середній час реагування (MTTR)	Середній час, необхідний для реагування на виявлену загрозу	Швидке реагування мінімізує наслідки інциденту
C3	Відсоток виявлених загроз	Частка загроз, які система здатна ефективно виявити	Високий показник дозволяє вчасно нейтралізувати загрози
C4	Рівень хибнопозитивних спрацювань (%)	Відсоток помилкових спрацювань системи захисту	Низький рівень хибнопозитивів зменшує навантаження на персонал
C5	Час усунення вразливостей (у днях)	Час, необхідний для усунення вразливості після її виявлення	Довгий час усунення підвищує ризик експлуатації вразливостей
C6	Рівень автоматизації реагування	Ступінь автоматизації дій у відповідь на інциденти	Автоматизація підвищує ефективність та швидкість реагування
C7	Рівень дотримання оновлень (патчів)	Частота своєчасного застосування оновлень системи	Забезпечує актуальність та стійкість до нових загроз
C8	Рівень виявлення нових загроз	Здатність системи виявляти нові, раніше невідомі загрози	Критично для захисту від нових атак і 0-day вразливостей
C9	Покриття площини атаки	Обсяг компонентів та поверхонь, що можуть бути атаковані	Широке покриття знижує ймовірність непоміченої атаки
C10	Середній час відновлення після інциденту (MTTRc)	Середній час, необхідний для повного відновлення після інциденту	Швидке відновлення мінімізує простої та втрати
C11	Повернення інвестицій у безпеку (Security ROI)	Ефективність інвестицій у кібербезпеку з точки зору зниження ризиків	Допомагає оцінити економічну ефективність безпекових заходів
C12	Частота успішних зламів	Кількість успішних зламів у певний проміжок часу	Низька частота зламів свідчить про ефективність системи
C13	Рівень відповідності політикам	Міра дотримання політик безпеки та стандартів	Відповідність стандартам є вимогою для багатьох сфер
C14	Вартість впровадження	Витрати, пов’язані з початковим розгортанням системи	Визначає початкові інвестиції та бюджетування
C15	Вартість обслуговування	Регулярні витрати на підтримку та оновлення системи	Впливає на довгострокову економічну ефективність системи

На першому етапі реалізується попарне порівняння критеріїв експертами з використанням шкали Сааті, що дозволяє отримати матрицю переваг. Далі здійснюється нормалізація матриці та обчислення вектора ваг критеріїв $W = (w_1, w_2, \dots, w_n)$, який відображає їх відносну важливість.

На наступному етапі кожна альтернатива оцінюється за кожним критерієм, формуючи матрицю корисностей $U = [u_{ij}]$, де u_{ij} — ступінь відповідності j-ї

альтернативи *i*-му критерію. Корисності можуть бути отримані на основі емпіричних даних, експертного опитування або моделювання.

Підсумкова оцінка альтернативи розраховується за формулою:

$$U_{total} = \sum_{i=1}^{n} w_i * u_i,$$

де w_i — вага і-го критерію,

u_i — оцінка альтернативи за цим критерієм.

Таким чином, інтегральна оцінка відображає узагальнену ефективність кожного сценарію з урахуванням важливості всіх критеріїв. Модель дозволяє здійснювати ранжування альтернатив та приймати обґрунтовані управлінські рішення щодо побудови архітектури кіберзахисту відповідно до цілей, ресурсів і ризиків організації.

З метою забезпечення ґрунтовного вибору найбільш ефективної конфігурації системи кіберзахисту було проведено детальний аналіз критеріїв оцінювання. Для кожного критерію встановлено напрям функції корисності (зростаюча або спадна) згідно з його природою. Крім того, за результатами аналізу статистичних даних з урахуванням характеру зміни впливу критерію на результат було запропоновано відповідний тип функції корисності (лінійна, експоненційна, логістична тощо). Підхід ґрунтується на рекомендаціях провідних організацій (NIST, ENISA), а також сучасних дослідженнях у сфері побудови архітектур кіберзахисту [5].

У табл. 4 наведено опис критеріїв, їх коротке пояснення, обґрунтування важливості, напрям функції корисності та рекомендований тип функції.

Таблиця 4

Опис функцій корисностей за кожним критерієм

Ci	Критерій	Напрям функції	Тип функції корисності	Пояснення
C1	Середній час виявлення (MTTD)	Спадна	Експоненційна	Затримка виявлення швидко знижує ефективність
C2	Середній час реагування (MTTR)	Спадна	Експоненційна	Пізніше реагування призводить до значних втрат
C3	Відсоток виявлення загроз	Зростаюча	Логістична	Ефект зростає до насичення
C4	Рівень хибнопозитивних спрацювань (%)	Спадна	Лінійна або логістична	Падаюча шкода від зменшення помилок
C5	Час усунення вразливостей	Спадна	Лінійна	Пряма залежність шкоди від часу
C6	Рівень автоматизації реагування	Зростаюча	Логістична	Ефект автоматизації зростає до певної межі
C7	Рівень дотримання оновлень (патчів)	Зростаюча	Логістична	Зменшує ризики до певного рівня
C8	Рівень виявлення нових загроз	Зростаюча	Експоненційна	Висока критичність для нових типів атак
C9	Покриття площини атаки	Зростаюча	Лінійна	Пряма залежність захищеності від площини покриття
C10	Середній час відновлення після інциденту (MTTRc)	Спадна	Експоненційна	Швидкість відновлення критична для функціонування
C11	Повернення інвестицій у безпеку (ROI)	Зростаюча	Логістична або експоненційна	ROI має ефект зменшення приросту

C12	Частота успішних зламів	Спадна	Логістична	Часті злами – різке зниження ефективності
C13	Рівень відповідності політикам	Зростаюча	Лінійна	Чітка регуляторна залежність
C14	Вартість впровадження	Спадна	Лінійна	Пряма фінансова залежність
C15	Вартість обслуговування	Спадна	Лінійна	Тривалий економічний ефект витрат

З метою практичного впровадження розробленого підходу до багатокритеріального оцінювання альтернативних рішень у сфері кіберзахисту було розроблено спеціалізовану систему підтримки прийняття рішень. Цей інструмент орієнтований на експертно-аналітичну обробку даних та реалізує поетапну процедуру ухвалення ґрунтовного рішення щодо вибору оптимальної архітектури системи кібербезпеки.

СППР інтегрує методологію аналізу ієрархій з модулем Cross-Impact Analysis для оцінки взаємного впливу факторів, а також включає механізм динамічного оновлення ваг критеріїв у разі зміни ризиків та актуальних загроз. Такий підхід забезпечує адаптивність системи до зовнішніх умов і дозволяє проводити повторну оцінку альтернатив у режимі реального часу.

Програмний комплекс реалізовано мовою Python із застосуванням бібліотеки Streamlit, що забезпечує сучасний веб-інтерфейс з поетапною навігацією, інтерактивним введенням експертних оцінок, автоматизованим обчисленням локальних і глобальних пріоритетів, а також візуалізацією результатів у вигляді таблиць, графіків і діаграм.

Початковий етап роботи з розробленим програмним модулем передбачає формалізацію структури досліджуваної системи у вигляді матриці взаємовпливу факторів. На цьому етапі користувач ініціює створення або редагування матриці, у якій числові значення відображають інтенсивність впливу одного фактору на інші. Такий підхід дає змогу врахувати причинно-наслідкові зв’язки між ключовими елементами системи та формує основу для подальшого багатокритеріального оцінювання.

Програмна реалізація виконана із використанням фреймворку Streamlit, що забезпечує інтерактивну роботу з інтерфейсом безпосередньо в браузері. У бічній панелі користувач має змогу обрати один із двох режимів (рис. 2):

– завантаження наявного проєкту з каталогу data/projects/;
– створення нового проєкту із зазначенням імені.

За необхідності створення нового проєкту система автоматично генерує порожню матрицю впливів, яку можна заповнити вручну в інтерфейсі веб-додатку. Усі дані зберігаються у форматі CSV, що дозволяє легко здійснювати подальший аналіз та архівацію.

Однією з ключових функціональних особливостей цього етапу є візуалізація моделі системи у вигляді орієнтованого графа (рис. 3). Побудова графа здійснюється на основі заданої матриці впливу за допомогою бібліотек NetworkX і Plotly. Вершини графа відповідають окремим факторам, а орієнтовані ребра демонструють напрямок та інтенсивність впливу між ними. Візуальні характеристики вузлів (зокрема, розмір і колір) формуються відповідно до інтегрального показника впливу, який обчислюється як сума вхідних і вихідних зв’язків кожного фактору.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023

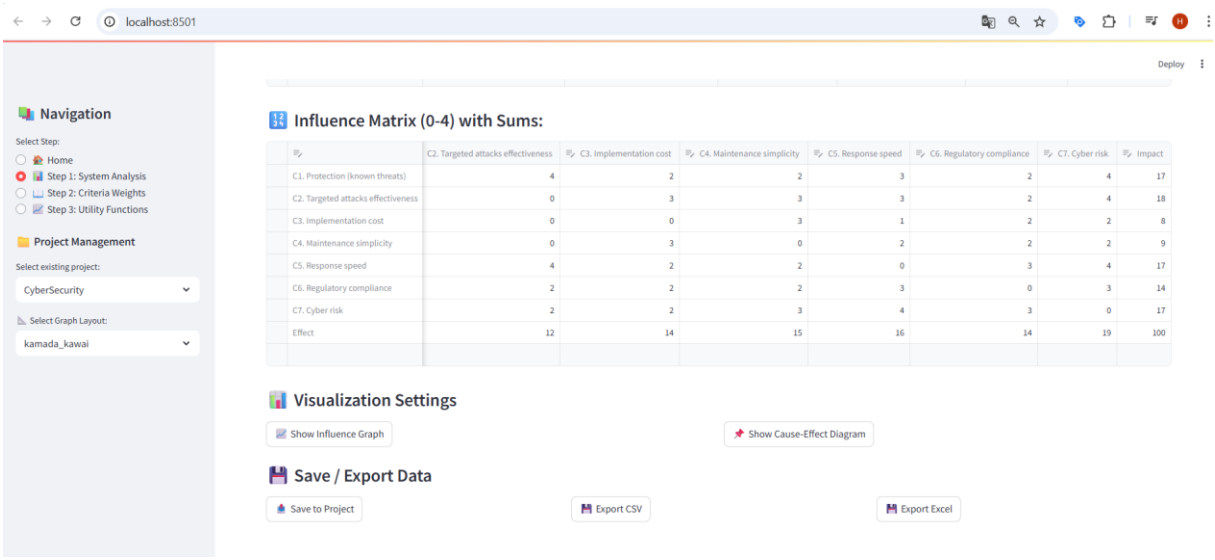


Рис. 2. Фрагмент інтерфейсу модуля створення матриці впливів

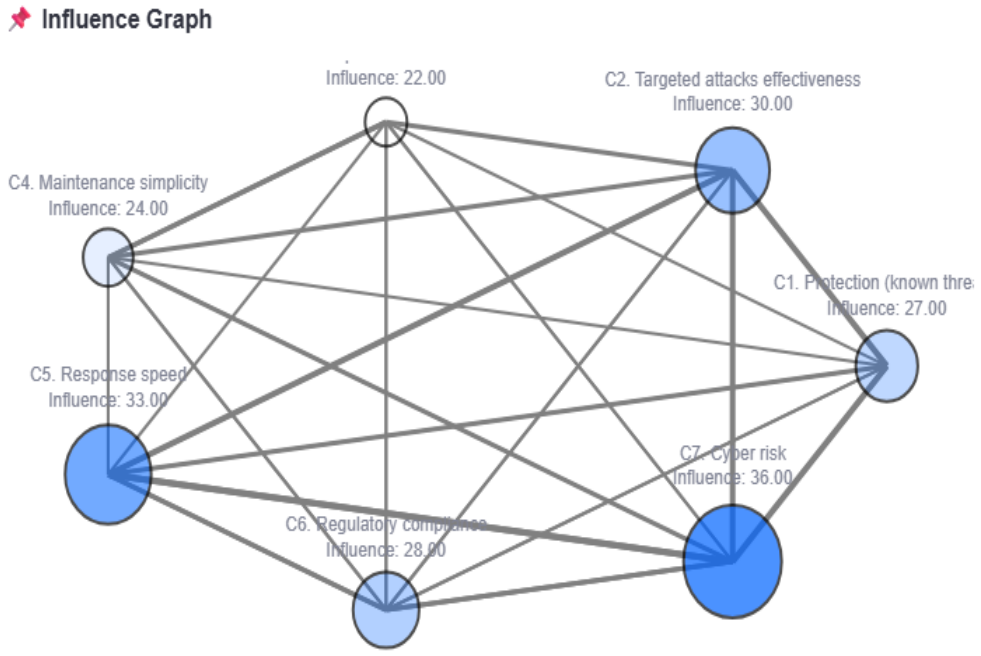


Рис. 3. Орієнтований граф із візуалізацією впливів між факторами

Користувачеві доступні кілька варіантів відображення просторової структури графа, зокрема:

- kamada-kawai;
- spring;
- circular;

Це надає змогу обрати найзручніший формат візуальної інтерпретації взаємозв'язків системи, що, в свою чергу, забезпечує швидке виявлення факторів, які мають найбільший вплив на систему, а також тих, що є найбільш вразливими до зовнішніх чинників.

Діаграма взаємовпливів факторів (рис. 4) дозволяє наочно побачити групи факторів, що мають найбільший вплив один на одного та на ефективність системи захисту в цілому. Ця інформація дозволяє перейти до більш детального аналізу відповідних груп факторів з вибору критеріїв для їх оцінювання на наступному,другому етапі дослідження.

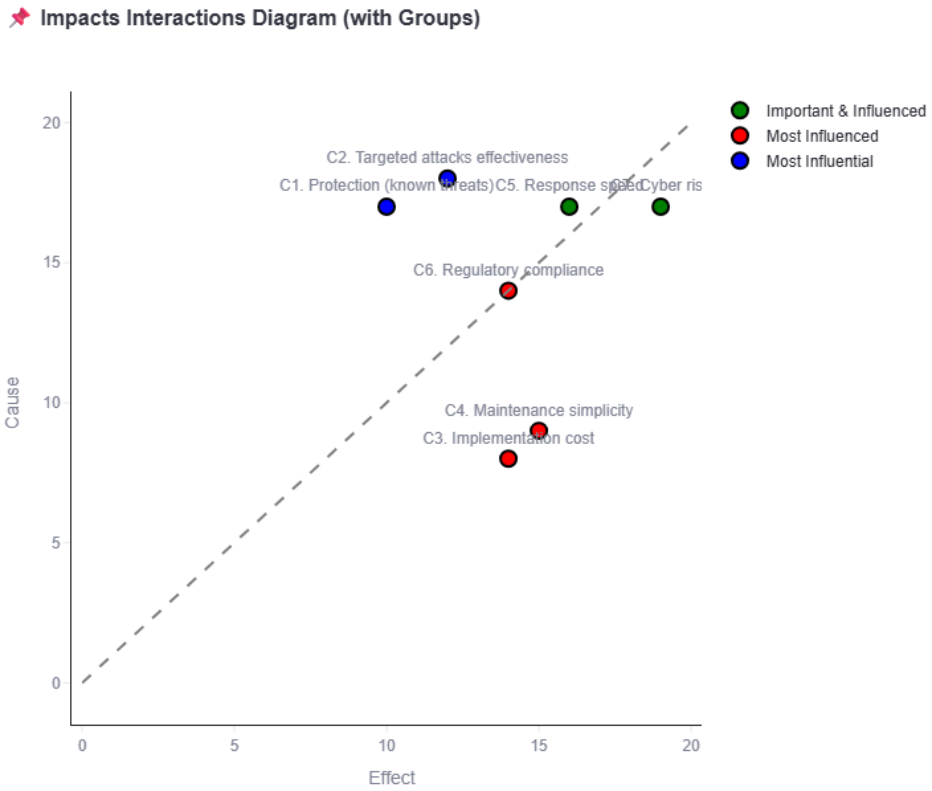


Рис. 4. Діаграма Cause-Effect взаємовпливів факторів

Результатом даного етапу є:

- сформована та збережена матриця впливу у форматі CSV;
- інтерактивна графічна модель досліджуваної системи;
- підготовлені дані для переходу до наступного етапу — визначення вагових коефіцієнтів із використанням методу аналізу ієрархій (MAI).

Другий етап функціонування програмного комплексу реалізує процедуру визначення відносної важливості критеріїв шляхом побудови матриці попарних порівнянь за MAI. Цей підхід є одним із найбільш поширених у сфері багатокритеріального прийняття рішень, особливо в умовах невизначеності та при роботі з експертними оцінками.

На початку даного етапу користувач обирає один із проєктів, розглянутих на попередньому етапі і заповнює матрицю попарних порівнянь, де кожен елемент a_{ij} характеризує відносну перевагу критерію i над критерієм j за шкалою Сааті (від 1 до 9) (рис. 5).

ISSN 2663 - 4023

Після завершення введення даних система автоматично виконує обчислення:

– нормалізованої матриці парних порівнянь;
– вектора пріоритетів — вагових коефіцієнтів за кожним критерієм;
– коефіцієнта узгодженості (CR), що дозволяє оцінити логічну послідовність і надійність експертних оцінок.

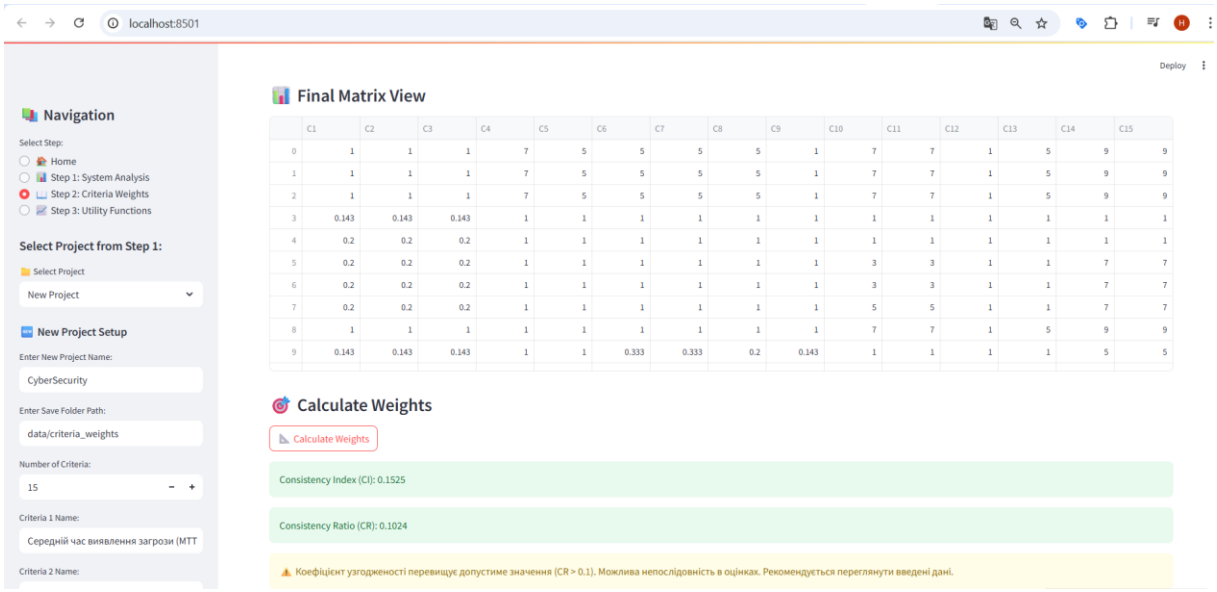


Рис. 5. Інтерфейс модуля заповнення матриці попарних порівнянь

В СППР алгоритм MAI реалізовано у вигляді окремого функціонального модуля, в межах якого виконуються наступні розрахунки:

– нормалізація елементів кожного стовпця матриці шляхом їх ділення на суму відповідного стовпця;
– обчислення ваг кожного фактору як середнього значення за кожним рядком нормалізованої матриці;
– оцінювання наближеного максимального власного значення λ_{max};
– обчислення індексу узгодженості (CI) та коефіцієнта узгодженості (CR) за формулами:

$$CI = \frac{\lambda_{max} - n}{n-1},$$

$$CR = \frac{CI}{RI},$$

де n — кількість критеріїв,

RI — середнє випадкове значення індексу узгодженості для матриці розмірності n.

Якщо коефіцієнт узгодженості перевищує порогове значення ($CR > 0.1$), система видає попередження щодо ймовірної непослідовності в оцінках та рекомендує їх переглянути (рис. 5). Якщо коефіцієнт узгодженості не перевищує порогове значення ($CR > 0.1$), отримані ваги критеріїв зберігаються у вигляді CSV-файлу для подальшого використання на третьому етапі (рис. 6).

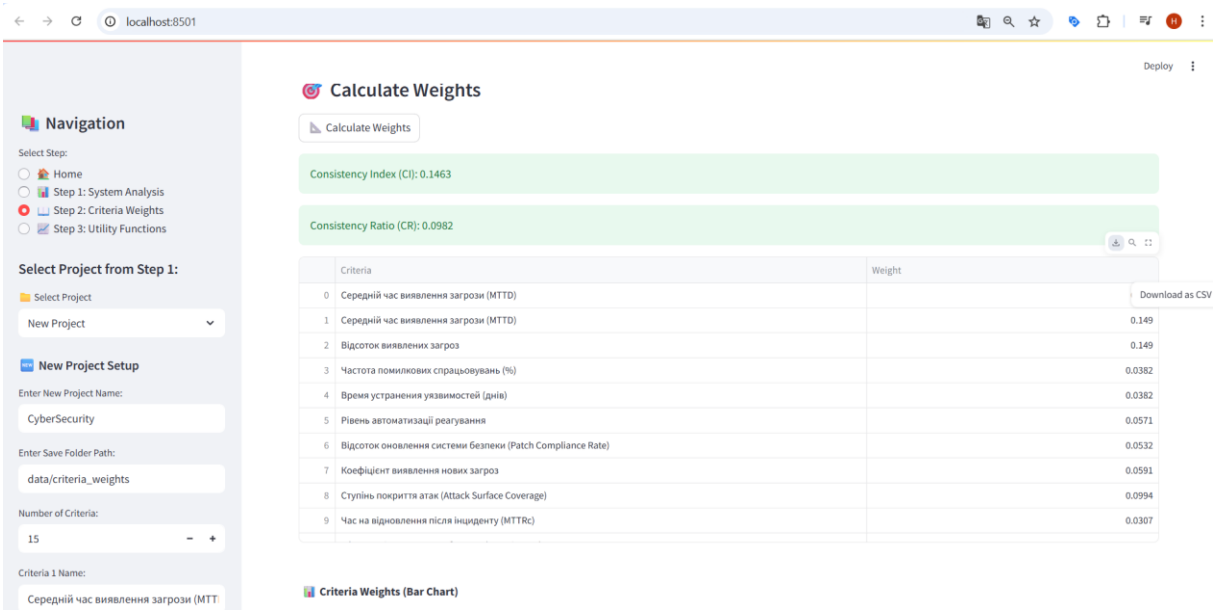


Рис. 6. Таблиця з розрахованими вагами критеріїв

До переваги реалізації другого етапу можна віднести наступне:

– автоматична перевірка послідовності суджень експерта;
– миттєвий розрахунок ваг без необхідності використання стороннього програмного забезпечення;
– гнучкий веб-інтерфейс, що дозволяє працювати як із новими наборами критеріїв, так і з раніше збереженими проєктами;
– повна інтеграція з результатами першого етапу (Cross-Impact Analysis) і підготовка до наступного кроку – оцінювання альтернатив.

Фінальний етап роботи реалізованого програмного комплексу спрямований на здійснення оцінювання альтернативних рішень та визначення найбільш ефективного з них. Основою для цього є вагові коефіцієнти критеріїв, розраховані на попередньому етапі за MAI, що дозволяє виконати багатокритеріальну агрегацію з урахуванням пріоритетності кожного критерію.

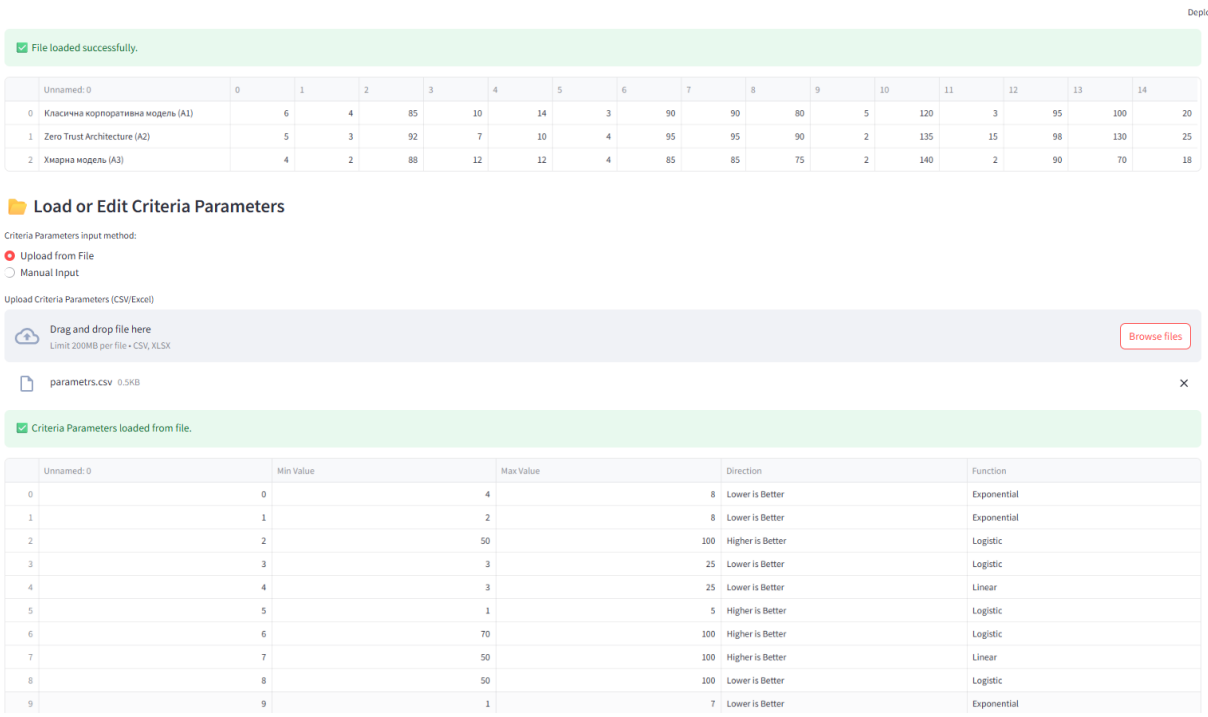
Користувач обирає проєкт, у якому збережено результати попередніх етапів. Система автоматично завантажує перелік критеріїв разом з відповідними вагами. Далі користувач:

– задає кількість альтернатив, що підлягають оцінюванню;
– обирає спосіб введення даних — вручну або завантаженням із CSV-файлу;
– вводить оцінки кожної альтернативи за низкою критеріїв (рис. 7).

В результаті формується матриця розміром «кількість альтернатив × кількість критеріїв», яка автоматично множиться на вектор ваг для отримання інтегральної оцінки кожної альтернативи. Цей механізм реалізовано на основі лінійної згортки, що дозволяє:

– відсортувати альтернативи за спаданням функції корисності;
– виявити найбільш доцільне рішення відповідно до заданих умов;
– провести аналіз чутливості — перевірку впливу зміни ваг або оцінок на підсумковий результат.

ISSN 2663 - 4023



	Unnamed: 0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	Класична корпоративна модель (A1)	6	4	85	10	14	3	90	90	80	5	120	3	95	100	20
1	Zero Trust Architecture (A2)	5	3	92	7	10	4	95	95	90	2	135	15	98	130	25
2	Хмарна модель (A3)	4	2	88	12	12	4	85	85	75	2	140	2	90	70	18

	Unnamed: 0	Min Value	Max Value	Direction	Function
0	0	4	8	Lower is Better	Exponential
1	1	2	8	Lower is Better	Exponential
2	2	50	100	Higher is Better	Logistic
3	3	3	25	Lower is Better	Logistic
4	4	3	25	Lower is Better	Linear
5	5	1	5	Higher is Better	Logistic
6	6	70	100	Higher is Better	Logistic
7	7	50	100	Higher is Better	Linear
8	8	50	100	Lower is Better	Logistic
9	9	1	7	Lower is Better	Exponential

Рис. 7. Інтерфейс введення або завантаження матриці оцінок альтернатив

Для зручності інтерпретації результатів в комплекс інтегровано модуль графічного відображення. Користувач має змогу обрати один із форматів подання результатів:

– гістограми, що ілюструють відносну оцінку кожної альтернативи (рис. 8);

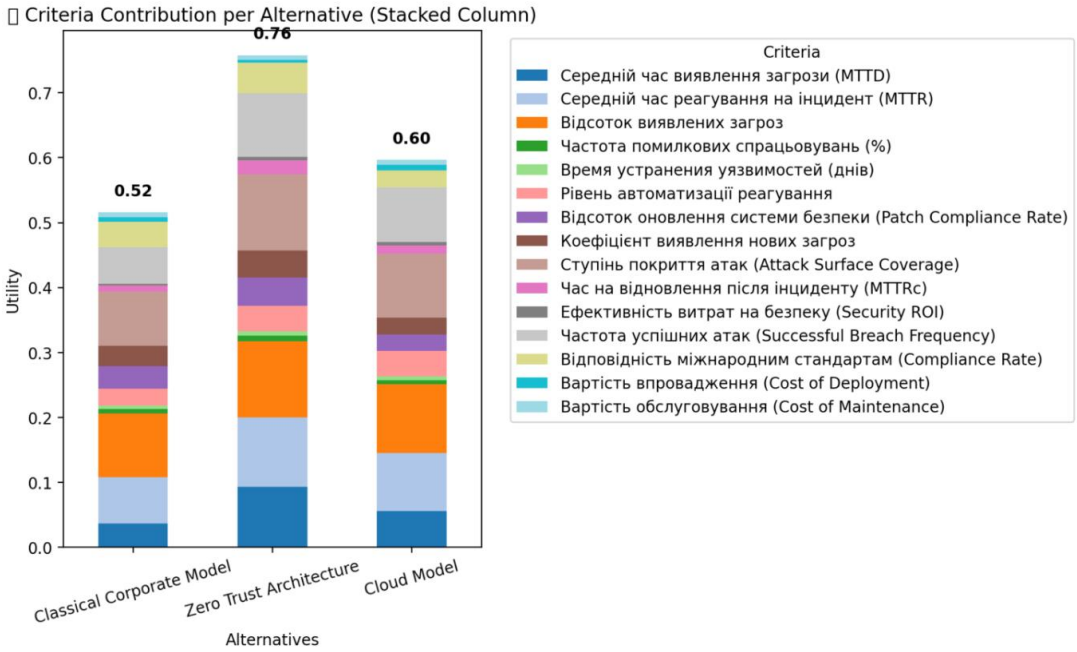
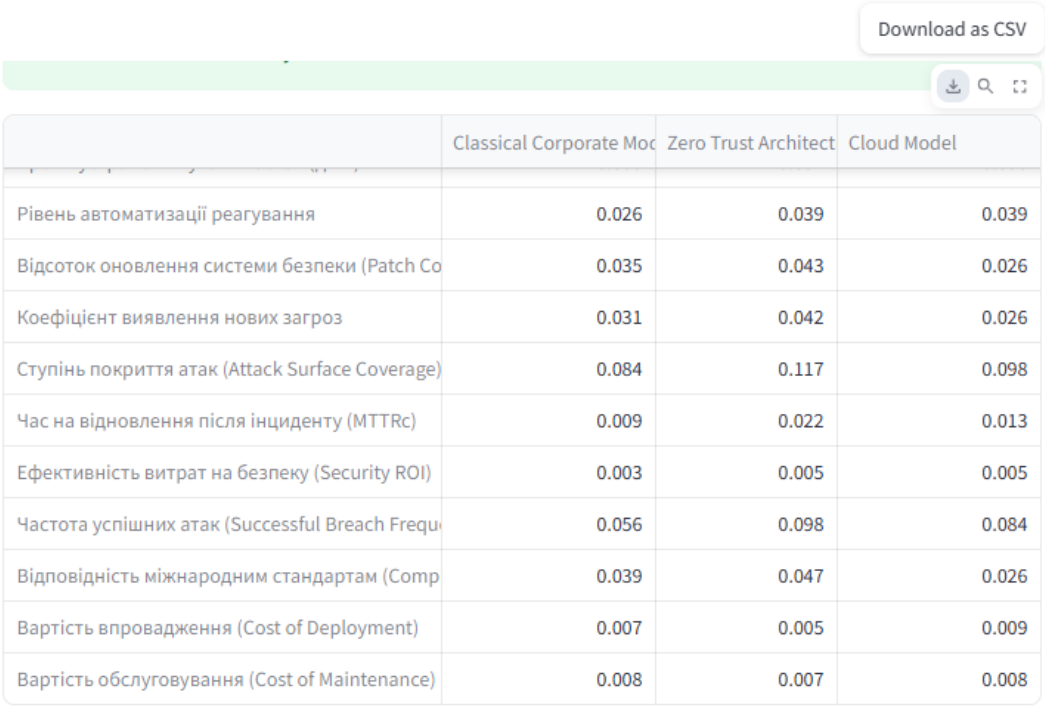


Рис. 8. Гістограма інтегральних оцінок альтернатив

– табличну форму, яка відображає детальний аналіз альтернатив за критеріями (рис. 9);



	Classical Corporate Moc	Zero Trust Architect	Cloud Model
Рівень автоматизації реагування	0.026	0.039	0.039
Відсоток оновлення системи безпеки (Patch Co	0.035	0.043	0.026
Коефіцієнт виявлення нових загроз	0.031	0.042	0.026
Ступінь покриття атак (Attack Surface Coverage)	0.084	0.117	0.098
Час на відновлення після інциденту (MTTRc)	0.009	0.022	0.013
Ефективність витрат на безпеку (Security ROI)	0.003	0.005	0.005
Частота успішних атак (Successful Breach Frequ	0.056	0.098	0.084
Відповідність міжнародним стандартам (Comp	0.039	0.047	0.026
Вартість впровадження (Cost of Deployment)	0.007	0.005	0.009
Вартість обслуговування (Cost of Maintenance)	0.008	0.007	0.008

Рис. 9. Таблиця ранжування альтернатив за критеріями

– експорт результатів у форматі CSV для подальшого аналізу або презентації.

Система автоматично адаптує інтерфейс під задану кількість критеріїв і альтернатив, що забезпечує гнучкість та масштабованість розв’язання.

Основні особливості реалізації програмного модуля полягають у високій ступені адаптивності системи до різних джерел даних та сценаріїв використання, що реалізується за рахунок підтримки як введення оцінок вручну, так і імпорту інформації з зовнішніх джерел.

Ключовим функціональним елементом є автоматизоване агрегування результатів, що відбувається з урахуванням вагових коефіцієнтів, визначених на попередньому етапі. Завдяки використанню методу лінійної згортки, користувач отримує об’єктивні інтегральні оцінки для кожної альтернативи.

Важливою перевагою є повна інтеграція третього етапу з результатами попередніх двох, а саме формуванням структури критеріїв та обчисленням їхньої важливості. Таким чином, забезпечується завершеність і логічна послідовність процесу прийняття ґрунтовного рішення.

За результатами виконання даного етапу користувач має змогу отримати:

– візуалізацію функцій корисності за кожним критерієм (рис. 10);
– результати оцінювання всіх альтернатив за кожним критерієм (рис. 9);
– підсумкову інтегральну оцінку кожної альтернативи;
– ранжування рішень за рівнем їхньої корисності;
– збережений проєкт, який містить усі вхідні, проміжні та підсумкові дані, що забезпечує можливість подальшого аналізу або повторного використання інформації.

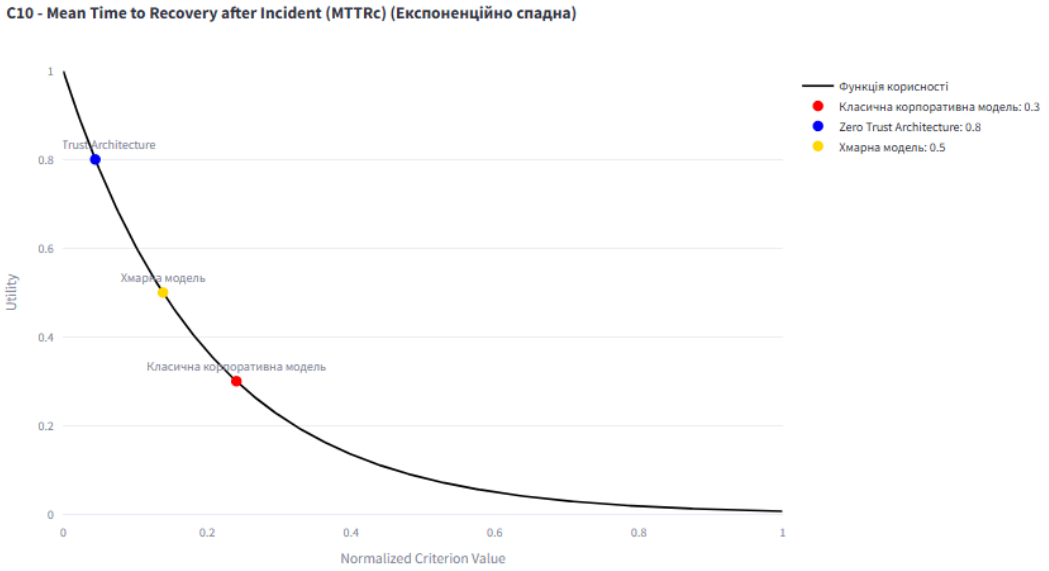


Рис. 10. Приклад візуалізації функції корисності

Таким чином, розроблена СППР може бути ефективно використана для підтримки рішень у сферах, що потребують складного багатокритеріального аналізу, зокрема у плануванні архітектури захисту критичної інформаційної інфраструктури. Об'єднання архітектурного підходу з критеріальною оцінкою дає змогу не лише будувати, але й ґрунтовно вибирати та вдосконалювати системи кіберзахисту, базуючись на реальних потребах і обмеженнях підприємств, особливо у сферах, де ризики критично високі — енергетика, транспорт, урядові організації.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті запропоновано системний підхід до підтримки прийняття архітектурних рішень у сфері кіберзахисту об'єктів критичної інфраструктури на основі багатокритеріального аналізу. Розроблена СППР інтегрує MAI, структурний аналіз впливів та механізми динамічного оновлення вагових коефіцієнтів відповідно до змін зовнішнього середовища. Це дозволяє здійснювати ґрунтовний вибір архітектури системи захисту з урахуванням множинних технічних, організаційних, економічних і ризик-орієнтованих критеріїв.

Проведено формалізацію оцінювання альтернатив на основі векторної моделі, описано принципи побудови системи показників ефективності (C1–C15) та визначено відповідні функції корисності. Практична реалізація СППР у середовищі Python/Streamlit демонструє її застосовність до задач проектування систем кібербезпеки різної складності, з можливістю інтерактивного введення даних, візуалізації зв'язків між критеріями та автоматичного ранжування варіантів.

Запропонований підхід забезпечує:

– прозорість та логічність прийняття рішень;
– врахування множинних міжкритеріальних впливів;
– адаптацію до змін середовища у режимі реального часу;

– можливість практичного використання у сферах енергетики, транспорту, зв'язку та інших критичних галузях.

Перспективи подальших досліджень полягають у:

– розширенні методології за рахунок включення нечіткої логіки та нейромережевих моделей у СППР;
– розробці модулів прогнозування динаміки кіберзагроз та автоматичного коригування ваг критеріїв;
– тестуванні СППР на реальних об'єктах критичної інфраструктури;
– інтеграції системи з існуючими платформами моніторингу інцидентів (SOC/SIEM);
– розробці навчального модуля для підготовки фахівців з архітектурного планування кібербезпеки.

Загалом, представлений підхід створює основу для формування адаптивних, прозорих і практично орієнтованих систем кіберзахисту, здатних реагувати на швидкоплинні зміни агресивного середовища.

ПОДЯКА

Хочемо подякувати проф. **Rodney Stevens**, University of Gothenburg, Sweden, що надихнув нас на проведення дослідження і підтримував в межах проходження курсу Project Scoping with AI Assistance. Його підтримка та влучні запитання допомогли подивитися на проблему під різними кутами та покращити якість роботи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Adapa, V. R. K. (2024). Zero Trust Architecture Implementation in Critical Infrastructure: A Framework for Resilient Enterprise Security. *International Journal of Advanced Research in Engineering and Technology (IJARET)*, *15*(6), 76–89. https://doi.org/10.34218/IJARET_15_06_006
2. Martínez, A., & Thompson, C. (2025). Zero Trust Architecture – A Systematic Literature Review. *arXiv preprint*, arXiv:2503.11659. https://doi.org/10.48550/arXiv.2503.11659
3. Khan, N., Ahmad, K., & Kim, D.-S. (2024). Explainable AI-based Intrusion Detection System for Industry 5.0: An Overview. *arXiv preprint*, arXiv:2408.03335. https://doi.org/10.48550/arXiv.2408.03335
4. Kenmogne, L. A., & Mocanu, S. (2024). Explainable AI for process-aware attack detection in industrial control systems. In *2024 IEEE 10th International Conference on Network Softwarization (NetSoft)* (pp. 363–368). IEEE. https://ieeexplore.ieee.org/document/10588940
5. Bhaskaran, D. (2025). Zero Trust Architecture: Securing America's Critical Infrastructure. *International Journal of Advances in Engineering and Management (IJAEM)*, *7*(2), 157–164. https://www.researchgate.net/publication/388921125
6. Ilienko, A., Teliushchenko, V., & Dubchak, O. (2023). Suchasni kiberzahrozy krytychnoi infrastruktury Ukrainy ta svitu. *Kiberbezpeka: osvita, nauka, tekhnika*, *27*, 150–164. https://doi.org/10.28925/2663-4023.2023.27.719
7. Murasov, R. K., & Melnyk, Ya. V. (2023). Otsiniuvannia zakhyshchenosti kiberprostoru obiektiv krytychnoi infrastruktury Ukrainy. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony*, *46*(1), 41–44. https://doi.org/10.33099/2311-7249/2023-46-1-41-44
8. Mohale, V. Z., & Obagbuwa, I. C. (2025). Evaluating machine learning-based intrusion detection systems with explainable AI: Enhancing transparency and interpretability. *Frontiers in Computer Science*, *7*, Article 1520741. https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2025.1520741/full
9. Murasov, R., Nikitin, A., & Meshcheriakov, I. (2024). Mathematical model of risk assessment of the operation of critical infrastructure objects based on the theory of fuzzy logic. *Social Development and Security*, *14*(5), 166–174. https://doi.org/10.33445/sds.2024.14.5.17

10. Triantaphyllou, E. (2000). *Multi-Criteria Decision Making: A Comparative Study*. Dordrecht, The Netherlands: Kluwer Academic Publishers (now Springer). ISBN 0-7923-6607-7. https://www.csc.lsu.edu/trianta/Books/DecisionMaking1/backup/Book_DM1.htm?utm_source=chatgpt.com
11. Shapovalova, O. O., & Burmenskyi, R. V. (2017). Rozrobka prohramnoho dodatka dlia realizatsii metodu analizu iierarkhii. *Systemy obrobky informatsii*, *3*(149), 45-48. https://doi.org/10.30748/soi.2017.149.09
12. Mockor, J., & Hynar, D. (2021). On unification of methods in theories of fuzzy sets, hesitant fuzzy set, fuzzy soft sets and intuitionistic fuzzy sets. *Mathematics*, *9*, 447. https://doi.org/10.3390/math9040447
13. Zakon Ukrainy «Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy» vid 05.10.2017 № 2163-VIII (v redaktsii 2025 r.). *Vidomosti Verkhovnoi Rady Ukrainy*, *2017*(45), st. 403. https://zakon.rada.gov.ua/laws/show/2163-19#Text
14. ISO/IEC. (2022). *ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. Geneva, ISO. https://www.iso.org/standard/27001
15. ISA/IEC. (2018). *ISA/IEC 62443. Series of Standards for Industrial Automation and Control Systems Security*. International Electrotechnical Commission. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
16. NIST. (2024). *NIST SP 800-82 Rev. 3. Guide to Operational Technology (OT) Security*. Gaithersburg, MD: National Institute of Standards and Technology. https://csrc.nist.rip/external/nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.ipd.pdf
17. Stevens, R. L., Aliyeva, S., Bornmalm, L., Calvache, C. D., & Ivanov, A. V. (2021, August 14–22). Tools for project scoping: Conceptual modeling of stakeholders, activities and goals. In *Proceedings of the 21st SGEM International Multidisciplinary Scientific GeoConference* (Vol. 2.1, pp. 193–200), Albena, Bulgaria. https://epslibrary.at/sgem_jresearch_publication_view.php?page=view&editid1=7877
18. Hendela, A., & Turoff, M. (2010). Cross impact security analysis using the HACKING Game. In *Proceedings of the 7th International ISCRAM Conference*, Seattle, USA, May 2010. ISCRAM. https://www.researchgate.net/publication/229049304_Cross_Impact_Security_Analysis_using_the_HACKING_Game

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023

Nataliya Dolgova
Ph.D. (Tech.), Associate Professor,
Associate Professor of the Department of Cybersecurity and Information Technology,
Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine
ORCID ID: 0000-0002-8950-8200
natalya.dolgova@hneu.net

Olena Shapovalova
Ph.D. (Tech.), Associate Professor,
Associate Professor of the Department of Cybersecurity and Information Technology,
Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine
ORCID ID: 0000-0003-4566-6634
olena.shapovalova@hneu.net

Hanna Solodovnyk
Ph.D. (Tech.), Associate Professor,
Associate Professor of the Department of Cybersecurity and Information Technology,
Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine
ORCID ID: 0000-0001-6323-5083
ganna.solodovnyk@m.hneu.edu.ua

DECISION SUPPORT FRAMEWORK FOR CRITICAL INFRASTRUCTURE CYBERSECURITY PLANNING

Abstract. The article addresses the challenge of making well-grounded architectural decisions in the field of cybersecurity for critical infrastructure facilities under increasing threats, limited resources, and complex interdisciplinary system structures. Modern approaches to building protection systems are analyzed, including the Zero Trust Architecture concept, Explainable AI methods, and risk-based models applied for threat detection and response in highly critical environments. It is identified that existing solutions lack sufficient adaptability and fail to account for the set of interrelated criteria that influence the effectiveness of the protection system architecture. The aim of the research is to develop an integrated decision support system (DSS) that considers the multidimensional nature of cybersecurity tasks and enables the selection of optimal architectures taking into account technical, organizational, and economic factors. A multi-criteria approach based on AHP is proposed, complemented by a structural impact analysis module and a dynamic mechanism for updating criterion weights in accordance with evolving threats and risks. Evaluation criteria for protection architectures (MTTD, MTTR, threat detection rate, automation level, cost, policy compliance, etc.) are formalized with consideration of their functional characteristics and types of utility functions. The practical implementation of the DSS is carried out using Python and the Streamlit library, which provides interactive user engagement, construction of comparison matrices, visualization of causal relationships, and generation of ranked solutions in a user-friendly format. The article presents the architecture of the software module, an example of system functionality based on three architectural models (classical, ZTA, cloud-based), and justifies the choice of an alternative in the context of critical infrastructure. The proposed approach improves the justification and transparency of cybersecurity-related decisions and allows for system adaptation to real-world operational environments, ensuring resilience to complex multi-vector attacks. The results can be applied for the automated design of security architectures in sectors such as energy, transportation, telecommunications, and other critical domains.

Keywords: decision support system; cybersecurity; critical infrastructure; systems approach; multi-criteria analysis; Zero Trust; Explainable AI; Cross-Impact Matrix; AHP.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Adapa, V. R. K. (2024). Zero Trust Architecture Implementation in Critical Infrastructure: A Framework for Resilient Enterprise Security. *International Journal of Advanced Research in Engineering and Technology (IJARET), 15*(6), 76–89. https://doi.org/10.34218/IJARET_15_06_006

2. Martínez, A., & Thompson, C. (2025). Zero Trust Architecture – A Systematic Literature Review. *arXiv preprint*, arXiv:2503.11659. https://doi.org/10.48550/arXiv.2503.11659
3. Khan, N., Ahmad, K., & Kim, D.-S. (2024). Explainable AI-based Intrusion Detection System for Industry 5.0: An Overview. *arXiv preprint*, arXiv:2408.03335. https://doi.org/10.48550/arXiv.2408.03335
4. Kenmogne, L. A., & Mocanu, S. (2024). Explainable AI for process-aware attack detection in industrial control systems. In *2024 IEEE 10th International Conference on Network Softwarization (NetSoft)* (pp. 363–368). IEEE. https://ieeexplore.ieee.org/document/10588940
5. Bhaskaran, D. (2025). Zero Trust Architecture: Securing America's Critical Infrastructure. *International Journal of Advances in Engineering and Management (IJAEM), 7*(2), 157–164. https://www.researchgate.net/publication/388921125
6. Ilienko, A., Teliushchenko, V., & Dubchak, O. (2023). Suchasni kiberzahrozy krytychnoi infrastruktury Ukrainy ta svitu. *Kiberbezpeka: osvita, nauka, tekhnika*, *27*, 150–164. https://doi.org/10.28925/2663-4023.2023.27.719
7. Murasov, R. K., & Melnyk, Ya. V. (2023). Otsiniuvannia zakhyshchenosti kiberprostoru obiektiv krytychnoi infrastruktury Ukrainy. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony*, *46*(1), 41–44. https://doi.org/10.33099/2311-7249/2023-46-1-41-44
8. Mohale, V. Z., & Obagbuwa, I. C. (2025). Evaluating machine learning-based intrusion detection systems with explainable AI: Enhancing transparency and interpretability. *Frontiers in Computer Science*, *7*, Article 1520741. https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2025.1520741/full
9. Murasov, R., Nikitin, A., & Meshcheriakov, I. (2024). Mathematical model of risk assessment of the operation of critical infrastructure objects based on the theory of fuzzy logic. *Social Development and Security*, *14*(5), 166–174. https://doi.org/10.33445/sds.2024.14.5.17
10. Triantaphyllou, E. (2000). *Multi-Criteria Decision Making: A Comparative Study*. Dordrecht, The Netherlands: Kluwer Academic Publishers (now Springer). ISBN 0-7923-6607-7. https://www.csc.lsu.edu/trianta/Books/DecisionMaking1/backup/Book_DM1.htm?utm_source=chatgpt.com
11. Shapovalova, O. O., & Burmenskyi, R. V. (2017). Rozrobka prohramnoho dodatka dlia realizatsii metodu analizu iierarkhii. *Systemy obrobky informatsii*, *3*(149), 45-48. https://doi.org/10.30748/soi.2017.149.09
12. Mockor, J., & Hynar, D. (2021). On unification of methods in theories of fuzzy sets, hesitant fuzzy set, fuzzy soft sets and intuitionistic fuzzy sets. *Mathematics*, *9*, 447. https://doi.org/10.3390/math9040447
13. Zakon Ukrainy «Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy» vid 05.10.2017 № 2163-VIII (v redaktsii 2025 r.). *Vidomosti Verkhovnoi Rady Ukrainy*, *2017*(45), st. 403. https://zakon.rada.gov.ua/laws/show/2163-19#Text
14. ISO/IEC. (2022). *ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. Geneva, ISO. https://www.iso.org/standard/27001
15. ISA/IEC. (2018). *ISA/IEC 62443. Series of Standards for Industrial Automation and Control Systems Security*. International Electrotechnical Commission. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
16. NIST. (2024). *NIST SP 800-82 Rev. 3. Guide to Operational Technology (OT) Security*. Gaithersburg, MD: National Institute of Standards and Technology. https://csrc.nist.rip/external/nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.ipd.pdf
17. Stevens, R. L., Aliyeva, S., Bornmalm, L., Calvache, C. D., & Ivanov, A. V. (2021, August 14–22). Tools for project scoping: Conceptual modeling of stakeholders, activities and goals. In *Proceedings of the 21st SGEM International Multidisciplinary Scientific GeoConference* (Vol. 2.1, pp. 193–200), Albena, Bulgaria. https://epslibrary.at/sgem_jresearch_publication_view.php?page=view&editid1=7877
18. Hendela, A., & Turoff, M. (2010). Cross impact security analysis using the HACKING Game. In *Proceedings of the 7th International ISCRAM Conference*, Seattle, USA, May 2010. ISCRAM. https://www.researchgate.net/publication/229049304_Cross_Impact_Security_Analysis_using_the_HACKING_Game