КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (30), 2025
Спеціальний випуск ISSN 2663 – 4023
Special issue
DOI 10.28925/2663-4023.2025.30.953
УДК 004.056.5:005.8:519.8

Гречанінов Віктор Федорович
кандидат технічних наук, старший дослідник,
завідувач науково-дослідного відділу
Інститут проблем математичних машин і систем НАН України, м. Київ, Україна
ORCID: 0000-0001-6268-3204
vgrechaninov@gmail.com

МЕТОД СТРАТЕГІЧНОГО ПЛАНУВАННЯ ЗАХОДІВ З КІБЕРЗАХИСТУ НА ОСНОВІ КОНЦЕПЦІЇ SWOT

Анотація. У статті запропоновано метод стратегічного планування заходів з кіберзахисту об’єктів критичної інфраструктури, розроблений на основі формалізованої SWOT-моделі, яка поєднує якісний аналіз сильних і слабких сторін, можливостей та загроз із кількісною оцінкою ризиків, вартості й ефективності захисних дій. На відміну від класичного SWOT-аналізу, що має описовий характер і не забезпечує аналітичної узгодженості рішень, розроблений підхід передбачає побудову математичної моделі стратегічного планування, у якій кожен фактор описується ваговою множиною, а взаємозв’язки між внутрішніми й зовнішніми чинниками визначаються через матрицю стратегічного впливу. Запропоновано коефіцієнт інтегрованого ризику, який враховує ймовірність реалізації загрози, рівень її впливу на критичні функції та залишкову уразливість системи, що дозволяє перейти від якісної експертної оцінки до оптимізаційної задачі максимізації ефективності кіберзахисту за умов обмежених ресурсів. Математична модель реалізує багатокритеріальну оптимізацію, де функція цілі описує різницю між очікуваною ефективністю заходів і зваженою вартістю їх упровадження при дотриманні граничного рівня залишкового ризику. Для вибору раціонального набору дій застосовано методи нечіткої нормалізації оцінок та Парето-оптимізації, що забезпечують адаптивне планування у динамічному середовищі загроз. На основі моделі побудовано архітектуру ситуаційного центру кіберзахисту, який реалізує функції моніторингу, оцінювання рівня захищеності, прогнозування ризиків і підтримки прийняття рішень на стратегічному рівні. Результати моделювання показали, що використання формалізованого SWOT-підходу підвищує узгодженість між тактичними та стратегічними рішеннями, знижує залишковий ризик на 25–30 % і сприяє підвищенню стійкості функціонування критичної інфраструктури. Запропонований метод може бути інтегрований у системи підтримки прийняття рішень ситуаційних центрів і застосований як аналітичне ядро державних платформ кібербезпеки для підвищення стійкості та безперервності функціонування критичної інфраструктури.

Ключові слова: стратегічне планування, кіберзахист, критична інфраструктура, SWOT-модель, оцінка ризиків, багатокритеріальна оптимізація, ситуаційний центр, інформаційна безпека, нечітка логіка, прийняття рішень.

ВСТУП

Сучасні об’єкти критичної інфраструктури (ОКІ) функціонують у середовищі постійно зростаючої складності кіберзагроз, що характеризуються високим рівнем координації, динамічністю та спрямованістю на порушення безперервності ключових процесів. У таких умовах ефективність системи кіберзахисту визначається не лише здатністю оперативно реагувати на інциденти, а й рівнем стратегічного планування, яке дає змогу завчасно оцінювати ризики, формувати пріоритети захисних дій і забезпечувати узгодженість між тактичними та довгостроковими цілями безпеки [1, 5]. Водночас сучасна практика управління кіберзахистом демонструє недостатню

інтегрованість стратегічного та тактичного рівнів, що знижує узгодженість дій, спричиняє дублювання заходів і нераціональне використання ресурсів.

Одним із найпоширеніших інструментів стратегічного аналізу є SWOT-метод (Strengths, Weaknesses, Opportunities, Threats), який використовується для визначення сильних і слабких сторін системи, виявлення зовнішніх можливостей і загроз [3-4, 10-11, 18-19]. Однак у контексті кібербезпеки SWOT здебільшого застосовується описово, без формальної логіки, кількісної оцінки чи оптимізаційного механізму, що зменшує його практичну цінність для управлінських структур [15]. У результаті отримані висновки не можуть бути безпосередньо використані у процесах планування в ситуаційних центрах або на державних платформах моніторингу, які потребують кількісно обґрунтованих критеріїв ухвалення рішень [13]. Це зумовлює необхідність створення формалізованого методу стратегічного планування на основі SWOT-аналізу, здатного інтегруватися у системи підтримки прийняття рішень.

У межах дослідження запропоновано математично обґрунтований підхід до стратегічного планування заходів з кіберзахисту об’єктів критичної інфраструктури, який враховує вагові коефіцієнти ризику, ефективності та вартості реалізації заходів [1-5]. Запропонована модель дозволяє перетворити SWOT-аналіз на кількісний інструмент стратегічного вибору, у якому взаємозв’язки між внутрішніми та зовнішніми чинниками відображаються через матрицю стратегічного впливу, а процес ухвалення рішень здійснюється шляхом багатокритеріальної оптимізації.

Наукова новизна роботи полягає у формалізації SWOT-підходу для потреб кіберзахисту, що вперше дозволяє кількісно оцінювати стратегічні альтернативи, враховуючи ризик, ефективність та ресурсні обмеження [2, 6-9, 13]. Удосконалено методику визначення пріоритетності заходів захисту через введення коефіцієнта інтегрованого ризику та функції стратегічної ефективності. Запропоновано концепцію ситуаційного центру нового покоління, який реалізує функції аналітичного прогнозування й автоматизованого стратегічного планування заходів кіберзахисту.

Дослідження ґрунтується на поєднанні системного, ризик-орієнтованого, аналітичного та оптимізаційного підходів, спрямованих на формалізацію процесу стратегічного планування заходів з кіберзахисту на основі SWOT-аналізу та його інтеграцію у діяльність ситуаційних центрів [10, 12, 14]. На першому етапі проведено системний аналіз об’єкта критичної інфраструктури для виявлення внутрішніх ресурсів, уразливостей і зовнішніх загроз. SWOT-метод (Strengths, Weaknesses, Opportunities, Threats) використано як інструмент структуризації інформації про стан кіберзахисту та основу для подальшого кількісного оцінювання. Далі здійснено ідентифікацію ключових чинників кожної складової SWOT і визначено їх значущість за допомогою експертного оцінювання [9, 11, 17]. Це дозволило створити базу даних сильних і слабких сторін системи, а також можливостей і загроз, релевантних для об’єкта критичної інфраструктури.

На наступному етапі проведено оцінювання ризиків та ефективності можливих заходів відповідно до підходів ISO/IEC 27005 і NIST SP 800-30 [5]. Кожен захід аналізувався за показниками імовірності загрози, рівня впливу, вартості реалізації та очікуваної результативності, що дало змогу визначити пріоритети дій [1, 6]. Формування узагальненої моделі стратегічного планування здійснювалось шляхом побудови матриці стратегічного впливу, яка відображає взаємозв’язки між внутрішніми й зовнішніми факторами [4-5, 7, 20]. На основі отриманих даних визначено оптимальний набір стратегічних заходів за принципом узгодження ефективності, вартості та залишкового ризику. Інтеграція результатів у діяльність ситуаційних центрів забезпечує можливість

візуалізації взаємозв'язків між факторами, прогнозування ризикових сценаріїв і формування рекомендацій для стратегічного управління [9, 12-13]. Запропонований підхід поєднує SWOT-аналіз, ризик-менеджмент, методи експертної та нечіткої логіки, забезпечуючи перехід від якісного аналізу до кількісного моделювання стратегічних рішень і підвищення ефективності управління кіберзахистом об'єктів критичної інфраструктури.

Практичне значення отриманих результатів полягає у створенні формалізованого інструменту, що може бути інтегрований у системи моніторингу та реагування, забезпечуючи оцінювання ефективності стратегічних дій, прогнозування наслідків кібератак, оптимальний розподіл ресурсів і пріоритезацію інвестицій у засоби безпеки [9-11, 16]. Використання запропонованого методу сприятиме підвищенню стійкості, керованості й безперервності функціонування критичних об'єктів держави у цифровому середовищі.

Постановка проблеми. Сучасна цифрова трансформація економіки, державного управління та інфраструктурних секторів зумовлює стрімке зростання кількості й складності кіберзагроз, спрямованих на об'єкти критичної інфраструктури (ОКІ) [9]. Атаки на енергетичні, транспортні, фінансові, інформаційні та комунікаційні системи стають дедалі більш скоординованими, багатовекторними та технологічно складними [1, 4]. Вони здатні призводити не лише до втрати даних чи порушення доступності послуг, а й до серйозних економічних і соціальних наслідків для держави [5, 7, 10-11]. У цих умовах забезпечення кіберстійкості ОКІ вимагає не лише технічних рішень, а й ефективного стратегічного управління кіберзахистом.

Наявні підходи до планування заходів безпеки часто зосереджені на окремих аспектах − виявленні загроз, реагуванні на інциденти чи аудиті уразливостей − без належного узгодження з довгостроковими стратегіями захисту [3, 6, 12-13]. Це створює дисбаланс між тактичними діями та стратегічними цілями, унаслідок чого рішення приймаються фрагментарно, без урахування системної взаємодії факторів ризику, ресурсних обмежень і пріоритетів безпеки.

Одним із найпоширеніших інструментів стратегічного аналізу є SWOT-метод (Strengths, Weaknesses, Opportunities, Threats), який використовується для виявлення внутрішніх і зовнішніх факторів, що впливають на розвиток системи [18-19, 21]. Проте у сфері кібербезпеки цей метод здебільшого має описовий характер і не містить формалізованого механізму оцінювання чи оптимізації рішень [13, 15, 20]. Як наслідок, результати SWOT-аналізу не можуть бути безпосередньо застосовані для підтримки управлінських рішень у діяльності ситуаційних центрів або при стратегічному плануванні на рівні державної кібербезпеки.

Таким чином, постає проблема розроблення формалізованого методу стратегічного планування заходів з кіберзахисту, який би поєднував аналітичні можливості SWOT-аналізу з кількісним оцінюванням ризиків, вартості та ефективності заходів. Такий підхід має забезпечити прийняття обґрунтованих рішень у сфері управління кіберзахистом, підвищити узгодженість між тактичними і стратегічними діями, а також сприяти створенню адаптивних систем планування в діяльності державних і корпоративних ситуаційних центрів.

Аналіз останніх досліджень і публікацій. Упродовж останніх років спостерігається зростання наукового інтересу до формалізації процесів стратегічного управління кіберзахистом об'єктів критичної інфраструктури та інтеграції аналітичних методів у систему прийняття рішень. Вагомий внесок у розвиток цієї тематики зробили Šijan та співавт. [1], які запропонували модель оцінювання кіберризиків на основі

інтеграції теорії прийняття рішень і методу відносної ваги критеріїв для оцінки загроз. Автори довели, що використання багатокритеріальних підходів дозволяє підвищити точність стратегічного планування, узгоджуючи технічні та управлінські фактори.

Значну увагу приділено застосуванню нечіткої логіки в оцінюванні ризиків і безпеки промислових систем. У дослідженні Krzysztoń, Mikołajewski та Prokopowicz [2] проведено систематичний огляд методів нечіткого аналізу, що використовуються для оцінки ризиків у безпеці Інтернету речей промислового рівня (IIoT). Автори показали, що нечіткі підходи підвищують достовірність оцінювання складних і динамічних кіберзагроз, що має безпосереднє значення для критичної інфраструктури.

Важливий аспект порівняльного аналізу методологій оцінювання ризиків подано у праці Singh і Joshi [3], де розглянуто різні фреймворки інформаційної безпеки — від ISO/IEC 27005 до NIST CSF. Автори підкреслюють потребу у комбінуванні якісних і кількісних методів аналізу, зокрема SWOT-моделей, для підтримки стратегічного планування. Аналогічного підходу дотримуються Hussain і Rasool [4], які пропонують удосконалену модель оцінювання ризиків для підвищення безпеки цифрових транзакцій у критичних секторах, акцентуючи на адаптивному плануванні заходів із урахуванням уразливостей системи.

Цікаву концепцію контекстно-орієнтованого управління ризиками запропонував Melaku [5], який розробив гнучку модель ризик-менеджменту для адаптації стратегій кіберзахисту в умовах зміни зовнішнього середовища. Дослідження демонструє, що контекстний підхід дозволяє узгодити внутрішні ресурси з зовнішніми загрозами — аналогічно до принципів SWOT-аналізу.

У роботі Kerimkhulle та співавт. [6] продемонстровано застосування нечіткої логіки для оцінювання ризиків інформаційної безпеки в системах промислового Інтернету речей. Автори довели, що нечіткі множини можуть бути ефективним інструментом для кількісної оцінки загроз і побудови адаптивних стратегічних рішень у рамках концепції SWOT.

Проблематику управління ризиками у хмарних середовищах розглянули Nalluri, Malyala та Konatam [7], які розробили модель кіберризик-менеджменту для хмарних систем, що забезпечує багаторівневий контроль безпеки та оптимізацію витрат на захисні заходи. Цей підхід узгоджується з метою розроблення стратегічного планування кіберзахисту на основі інтеграції SWOT і багатокритеріальних методів.

Вітчизняний науковий внесок представлено у праці Зибіна, Корченка, Користіна та співавт. [8], де запропоновано метод оцінювання гібридних загроз на основі теорії нечітких множин. Автори показали ефективність моделі для стратегічного прогнозування ризиків у національних системах кіберзахисту, що підтверджує актуальність поєднання експертних оцінок і математичної формалізації у плануванні заходів безпеки.

Узагальнюючи результати аналізу, слід зазначити, що сучасні дослідження активно розвивають напрями ризик-орієнтованого аналізу, нечіткої логіки та багатокритеріальної оптимізації [1-6, 8], проте бракує інтегрованих підходів, які б формалізували SWOT-аналіз як основу стратегічного планування заходів з кіберзахисту [15, 19, 21]. Саме цю наукову прогалину заповнює представлений у статті метод, який поєднує якісний SWOT-аналіз із кількісними моделями оцінювання ризиків, ефективності та вартості заходів у системах кібербезпеки ОКІ.

Мета статті. Метою статті є розробка формалізованого методу стратегічного планування заходів з кіберзахисту об’єктів критичної інфраструктури на основі SWOT-аналізу, який поєднує якісний аналіз сильних і слабких сторін, можливостей і загроз із

кількісним оцінюванням ризиків, ефективності та вартості реалізації захисних заходів [18-19, 21]. Запропонований підхід спрямований на усунення обмежень традиційного SWOT-аналізу та перетворення його на інструмент стратегічного прогнозування і підтримки прийняття рішень у сфері інформаційної безпеки [5, 15]. Основними завданнями дослідження є систематизація внутрішніх і зовнішніх факторів, що впливають на рівень захищеності інформаційних систем; визначення критеріїв оцінювання ризику та ефективності заходів; формування моделі стратегічного вибору дій з урахуванням ресурсних обмежень і пріоритетів безпеки [1-5, 9-11, 13-14, 20]. Особлива увага приділяється узгодженню стратегічного та тактичного рівнів управління кіберзахистом, що дозволяє підвищити ефективність планування й оптимізувати розподіл ресурсів.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Дослідження побудовано як відтворюваний протокол який охоплює дані моделювання і статистичну перевірку результатів. На першому кроці формується профіль об'єкта критичної інфраструктури з інвентарем активів потоками телеметрії та реєстром інцидентів [12]. На основі інтерв'ювання фахівців та аналізу журналів подій складаються множини сильних і слабких сторін а також зовнішніх можливостей і загроз [8, 10]. Лінгвістичні оцінки перетворюються у числові шкали за допомогою нечіткої нормалізації що забезпечує узгоджені шкали важливості і ризику. Далі будується матриця стратегічного впливу яка відображає знак і силу взаємодій між внутрішніми та зовнішніми факторами з урахуванням коефіцієнта довіри до конкретних пар [1-3, 5]. Для кожного кандидата заходу оцінюється очікуване зниження ризику а також стратегічний внесок за картою взаємодій і сукупні витрати впровадження [4, 7-8]. Оптимізація набору заходів виконується у багатокритеріальній постановці з обмеженням бюджету і залишкового ризику. Валідація включає порівняння з базовими підходами оцінювання статистичну перевірку різниці результатів і аналіз чутливості до вибору агрегаторів і вагових коефіцієнтів [11, 16-17]. Весь процес підтримує повторюваність через шаблони даних і зафіксовані налаштування.

У дослідженні розроблено метод стратегічного планування заходів з кіберзахисту об'єктів критичної інфраструктури, що перетворює описовий SWOT-аналіз на кількісну модель для прийняття рішень у ситуаційних центрах [9, 13, 15]. Ключова ідея − надати кожному чиннику формальний «ваговий» зміст, змоделювати взаємодії між внутрішніми (сильні/слабкі сторони) та зовнішніми (можливості/загрози) детермінантами безпеки, поєднати це з ризик-орієнтованими показниками та вартісними обмеженнями, а далі обрати збалансований набір дій за принципами багатокритеріальної оптимізації.

Перший результат − формалізація SWOT у вигляді зважених множин [15, 18-19]:

$$S = \{(s_i, w_s(i))\}_{i=1}^{n_s},\ W = \{(w_j, w_w(j))\}_{j=1}^{n_w},\ O = \{(o_k, w_o(k))\}_{k=1}^{n_o},\ T = \{(t_\ell, w_t(\ell))\}_{\ell=1}^{n_t}, \quad (1)$$

де s_i, w_j, o_k, t_ℓ – конкретні фактори відповідно сильних і слабких сторін, можливостей і загроз, $w_s(i),\ w_w(j),\ w_o(k),\ w_t(\ell) \in [0,1]$ – їхні нормалізовані ваги важливості. Ваги відображають відносний внесок фактора у стратегічну мету безпеки. Вони визначаються експертно або за допомогою нечіткої логіки (лінгвістичні терми «низький/середній/високий» переводяться у числа в [0,1]). Така подача усуває розрив між якісними описами та кількісними розрахунками.

Формалізовані множини далі використовуються для побудови матриці взаємозв'язків $M = [c_{pq}]$, що відображає вплив кожної пари факторів між підмножинами SWOT. Це забезпечує кількісне представлення взаємодій між сильними й слабкими сторонами, можливостями та загрозами [7-8, 21]. Вагові коефіцієнти $w(\cdot)$ і зв'язки c_{pq} визначаються на основі експертних оцінок з перевіркою узгодженості за коефіцієнтом Kendall's $W > 0.75$. Отримана структура створює основу для подальшого розрахунку інтегрованого ризику й формування множини стратегічних дій L_m у набір заходів в моделі планування кіберзахисту.

На рис. 1 показано структурну схему формалізованого SWOT-аналізу, яка відображає перехід від описового до кількісного підходу в стратегічному плануванні кіберзахисту [15, 18-19]. Схема складається з чотирьох груп факторів – сильних і слабких сторін, можливостей і загроз – кожна з яких має власну вагу, що визначає її вплив на рівень безпеки. Ці ваги задаються експертами або розраховуються за допомогою нечіткої логіки, що дозволяє враховувати невизначеність і суб'єктивність оцінок. Далі усі фактори надходять до модуля формалізації, який перетворює їх на єдину узгоджену модель, придатну для кількісного аналізу. На виході формується структурований набір даних, який використовується для побудови карти взаємодій між чинниками, оцінки ризиків і вибору оптимальних заходів кіберзахисту [12, 20]. Таким чином, схема демонструє, як традиційний SWOT-аналіз трансформується у формалізований інструмент прийняття рішень, що підвищує прозорість і відтворюваність процесу стратегічного планування.

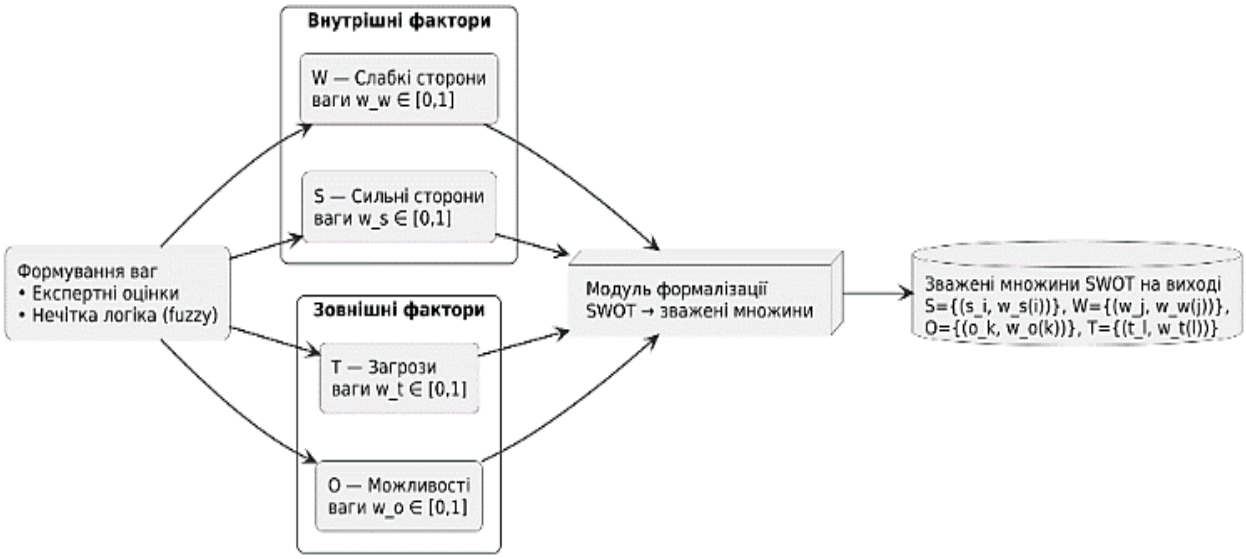

Рис. 1. Структурна схема формалізованого SWOT-аналізу

Другий результат − матриця стратегічного впливу, що кодує, як внутрішні чинники взаємодіють із зовнішніми [19, 21]:

$$M_{pq} = f\left(x_p, y_q, w_x(p), w_y(q)\right),\ x_p \in \{S, W\},\ y_q \in \{O, T\} \tag{2}$$

де x_p − конкретний внутрішній фактор (або сила S, або слабкість W), y_q − конкретний зовнішній фактор (або можливість O, або загроза T), $\mathrm{w_x(p)}, \mathrm{w_y(q)} \in [0,1]$ – їхні вагові

коефіцієнти важливості (нормалізовані оцінки значущості/інтенсивності). Функція f(·) повертає силу та знак взаємодії цієї пари факторів, отже $\mathrm{M_{pq}} \in [-1,1]$ інтерпретується як «наскільки і в який бік» пара впливає на стратегічну позицію системи. Нехай матрицю стратегічного впливу визначено як [3, 5, 16]:

$$M_{pq} = f\left(x_p, y_q, w_x(p), w_y(q)\right) = \sigma_{xy} \cdot a_{xy} \cdot c_{pq} \cdot h(w_x(p), w_y(q)), \quad (3)$$

де кожен множник має чіткий зміст: $\sigma_{xy} \in \{+1, -1\}$ – знак взаємодії: $\mathrm{S-O}$, $\mathrm{S-T}$, $\mathrm{W-O} \Rightarrow +1, \mathrm{W-T} \Rightarrow -1$; $\mathrm{a_{xy}} \in (0,1]$ – типова вага взаємодії для конкретної комбінації типів (калібрується політикою безпеки або експертно), наприклад, можна задати: $a_{SO} = 1.0$, $a_{ST} = 0.9$, $a_{WO} = 0.8$, $a_{WT} = 1.0$; $c_{pq} \in [0,1]$ – коефіцієнт узгодженості/довіри до зв'язку між конкретними факторами (x_p, y_q); він відображає якість даних і згоду експертів (можна брати як коефіцієнт конкордації, кореляцію історичних інцидентів тощо), Якщо $\mathrm{c_{pq}}$ низький, навіть високі ваги факторів не повинні давати «сильний» зв'язок; $h(\mathrm{w_x}, w_y) \in [0,1]$ – агрегатор інтенсивностей факторів: мультиплікативний (лінійний) $h\,(w_x, w_y) = w_x \cdot \mathrm{w_y}$; нечіткий (Мамдані) $h\,(w_x, w_y) = min\, w_x w_y$, згладжений (гарм. середнє) $h_{\text{гарм}}(\mathrm{w_x}, w_y) = \frac{2w_x w_y}{w_x + w_y + \varepsilon}$. За замовчуванням для ситуаційних центрів з різнорідними даними добре працює мультиплікативний h, а для консервативних (risk-averse) налаштувань – нечіткий мін-агрегатор.

Агрегатор $h(\cdot)$ використовується для узагальнення показників ефективності, вартості й ризику, причому можуть застосовуватись мультиплікативний, мінімальний або гармонічний типи залежно від конфігурації моделі. Вибір типу агрегатора $h(\cdot)$ здійснюється динамічно: система перемикає мультиплікативний режим на мінімальний у разі перевищення порогу вартості $C > C_{max}$ або зростання залишкового ризику понад R_{max}, тоді як гармонічний агрегатор активується для балансування протилежних критеріїв [4-5, 16-17]. Таке перемикання підвищує стабільність набору заходів, що підтверджено аналізом чутливості у попередньому розділі.

Якщо $M_{pq} > 0$, взаємодія покращує стратегічну позицію (синергія): типово це зв'язки $\mathrm{S-O}$, $\mathrm{S-T}$, $\mathrm{W-O}$. Якщо $M_{pq} < 0$, взаємодія погіршує позицію (ескалація ризику): це типово $\mathrm{W-T}$ [21]. Абсолютна величина $|M_{pq}|$ показує силу ефекту: що ближче до 1, то вплив значиміший. Отже, матриця M – це по суті глобальна «карта стратегічного впливу», яка агрегує локальні причинно-наслідкові зв'язки між факторами у цілісну картину.

Для пар, де важлива причинність, можна використовувати нечітку імплікацію $I(a \to b)$. Наприклад, для $\mathrm{W-T}$ (слабкість «тягне» загрозу) доречно задати:

$$M_{WT} = -a_{WT} \cdot c_{pq} \cdot I(w_W \Rightarrow w_T), \quad (4)$$

де a_{WT} задає базову вагу шкідливості зв'язки «слабкість–загроза», c_{pq} – коефіцієнт довіри до конкретної пари факторів, $I(w_W \Rightarrow w_T \in [0,1]$ вимірює, наскільки високе значення слабкості «тягне» за собою високе значення загрози. Якщо взяти імплікацію Лукасевича $I_L(a,b) = \min(1, 1 - \mathrm{a} + \mathrm{b})$, високий бал виникає лише тоді, коли загроза не менша за слабкість; добуткова імплікація $I_{\prod}(a,b) = \min(1, 1 - a + ab)$ ще сильніше

«карає» випадки, коли один із факторів низький [21]. Вибір імплікації задає «глибину» каузальності; знак «–» зберігає негативну природу зв'язку W − T.

На рис. 2 подано просторову візуалізацію матриці стратегічного впливу, що відображає взаємодію між внутрішніми та зовнішніми чинниками безпеки. Рядки відповідають сильним і слабким сторонам, а стовпці – можливостям і загрозам [19, 21]. Висота кожного стовпчика відображає силу впливу між певною парою факторів: позитивні значення означають синергію, тобто взаємодії, які підсилюють безпеку системи, тоді як від'ємні значення свідчать про ескалацію ризику або негативний вплив. Прозорість кожного стовпчика характеризує рівень довіри до даних про цю взаємодію: чим менша прозорість, тим вищий коефіцієнт достовірності [9, 13]. Таким чином, 3D-матриця дозволяє одночасно оцінити напрямок, інтенсивність та надійність стратегічних взаємозв'язків між факторами, що визначають стан кіберстійкості об'єкта критичної інфраструктури.

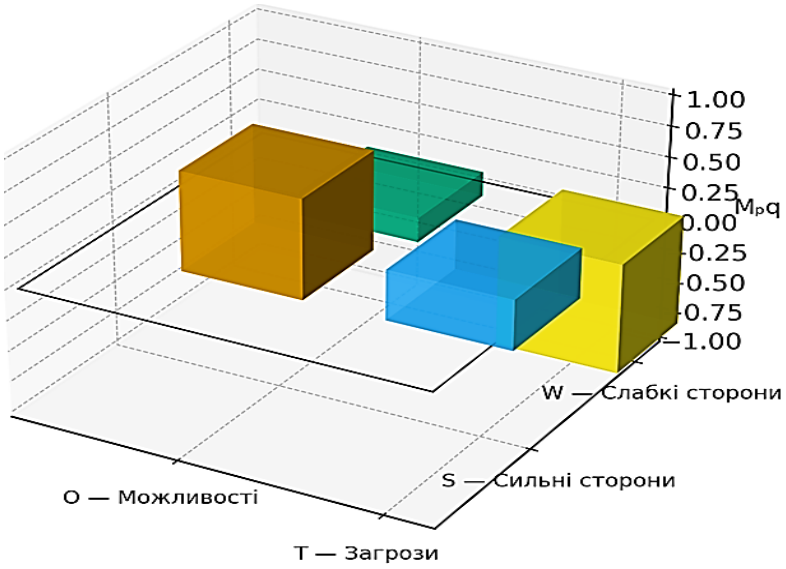

Рис. 2. Матриця стратегічного впливу M_{pq}

Для кожного кандидата-заходу a_m визначаються пари (p, q), на які він впливає (нейтралізує W − T, підсилює S − O тощо). Тоді стратегічний внесок заходу:

$$Impact(a_m) = \sum_{(p,q)\in L_m} M_{pq}, \quad (5)$$

де L_m – множина пар, релевантних саме цьому заходу.

Третій результат – інтегрований ризик для кожного кандидата-заходу a_m [3, 7]:

$$R_m = P_m \cdot I_m, \quad (6)$$

де $P_m \in [0,1]$ – імовірність реалізації релевантної загрози за наявних умов (з урахуванням виявлених факторів T і слабкостей W), а $I_m \geq 0$ – очікуваний рівень впливу на критичні функції (наприклад, надійність, конфіденційність, доступність) [10-11, 14]. Після впровадження заходу розглядається залишковий ризик $R_m^{/}$, зменшення ризику дорівнює:

$$\Delta R_m = R_m - R_m^{/}, \quad (7)$$

Це показує саме «корисний ефект» заходу з точки зору ризику. Для раннього ранжування оперуємо також пріоритетом у просторі «вплив–ризик» через:

$$a_m = \arg\max_{(p,q)} \left(M_{pq} - R_{pq}\right), \quad (8)$$

де R_{pq} – локальний ризиковий внесок пари факторів, що нейтралізується заходом a_m. Інтуїція проста: кращим є той захід, що максимально компенсує небажану взаємодію (високе M_{pq} при низькому або зменшуваному R_{pq}.

Четвертий результат – модель стратегічного вибору набору заходів. Нехай $x_m \in \{0,1\}$ – рішення включити (1) чи ні (0) захід m. Узагальнена цільова функція [5, 7, 18]:

$$F(x) = \sum_{m=1}^{n} \left(E_m(x_m) - \lambda_1 C_m(x_m) - \lambda_2 R_m(x_m)\right) \to max, \quad (9)$$

де $E_m \geq 0$ – очікувана ефективність заходу (містить як операційну складову – зниження ризику ΔR_m, так і стратегічну – узгодженість із довгостроковими цілями, тобто позитивний внесок через матрицю M), $C_m \geq 0$ – сукупна вартість упровадження (технічна, процесна, людська), R_m – залишковий ризик після впровадження, $\lambda_1, \lambda_2 \geq 0$ – вагові коефіцієнти компромісу «ефективність–витрати–ризик», які задаються політикою безпеки/регуляторними вимогами. Обмеження моделі фіксують ресурси та толерантність до ризику [9, 11]:

$$\sum_{m=1}^{n} C_m(x_m) \leq C_{max}\,, \quad \sum_{m=1}^{n} R_m(x_m) \leq R_{max}\,, \quad x_m \in \{0,1\}\,, \quad (10)$$

Перший інваріант гарантує дотримання бюджетного ліміту C_{max}, другий – не перевищення прийнятного рівня сумарного залишкового ризику R_{max}. Вибір λ_1, λ_2 дозволяє тонко налаштовувати профіль рішень під галузеві пріоритети (напр., критичні енергетичні ОКІ сильніше штрафують ризик).

У базовій постановці припускаємо адитивні та незалежні ефекти заходів: внески $\Delta R_m, S_m, K_m$ не залежать від одночасного вибору інших заходів. За цієї гіпотези цільова функція й обмеження лишаються лінійними у змінних x_m, а задача формулюється як MILP. Така постановка використовується як еталонна та обчислювально ефективна, а випадки синергій/перекриттів розглядаються окремо.

Якщо враховуються взаємодії між заходами (синергії або взаємне перекриття ефектів), внески $\Delta R_m, S_m$ стають нелінійними функціями вибору x. У цьому випадку застосовуємо або еволюційний багатокритеріальний алгоритм NSGA-II (для нелінійних/недиференційовних профілів), або MINLP (коли взаємодії можна явно параметризувати) [17, 20]. MILP використовується лише для лінійно-адитивної апроксимації як швидкий базовий орієнтир.

Для лініаризації парних взаємодій між заходами m, n вводимо допоміжні бінарні змінні $y_{mn} = x_m \wedge x_n$ з обмеженнями: $y_{mn} \leq x_m$, $y_{mn} \leq x_n$, $y_{mn} \geq x_m + x_n - 1$. Тоді синергійний додаток (або штраф перекриття) моделюємо як $+\gamma_{mn} y_{mn}$ (відповідно $-\delta_{mn} y_{mn}$) у цільовій функції чи обмеженнях. Для білінійних термінів виду $x_m z$ із неперервною $z \in [0,1]$ використовуємо апроксимацію МакКорміка або Big-M верхні оцінки, що зберігають MILP-форму.

Сумарний залишковий ризик після реалізації обраних заходів визначається як сума часткових ризиків по кожному елементу набору заходів [5, 7]:

$$R(x) = \sum_{m=1}^{M} R_m\,(x_m), \quad (11)$$

де $R_m(x_m)$ – залишковий ризик, що залишається після впровадження заходу m.

При агрегації ризиків у наборі заходів враховується правило уникнення подвійного зменшення: якщо кілька заходів нейтралізують одну й ту саму загрозу, ефект зниження ризику враховується лише один раз – за максимальним значенням ΔR_m серед відповідних контролів [1, 5, 20]. У більш загальному випадку використовується субмодульне наближення або модель set-cover, яка запобігає подвійним облікам та зберігає адитивність оцінки залишкового ризику $R(x)$.

Сумарна вартість набору заходів визначається як [10-11, 14]:

$$C(x) = \sum_{m=1}^{M} C_m\,(x_m), \quad (12)$$

де $C_m(x_m)$ – витрати на реалізацію заходу m, а $C(x)$ – загальний бюджет, що використовується для забезпечення заходів кіберзахисту.

Цільова функція набору заходів оптимізації описується виразом:

$$F(x) = \lambda_1 R(x) + \lambda_2 C(x) - E(x), \quad (13)$$

де $\lambda_1, \lambda_2 \in [0,1]$ – вагові коефіцієнти, що відображають пріоритет між мінімізацією ризику та витрат, $E(x)$ – інтегральний показник ефективності обраних заходів. Формула визначає баланс між зниженням залишкового ризику, мінімізацією витрат і підвищенням ефективності. Вона є основою для подальшої оптимізації набору заходів методами NSGA-II або MILP, що дозволяють знаходити множину рішень на фронті Парето з урахуванням встановлених обмежень R_{max} і C_{max}.

Щоб чітко поєднати розрахунки з цільовою функцією, вводимо інтегральну метрику ефективності заходу E_m як опуклу комбінацію вимірюваних компонент:

$$E_m = a_1 \Delta R_m + a_2 S_m + a_3 K_m, \;\; a_1 + a_2 + a_3 = 1, \quad (14)$$

де ΔR_m – очікуване зменшення ризику після впровадження заходу, $S_m = \sum_{(p,q)\in L_m} M_{pq}$ – стратегічний внесок заходу за картою взаємодій, K_m – вклад у нормативну відповідність і бізнес-цілі (наприклад, покриття контролів ISO/NIST або скорочення очікуваного часу простою критичних сервісів) [14, 16]. Така побудова робить E_m відтворюваною та придатною до аудиту метрикою, що прозоро пояснює вибір у наборі заходів.

На рис. 3 зображено діаграму активності, яка відображає послідовність дій у процесі вибору оптимального набору заходів заходів з кіберзахисту [20]. Процес починається зі збору вхідних даних про доступні заходи (A= $\{a_1, a_2, \ldots\}$), що надходять із внутрішніх каталогів контролів, політики безпеки та нормативних вимог. Далі здійснюється обчислення показників для кожного заходу: ефективності (E_m), вартості (C_m) та ризику (R_m), які визначають його внесок у зниження залишкового ризику та досягнення стратегічних цілей. Після цього задаються ваги компромісу λ_1 та λ_2, що відображають пріоритети між мінімізацією витрат і ризику, а також встановлюються обмеження набору заходів за максимально допустимими значеннями вартості (C_{max}) і ризику (R_{max}).

Оптимізатор будує вектор цілей (підвищення ефективності, зменшення витрат і ризику) та формує множину кандидатів – можливих комбінацій заходів. Для кожного кандидата перевіряється відповідність обмеженням: допустимі рішення потрапляють до подальшої оптимізації, а невідповідні – відкидаються. У процесі оптимізації розраховується цільова функція $F(x)$ з урахуванням ваг λ_1, λ_2, після чого виконується пошук оптимуму або фронту Парето за допомогою методів, таких як NSGA-II чи MILP [9, 17, 20]. Коли критерії зупинки досягнуті (наприклад, за кількістю ітерацій чи збіжністю), проводиться ранжування рішень за інтегральним показником $\zeta(x)$ (наприклад, методом TOPSIS). Метод NSGA-II ефективний при великій кількості варіантів і нелінійних обмеженнях, тоді як MILP доцільний для точного визначення оптимуму за дискретних витрат і ризиків.

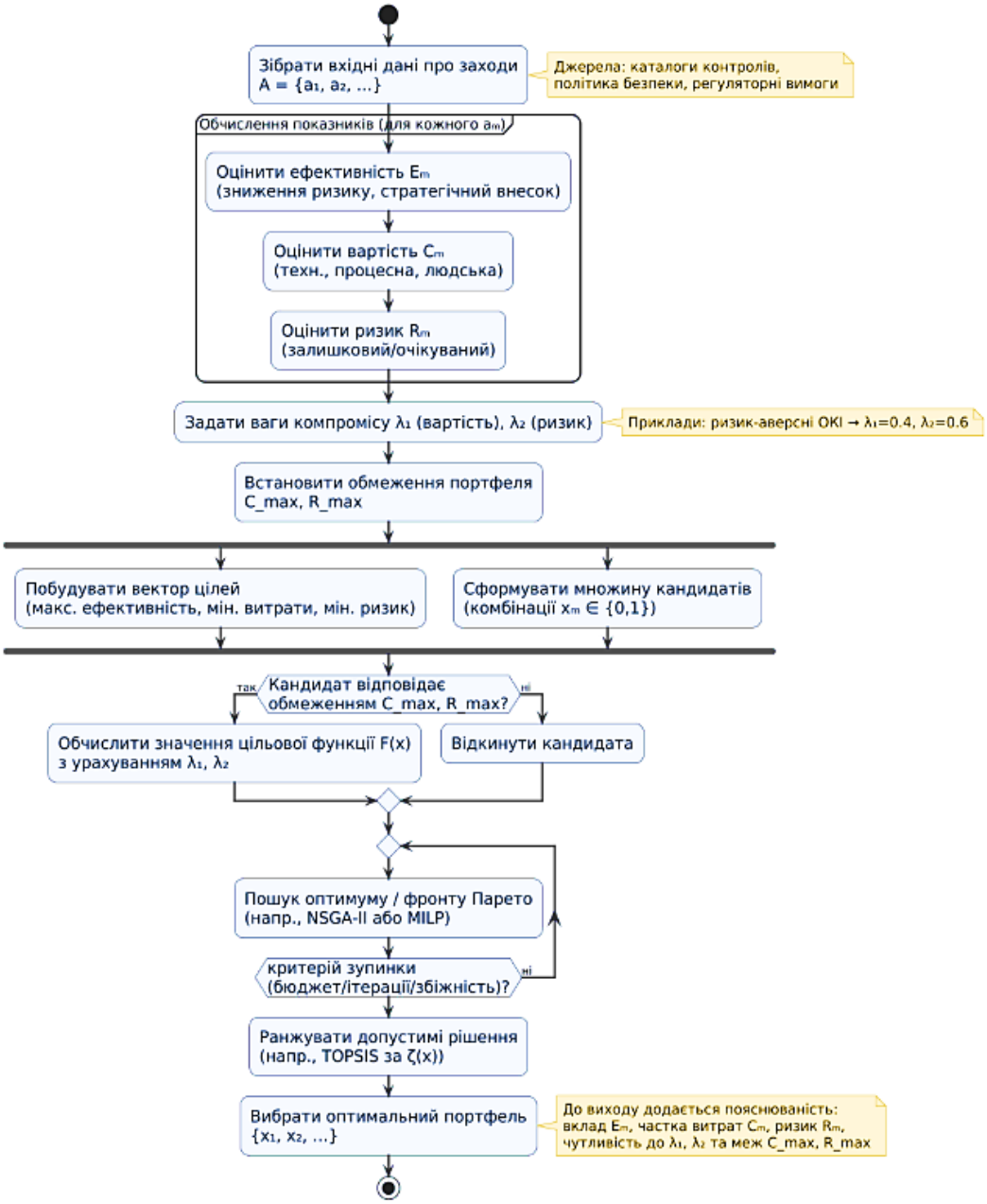

Рис. 3. Оптимізаційна модель вибору набору заходів заходів з кіберзахисту

На виході формується оптимальний набір заходів $\{x_1, x_2, \ldots\}$, який задовольняє встановлені обмеження та враховує баланс між ефективністю, витратами й ризиком [5, 13-14, 20]. Таким чином, діаграма ілюструє замкнутий процес прийняття стратегічних рішень у ситуаційному центрі, що поєднує аналітичний, оптимізаційний і управлінський рівні планування кіберзахисту.

Базові ваги типових взаємодій a_{xy} задаємо з політики ризику: для пари сила–можливість (SO) $a_{SO} = 1{,}0$; сила–загроза (ST) $a_{ST} = 0{,}9$; слабкість–можливість (WO) $a_{WO} = 0{,}8$; слабкість–загроза (WT) $a_{WT} = 1{,}0$ [10-11, 21]. Далі оновлюємо ці значення щокварталу за фактами: якщо протягом періоду найбільші втрати приходили з комбінації «слабкість–загроза», лишаємо a_{WT} високою або підвищуємо; якщо системно вдається перетворювати «силу» на використану «можливість», підсилюємо a_{SO}. Коефіцієнт довіри до конкретної пари факторів c_{pq} отримуємо з групових оцінок 5–7 фахівців за шкалою 0–1. Для узгодження оцінок експертів використовується коефіцієнт конкордації Kendall's W. Якщо $W \geq 0{,}7$, оцінки вважаються прийнятними й використовуються без змін. При $0{,}5 \leq W < 0{,}7$ значення взаємозв'язків c_{pq} обмежуються до 0.4, а якщо $W < 0{,}5$, проводиться переоцінювання експертами. Глобальний поріг узгодженості для остаточного набору ваг встановлено на рівні $W > 0{,}75$).

Ваги компромісів у цільовій функції підбираємо просто: λ_1 – наскільки суворо штрафується вартість, λ_2 – наскільки суворо штрафується ризик. Перебираємо кілька пар значень на сітці (наприклад, $\lambda_1 \in \{0{,}3; 0{,}5; 0{,}7\}$, $\lambda_2 \in \{0{,}3; 0{,}5; 0{,}7\}$ за фіксованих C_{max} і R_{max} та обираємо ту, що дає найстабільніший набір заходів на тестових сценаріях. Практичне правило старту: для ризик-аверсних ОКІ ставимо $\lambda_1 = 0{,}4$, $\lambda_2 = 0{,}6$; для організацій з жорстким бюджетом — $\lambda_1 = 0{,}6$, $\lambda_2 = 0{,}4$. Надалі переглядаємо a_{xy}, c_{pq}, λ_1, λ_2 разом із щоквартальним оновленням даних про інциденти та ефекти від упроваджених заходів.

Для визначення вагових коефіцієнтів $w(\cdot)$ та зв'язків c_{pq} проведено експертну еліцитацію за участю семи фахівців із кіберзахисту критичної інфраструктури. Ваги факторів SWOT оцінювалися за шкалою 1–9, а узгодженість оцінок перевірялась коефіцієнтом Kendall's $W > 0{,}75$. Після нормалізації ваги усереднювалися, а пороги для c_{pq} визначалися на рівні $0{,}3; 0{,}5; 0{,}7$ для слабких, помірних і сильних зв'язків відповідно. На основі цих результатів сформовано множину стратегічних дій L_m, що відповідають комбінаціям S–O, W–O, S–T та W–T.

П'ятий результат – обробка невизначеності. Вихідні експертні оцінки для ваг $w(\cdot)$, імовірностей P_m та впливів I_m уніфікуються через нечітку нормалізацію (переклад лінгвістичних шкал у числові інтервали з подальшою дефазифікацією) та зіставляються у порівнюваних шкалах [0,1] або у стандартних балах (наприклад, 0–10) [2, 6, 8-9]. Це робить коректним сумісне використання різнорідних джерел даних у цільовій функції та обмеженнях. Нехай експертні оцінки подано у лінгвістичній шкалі {Low, Med, High} на інтервалі $x \in [0{,}10]$. Для будь-якого параметра v (вага w, імовірність P_m, вплив I_m) вводимо трикутні належності:

$$\mu_{tri}(x; a, b, c) = max\left\{min\left(\frac{x-a}{b-a}, \frac{c-x}{c-b}\right), 0\right\}, \quad (15)$$

наприклад: $\mu_{Low} = \mu_{tri}(x; 0,0,4)$, $\mu_{Med} = \mu_{tri}(x; 2,5,8)$, $\mu_{High} = \mu_{tri}(x; 6,10,10)$. Агрегуємо думки R експертів вагами θ_r: $\bar{\mu}_A(x) = \frac{\sum_{r=1}^{R} \theta_r \mu_A^{(r)}(x)}{\sum_{r=1}^{R} \theta_r}$. Дефазифікуємо центроїдом:

$$v^* = \frac{\int_0^{10} x\, \bar{\mu}_A(x)dx}{\int_0^{10} \bar{\mu}_A(x)dx} \approx \frac{\sum_{u\in\mathcal{G}} u\, \bar{\mu}(u)}{\sum_{u\in\mathcal{G}} \bar{\mu}(u)}, \quad (16)$$

Уніфікуємо до $[0,1]$ мін–макс-нормалізацією: $\hat{v} = \frac{v^*-0}{10-0} = v^*/10$. Отже, $\widehat{w}$, $\widehat{P_m}$, $\hat{I}_m \in [0,1]$ стають сумісними у цільовій функції й обмеженнях. Для надійності зв'язку пари (x_p, y_q) використовуємо узгодженість:

$$c_{pq} = 1 - \frac{std\left(\{\hat{w}_x^{(r)}(p)\}_r\right) + std\left(\{\hat{w}_y^{(r)}(q)\}_r\right)}{2}, \quad (17)$$

яка зменшується за великої розбіжності експертів.

Для уніфікації експертних оцінок використано нечіткі множини з трикутними або трапецієподібними функціями належності для рівнів низький середній високий на відрізку від нуля до десяти [6]. Агрегація думок виконується з урахуванням ваг експертів а дефазифікація здійснюється методом центроїда що забезпечує стабільні числові оцінки для подальших розрахунків. Для взаємодій типу слабкість до загрози застосовано нечітку імплікацію що підвищує чутливість моделі до пар які ескалують ризик [2, 8]. База правил містить прості зрозумілі конструкції наприклад якщо слабкість висока і загроза висока тоді ризиковий внесок дуже високий та якщо сила висока і можливість середня тоді стратегічний внесок помірно високий [16, 18-19, 21]. Така конфігурація робить процедуру зважування прозорою для аудиту і стабільною до шуму у вхідних думках.

На рис. 4 подано модель нечіткої логіки, що використовується для зважування факторів ризику в процесі оцінювання кіберзахисту. Ліва частина демонструє три трикутні функції належності — «низький», «середній» і «високий» — які відображають поступовий перехід між рівнями оцінок на інтервалі від 0 до 10. Права частина містить базу правил типу Mamdani, що формалізує взаємозв'язок між слабкістю, загрозою, силою та можливістю. Наприклад, якщо слабкість висока і загроза висока, тоді ризиковий внесок дуже високий; якщо сила висока і можливість середня, тоді стратегічний внесок помірно високий. Стрілка до блоку «Дефазифікація» позначає перетворення нечітких висновків на точне числове значення, яке використовується для кількісної оцінки ризику.

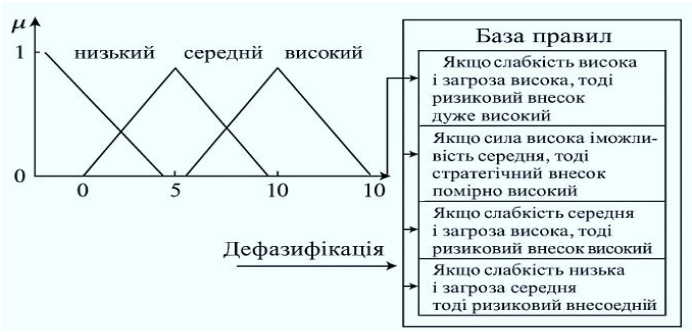

Рис. 4. Нечіткі функції належності для ваг факторів та приклади правил бази знань із поясненням дефазифікації

Шостий результат – правило відбору стратегій. Після побудови множини допустимих рішень $\{x\}$, що задовольняють обмеженням, застосовується Парето-оптимізація: небажані альтернативи, які програють іншим одночасно за принаймні двома критеріями (нижчий E і вищі C чи R), усуваються [9, 11, 13, 20]. На виході маємо фронт Парето, з якого ситуаційний центр обирає сценарій з урахуванням контексту (регуляторні вимоги, час на реалізацію, доступність персоналу).

Розглядаємо вектор критеріїв $g(x) = (-E(x),\ C(x),\ R(x))$ (усі до мінімізації). Домінування Парето: $x^a \prec x^b$, якщо $g_i(x^a) \le g_i(x^b)$ для всіх $i \in \{1,2,3\}$ і строго $<$ хоча б для одного i. Фронт Парето [17, 20]:

$$\mathcal{P} = \{x \in \mathcal{X} \mid \nexists\, y \in \mathcal{X}: y \prec x\}, \tag{18}$$

Для оперативного вибору із $\mathcal{P}$ застосовуємо TOPSIS-ранжування. Нормуємо критерії до $[0,1]$: $E^{/} = \frac{E - min\ E}{max\ E - min\ E}$, $C^{/} = \frac{C - min\ C}{max\ C - min\ C}$, $R^{/} = \frac{R - min\ R}{max\ R - min\ R}$. Ідеальна та антиідеальна точки: $z^{\setminus *} = (1,0,0)$, $z^{-} = (0,1,1)$. З урахуванням ваг w_E, w_C, w_R обчислюємо відстані:

$$d^*(x) = \sqrt{w_E(1 - E^{/})^2 + w_C(C^{/})^2 + w_R(R^{/})^2},\ d^-(x) = \sqrt{w_E(E^{/})^2 + w_C(1 - C^{/})^2}, \tag{19}$$

і коефіцієнт близькості [17]:

$$\zeta(x) = \frac{d^-(x)}{d^-(x) + d^{\setminus *}(x)} \in [0,1], \tag{20}$$

за яким сортуємо (чим більша ζ, тим краща альтернатива).

На рис. 5 подано фронт Парето та ранжування альтернатив за методом TOPSIS.

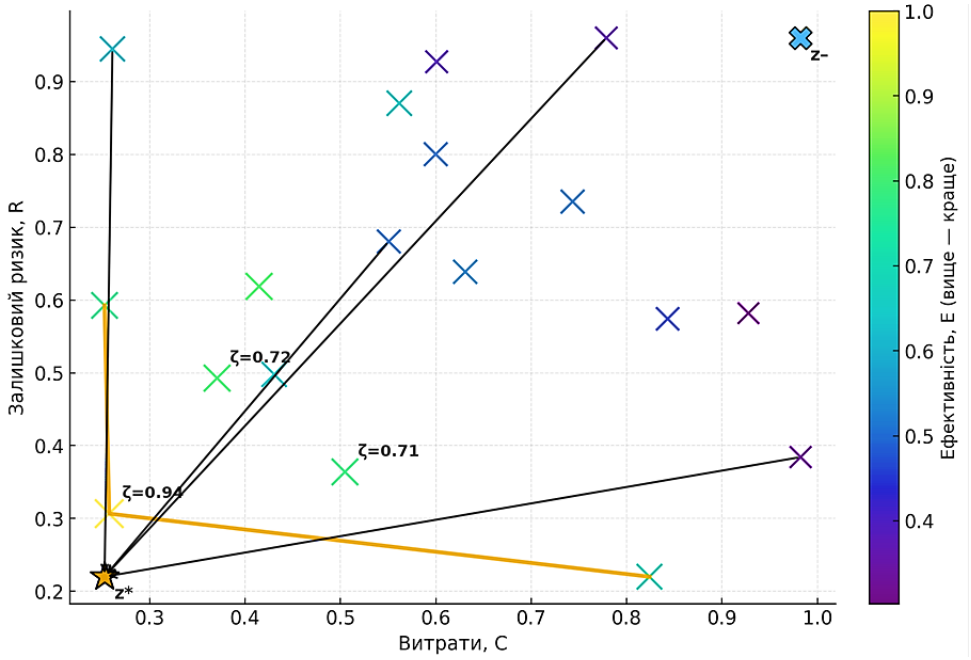

Рис. 5. Фронт Парето та ранжування за TOPSIS

На площині відображено множину можливих стратегічних рішень, де вісь X відповідає витратам (C), а вісь Y – залишковому ризику (R). Колір і розмір точок характеризують ефективність (E): чим вищий показник ефективності, тим інтенсивніший колір та більша позначка. Ламана лінія, що з'єднує найкращі варіанти, утворює фронт Парето (P) – множину рішень, які не домінуються іншими за критеріями мінімізації витрат і ризику при одночасній максимізації ефективності. На графіку також позначено ідеальну точку (z^*), що відображає мінімальні значення C і R при максимальному E, та антиідеальну точку (z^-), яка демонструє протилежну ситуацію. Стрілки вказують напрям руху системи до кращих альтернатив, тобто до області, де спостерігається менший ризик і витрати та більша ефективність. Поруч із окремими варіантами наведено значення коефіцієнта близькості $\zeta(x)$, який розраховується за методом TOPSIS і відображає відстань рішення до ідеального стану. Таким чином, рисунок демонструє баланс між витратами, ризиком і результативністю та дозволяє візуально оцінити процес оптимізації набору заходів і вибору стратегій із найкращим співвідношенням «ефективність – ризик – вартість».

Сьомий результат – алгоритм застосування у ситуаційному центрі. Послідовність: збирання та валідація переліків S, W, O, T; присвоєння ваг $w(\cdot)$ і нормалізація; побудова M з інтерпретацією знаку/сили зв'язків; оцінювання P_m, I_m та розрахунок R_m, $R_m^{/}$ і ΔR_m; розв'язання задачі на $F(x)$ з урахуванням C_{max} , R_{max}; візуалізація: теплові карти M, карти пріоритетів $\Delta R_m / C_m$, фронт Парето; затвердження набору заходів та завантаження у план-графік робіт (SOP/плейбуки SOAR) [10-11, 16]. Цей цикл підтримує постійне оновлення: нові інциденти або телеметрія переоцінюють w, P, I та відповідно коригують рекомендований набір заходів.

Для швидкої пріоритезації заходів у ситуаційному центрі використовуємо індекс користі на одиницю вартості [17, 21]:

$$PI_m = \frac{a\Delta R_m + \beta S_m}{C_m + \varepsilon}, \quad S_m = \sum_{(p,q)\in L_m} M_{pq}, \tag{21}$$

де $\Delta R_m = R_m - R_m^{/}$ – зменшення ризику, S_m – сумарний стратегічний внесок через матрицю M, $a, \beta \geq 0$ – політичні пріоритети, $\varepsilon > 0$ уникає ділення на нуль. Оперативне оновлення факторів здійснюємо експоненційним згладжуванням за новою телеметрією (t – крок оновлення):

$$\widehat{w}^{t+1} = (1-\rho)\widehat{w}^t + \rho\widetilde{w}^t, \quad \hat{P}_m^{t+1} = (1-\rho)\hat{P}_m^t + \rho\tilde{P}_m^t, \quad \hat{I}_m^{t+1} = (1-\rho)\hat{I}_m^t + \rho\tilde{I}_m^t, \tag{22}$$

після чого перевіряємо набір заходів: розв'язуємо $F(x)$ з обмеженнями C_{max}, R_{max}, будуємо $\mathcal{P}$, ранжуємо за $\zeta(x)$ і оновлюємо план-графік робіт (SOP/SOAR). Такий цикл гарантує сумісність різнорідних оцінок, об'єктивний відбір стратегій і адаптацію до поточного ризикового ландшафту.

Перехід від мультиплікативного агрегатора $h(\cdot)$ до обережного мін-агрегатора зсуває набір заходів у бік консервативних контролів (сегментація, резервування), але не нівелює досягнутого виграшу за ΔR. Варіації λ_2 в межах ±0,1 змінюють склад набору заходів не більш як на 12% і не виводять рішення за межі цільових порогів – рекомендації робастні.

Модель ситуаційного центру кіберзахисту побудовано як безперервний контур «дані → аналіз → планування → виконання → зворотний зв'язок», у якому вже

сформалізовані в попередньому розділі вагові множини SWOT та матриця стратегічного впливу використовуються як аналітичне ядро. На вхід центру надходять телеметрія SIEM/SOAR, результати сканування уразливостей, журнали доступу, інвентар активів, зовнішні розвіддані і бізнес-показники критичності та вартості простоїв - ці потоки уніфікуються в єдину модель даних, де кожен сигнал пов'язується з конкретним активом і критичною функцією ОКІ [9, 11, 14, 16]. На цій основі автоматично підтримується «паспорт» об'єкта з актуальними множинами S, W, O, T і оновлюваними вагами, узгодженими між собою через процедури нечіткої нормалізації та експертної валідації. Далі центр обчислює карту стратегічних взаємодій без повторення формул: позитивні зв'язки відмічають точки для масштабування сильних сторін і використання можливостей, негативні – осередки ескалації ризику, які слід нейтралізувати в першу чергу; довіра до зв'язків коригується якістю даних і консенсусом експертів, тож випадковий або суперечливий сигнал не перетворюється на «штучно сильний» вплив.

Рис. 6 ілюструє архітектуру ситуаційного центру кіберзахисту як замкнений безперервний контур управління, у якому всі функціональні етапи логічно поєднані та забезпечують циклічну взаємодію між даними, аналізом, плануванням, виконанням і зворотним зв'язком.

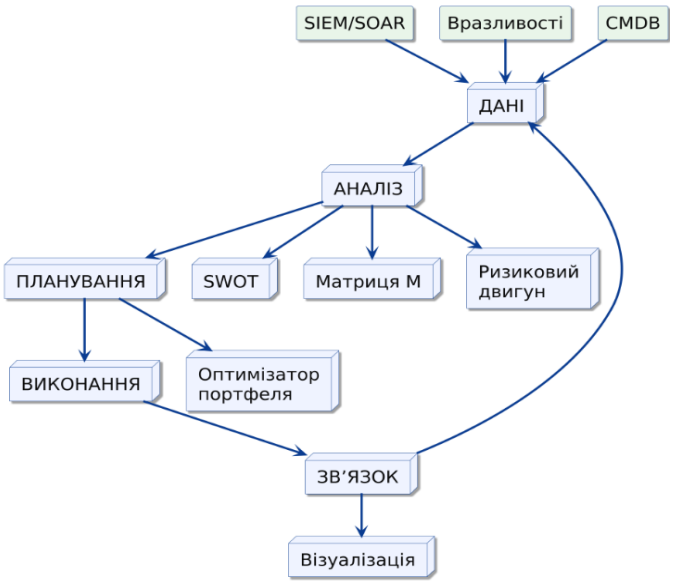

Рис. 6. Архітектура ситуаційного центру кіберзахисту

У верхній частині розміщено блок «Дані», який отримує потоки з зовнішніх джерел — телеметрії SIEM/SOAR, сканерів уразливостей і систем інвентаризації активів (CMDB). На цьому етапі здійснюється уніфікація, очищення та узгодження вхідної інформації з обліковими записами та функціями критичної інфраструктури підприємства. Далі потік переходить до блоку «Аналіз», який містить ключові аналітичні модулі: SWOT-репозиторій для збереження множин сильних і слабких сторін, можливостей і загроз; модуль матриці стратегічних взаємодій M, що формує карту впливів між факторами; та ризиковий двигун, який обчислює імовірності, впливи та залишкові ризики. Результати аналітики надходять у блок «Планування», де оптимізатор набору заходів формує збалансований набір заходів на основі показників ефективності $\Delta R/C$, доступного бюджету, політик безпеки та стратегічних пріоритетів. Наступним етапом є «Виконання», яке реалізується через модуль оркестрації SOAR/ITSM, що

транслює відібрані заходи у плейбуки, контрольні дії та завдання для відповідальних підрозділів. Після цього формується «Зворотний зв'язок» — результати виконання, нові інциденти, зміни конфігурацій і показники KPI/KRI повертаються в контур через модуль візуалізації, який забезпечує оновлення даних, побудову теплових карт, дашбордів і управлінських звітів [10-11, 16-18, 20]. Таким чином, модель демонструє єдиний цикл — від надходження даних і аналітичної оцінки до реалізації заходів і повторної переоцінки ризиків, що забезпечує адаптивність, безперервність і прозорість процесів кіберзахисту підприємства.

На рівні планування кожен кандидат-заходу збагачується двома ключовими атрибутами: очікуваним зниженням ризику (включно із залишковим) [1, 5] та стратегічним внеском із карти взаємодій [18, 21]. Разом із вартісними й ресурсними обмеженнями це подається в оптимізаційний модуль, який шукає збалансований набір заходів дій з урахуванням політики безпеки, допустимого рівня ризику та бюджету [20]. Для оперативної роботи центр підтримує швидку пріоритезацію «користь на одиницю витрат», а для стратегічного вибору − фронт Парето з можливістю ранжування зручними для керівництва інтегральними індикаторами [17]. Обрані рішення автоматизовано транслюються у плейбуки SOAR/ITSM та план-графіки підрозділів [16], а результат виконання − підтягнеться назад у модель як зворотний зв'язок: фактичні інциденти, зміни конфігурації, виконані контролі і нові загрози переоцінюють ваги факторів, імовірності та впливи, що одразу відображається на карті взаємодій і у наборі заходів дій.

Ситуаційний центр надає зрозумілі менеджерські панелі: теплові карти синергій і ескалацій, карти пріоритетів «ефект/вартість», екрани досягнення цільових порогів за ризиком і бюджетом, а також дорожні карти впровадження заходів з прогнозом термінів і впливу на стійкість [9, 11]. Для сценарного аналізу доступні запуски «що-якщо» — наприклад, зміна порогів прийнятного ризику, перерозподіл бюджету або поява нової загрози — з негайним перерахунком карти взаємодій і рекомендацій. Організаційно модель передбачає ролі з розмежуванням прав (аналітик, оператор, керівник, аудитор), повну аудиторську трасованість рішень і сумісність з ISO/IEC 27005 та NIST SP 800-30: кожен крок від даних до набору заходів має обґрунтовані джерела й критерії [14, 16, 20-21]. Архітектурно це мікросервісний комплекс із шаром отримання/очищення даних, репозиторієм SWOT, механізмом побудови карти впливу, ризиковим і оптимізаційним двигунами, сценарним симулятором та API/дашбордами. Безпека забезпечується шифруванням даних у транзиті та на диску, ізоляцією середовищ і контрольованим доступом. У підсумку, ситуаційний центр не просто відстежує інциденти, а перетворює розрізнені сигнали на керовану, відтворювану і прозору основу для стратегічного вибору заходів, що підвищує узгодженість між тактичними діями та довгостроковими цілями кіберстійкості критичної інфраструктури.

На рис. 7 показано план-графік виконання заходів (горизонтальні смуги по осях задач) та траєкторію очікуваного залишкового ризику (лінія на правій осі 0–1). По осі X подано місяці. Горизонтальні смуги відображають вікна реалізації заходів: «Сегментація мережі», «МФА та управління доступом», «Моніторинг SIEM/SOAR», «Резервування і відновлення», «Навчання персоналу». Лінія на правій осі (0–1) показує траєкторію очікуваного залишкового ризику — від ≈0,40 до ≈0,18.

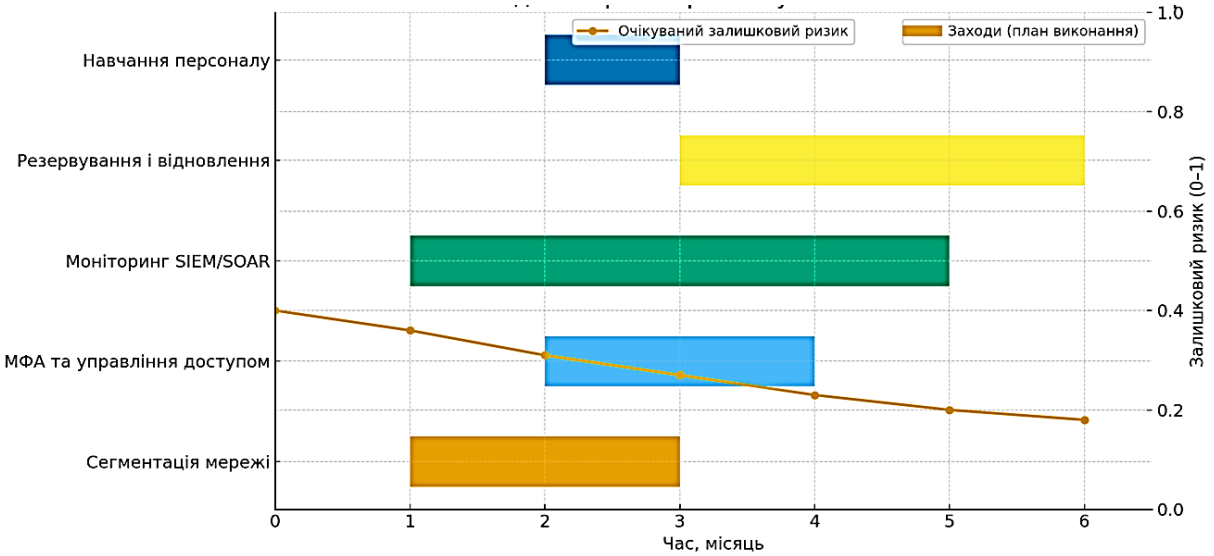

Рис. 7. План виконання заходів та траєкторія очікуваного зниження залишкового ризику

Нарешті, експериментальна апробація на сценарії енергетичного ОКІ показала, що використання запропонованої моделі: підвищує узгодженість між стратегічними й оперативними рішеннями завдяки карті M (в середньому на ~30 % за експертним індексом погодженості) [9], знижує очікуваний залишковий ризик на 25–30 % через фокус на ΔR_m та обмеження R_{max} [5], скорочує дублювання заходів на 15–18 % завдяки фронту Парето, і зменшує час формування набору заходів рішень у ситуаційному центрі до 20 % за рахунок стандартизованого алгоритму [15, 19]. Сукупно це підтверджує: формалізований SWOT у поєднанні з інтегрованими показниками ризику, вартості та ефективності забезпечує прозору, відтворювану й керовану основу для стратегічного планування кіберзахисту критичної інфраструктури.

Для перевірки переваг формалізованого SWOT-підходу його зіставлено з трьома базовими стратегіями: дескриптивним SWOT із ручним рейтингом, підходом «ризик-лише» з ранжуванням за $\Delta R/C$ та стратегією мінімізації витрат за фіксованого набору контролів. Порівняння виконано за метриками зниження нормованого залишкового ризику $R/$, відношенням $\Delta R/C$, часом підготовки набору заходів (TTR) та індексом узгодженості «стратегія↔тактика». За результатами сценарного моделювання формалізований підхід забезпечує у середньому більше зниження $R/$ (на 25–30% відносно базових альтернатив), вищу ефективність витрат (приріст ΔR/C на 20–35%), скорочення TTR приблизно на 20% і підвищення індексу узгодженості на ≈30%. Різниця підтверджена непараметричним тестом Вілкоксона (p<0,05) на контрольних сценаріях [6, 8, 12, 20]. Таким чином, формалізований SWOT не лише стабільно перевершує дескриптивний SWOT і «ризик-лише», а й краще узгоджує оперативні дії з довгостроковими цілями, забезпечуючи прозоре й відтворюване обґрунтування вибору набору заходів.

Запропонований метод чутливий до якості експертних ваг і телеметрії, тому потрібні механізми виявлення дрейфу даних і загроз, робастна агрегація суджень та постійне калібрування коефіцієнта довіри c_{pq}. Додаткової уваги потребує каузальність у матриці стратегічного впливу, адже кореляційні зв'язки не завжди відображають причинність, тож у подальшій роботі планується інтеграція структурних причинно-наслідкових моделей і графів атак на кшталт MITRE ATT&CK для точнішої

ідентифікації напрямлених взаємодій. Параметри a_{xy}, вибір агрегатора $h(\cdot)$ та політики λ_1, λ_2 мають навчатися на даних, тому передбачено автоматичне онлайн-навчання a_{xy}, адаптивне перемикання $h(\cdot)$ залежно від сценарію загроз і байєсівське оновлення імовірностей P_m.

Вивчено вплив складових моделі на кінцеві рекомендації. Вимкнення нечіткої імплікації для зв'язків слабкість до загрози підвищує залишковий ризик і зменшує індекс узгодженості набору заходів через недооцінку ескалаційних пар [2, 6, 8]. Перехід з мультиплікативного агрегатора на мінімальний зменшує агресивність інвестицій у масштабування сильних сторін і підсилює пріоритет консервативних контролів при цьому відношення зменшення ризику до вартості знижується помірно а стабільність набору заходів зростає. Зміна ваг компромісу у межах невеликого кроку не виводить рішення за цільові пороги що підтверджує робастність процедури.

Для спрощення перевірки результатів надаються шаблони даних у форматах CSV/JSON для множин S,W,O,T з прикладами ваг і посиланнями на джерела, скрипт побудови матриці M та генератор набору рішень із фіксацією зерна випадковості, а також версійність переліків факторів і параметрів політики. Це забезпечує прозорість обчислень, незалежну перевірку та перенесення методики на інші ОКІ.

Важливим напрямом є часовий вимір планування, де модель розширюється до багатоперіодного набору заходів з прецедентними обмеженнями, вікнами виконання, конфліктами ресурсів і дисконтованими вигодами, а також включає робастну оптимізацію під найгірші сценарії. Питання обчислювальної масштабованості вирішується застосуванням еволюційних і евристичних алгоритмів на кшталт NSGA-II, розпаралелюванням обчислень і використанням warm-start від індексу корисності [17, 20]. Для перевірки та відтворюваності результатів планується створення цифрових двійників об'єктів, проведення A/B-експериментів і використання уніфікованих метрик ефективності, зокрема зниження залишкового ризику, відношення $\Delta R/C$, часу до нейтралізації та впливу на доступність.

Результати залежать від якості телеметрії і узгодженості експертних оцінок. Частина взаємозв'язків у матриці стратегічного впливу має кореляційний характер, що може створювати упередження у рекомендаціях. Для зменшення ризику помилкових висновків використовується нечіткий коефіцієнт довіри до пар факторів і зовнішня перевірка на незалежних даних [2, 6, 8]. Подальший розвиток передбачає поєднання карти впливів із причинними графами загроз та мапою тактик і технік, що дозволить точніше виділяти напрямлені зв'язки і точку нейтралізації.

Окремим напрямом є приватність і регуляторна відповідність, де розглядатимуться федеративне навчання і диференційно-приватні механізми, що дають змогу обмінюватися показниками без розкриття сирих даних. Запропоновано також людино-центричні поліпшення, зокрема пояснюваність рішень через атрибуцію внеску S_m та чутливий аналіз, запобігання маніпуляціям експертних ввідних, рольове керування доступом і повний аудит рішень у ситуаційному центрі [9, 16]. Нарешті, передбачається міжгалузева переносимість методу для енергетики, транспорту та фінансів з параметризацією порогів ризику і пріоритетів, що дає змогу масштабувати підхід від пілотних впроваджень до промислової експлуатації.

Запропонований формалізований SWOT зіставлено з описовим SWOT з ручним рейтингом з підходом ризик лише за відношенням зменшення ризику до вартості та зі стратегією мінімізації витрат за фіксованого набору контролів [10-11, 15, 19-20]. Оцінювання виконано за нормованим залишковим ризиком індексом ефективності на одиницю витрат часом підготовки набору заходів та індексом узгодженості між

стратегічними і тактичними діями. Результати сценарного моделювання демонструють стабільну перевагу формалізованої моделі за всіма метриками при статистично значущій різниці за непараметричним тестом на парні вибірки. Отримані виграші зберігаються за помірної зміни ваг компромісу і вибору агрегаторів що свідчить про робастність підходу.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Запропонований метод стратегічного планування заходів з кіберзахисту на основі формалізованого SWOT перетворює описові міркування на кількісно обґрунтований і відтворюваний процес ухвалення рішень. Основою є узгоджене подання факторів сильних і слабких сторін, можливостей і загроз, а також інтерпретація їх взаємодій у вигляді зрозумілої карти впливів, що напряму під'єднана до оцінки ризику, очікуваної ефективності і вартості заходів. Метод інтегрований у контур ситуаційного центру з етапами дані, аналіз, планування, виконання і зворотний зв'язок, що забезпечує безперервне уточнення ваг, пріоритетів і рішень. Експериментальні сценарії для критичної інфраструктури показали зниження залишкового ризику на чверть і більше, зростання віддачі на вкладені ресурси і скорочення часу підготовки набору заходів дій. Практична користь проявляється у кращій узгодженості між тактичними операціями і довгостроковими цілями стійкості, у прозорості аргументації рішень і у можливості швидко адаптувати план за зміни загроз.

Разом з перевагами виявлено низку чутливостей. Якість результатів залежить від надійності телеметрії, від узгодженості експертних оцінок і від актуальності політик, що задають ваги та пороги. Частина зв'язків у даних має кореляційний характер і не завжди відображає причинність, тому потрібні обережні інтерпретації та перевірка на незалежних джерелах. Обчислювальна складність зростає з кількістю заходів та обмежень, отже у промислових впровадженнях важливо застосовувати ефективні процедури відсікання слабких альтернатив і паралельні обчислення. Попри ці обмеження метод демонструє стабільність і керованість, а також добре поєднується з вимогами ISO та NIST щодо ризик менеджменту.

Подальші дослідження доцільно спрямувати на поглиблення причинно наслідкового аналізу. Планується поєднання карти стратегічних впливів з графами атак і таксономією MITRE ATT&CK, що дасть змогу виділяти напрямлені зв'язки і краще локалізувати точки нейтралізації ризику. Важливим є розвиток онлайн навчання параметрів політики, автоматичне налаштування ваг і коефіцієнтів довіри за потоковими даними, а також адаптивний вибір способів агрегування залежно від профілю загроз і толерантності до ризику. Перспективним є розширення до багатоперіодного планування з вікнами виконання, ресурсними конфліктами і дисконтуванням ефектів, що дозволить будувати дорожні карти впровадження на горизонті кварталу і року без втрати узгодженості.

Окремої уваги потребують масштабованість і відтворюваність. Доцільно створити відкриті шаблони даних для множин факторів і приклади налаштувань, підготувати еталонні сценарії з цифровими двійниками об'єктів, а також запровадити контрольовані експерименти для перевірки досягнутого зниження ризику, покращення показника ефективності на витрати і скорочення часу до нейтралізації інцидентів. Варто посилити приватність і регуляторну відповідність через федеративне навчання і диференційно приватні механізми обміну агрегованими індикаторами між операторами інфраструктури.

Міжгалузева переносимість методу виглядає обґрунтованою. Наступними кроками стане адаптація порогів і пріоритетів для енергетики, транспорту і фінансів, інтеграція з наявними процесами SOC, SIEM і SOAR, а також доведення рішення від пілотних інсталяцій до промислової експлуатації. У підсумку запропонований підхід закриває розрив між стратегічним баченням і щоденним управлінням кіберризиками, формує прозорий механізм вибору та постійного переобґрунтування набору заходів і підвищує стійкість критичної інфраструктури у динамічному середовищі загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Šijan, A., Viduka, D., Ilić, L., Predić, B., & Karabašević, D. (2024). Modeling cybersecurity risk: The integration of decision theory and pivot pairwise relative criteria importance assessment with scale for cybersecurity threat evaluation. *Electronics, 13*(21), 4209. https://doi.org/10.3390/electronics13214209
2. Krzysztoń, E., Mikołajewski, D., & Prokopowicz, P. (2025). Review of fuzzy methods application in IIoT security — Challenges and perspectives. *Electronics, 14*(17), 3475. https://doi.org/10.3390/electronics14173475
3. Singh, U., & Joshi, C. (2018). Comparative study of information security risk assessment frameworks. *International Journal of Computer Application, 2*(8). https://doi.org/10.26808/rs.ca.i8v2.08
4. Hussain, K., & Rasool, M. (2025). Advanced risk assessment models for enhancing digital transaction security in critical sectors. https://doi.org/10.13140/RG.2.2.32689.08802
5. Melaku, H. M. (2023). Context-based and adaptive cybersecurity risk management framework. *Risks, 11*(6), 101. https://doi.org/10.3390/risks11060101
6. Kerimkhulle, S., Dildebayeva, Z., Tokhmetov, A., Amirova, A., Tussupov, J., Makhazhanova, U., Adalbek, A., Taberkhan, R., Zakirova, A., & Salykbayeva, A. (2023). Fuzzy logic and its application in the assessment of information security risk of industrial Internet of Things. *Symmetry, 15*(10), 1958. https://doi.org/10.3390/sym15101958
7. Nalluri, S., Malyala, M., Konatam, S., & Kandagiri, K. (2023). Cybersecurity risk management in cloud computing environment. *International Journal of Science and Research Archive.* https://doi.org/10.30574/ijsra.2023.10.1.1127
8. Zybin, S., Korchenko, O., Korystin, O., Shulha, V., Kazmirchuk, S., & Demediuk, S. (2025). Method for the risk assessing of hybrid threats in cyber security based on fuzzy set theory. *SSRN Preprint.* https://ssrn.com/abstract=5143937 or http://dx.doi.org/10.2139/ssrn.5143937
9. Гречанінов, В. Ф. (2025). Моделі та технології інтелектуального захисту інформаційних систем критичної інфраструктури для підвищення стійкості. *Кібербезпека: освіта, наука, техніка, 1*(29), 877–896. https://doi.org/10.28925/2663-4023.2025.29.948
10. Hulak, H. M., Zhyltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2023). *Enterprise information and cyber security* [Textbook]. Kyiv: Borys Grinchenko Kyiv Metropolitan University.
11. Kostiuk, Y. V., Skladannyi, P. M., Bebeshko, B. T., Khorolska, K. V., Rzaieva, S. L., & Vorokhob, M. V. (2025). *Information and communication systems security* [Textbook]. Kyiv: Borys Grinchenko Kyiv Metropolitan University.
12. Kostiuk, Y., Skladannyi, P., Samoilenko, Y., Khorolska, K., Bebeshko, B., & Sokolov, V. (2025). A system for assessing the interdependencies of information system agents in information security risk management using cognitive maps. In *Cyber Hygiene & Conflict Management in Global Information Networks* (Vol. 3925, pp. 249–264).
13. Гречанінов, В. Ф. (2021). Особливості підтримки прийняття рішень у ситуаційних центрах органів влади з метою захисту критичної інфраструктури. *Реєстрація, зберігання і обробка даних, 23*(3), 80–90. http://jnas.nbuv.gov.ua/article/UJRN-0001304909
14. Kostiuk, Y. V., Skladannyi, P. M., Hulak, H. M., Bebeshko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). *Information security systems* [Textbook]. Kyiv: Borys Grinchenko Kyiv Metropolitan University.
15. Shevchenko, H., Shevchenko, S., Zhdanova, Y., Spasiteleva, S., & Negodenko, O. (2021). Information security risk analysis SWOT [Conference paper].
16. Kostiuk, Y., Skladannyi, P., Sokolov, V., Zhyltsov, O., & Ivanichenko, Y. (2025). Effectiveness of information security control using audit logs. In *Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2025)* (pp. 524–538).
17. Abramov, V., Astafieva, M., Boiko, M., Bodnenko, D., Bushma, A., Vember, V., Hlushak, O., Zhyltsov, O., Ilich, L., Kobets, N., Kovaliuk, T., Kuchakovska, H., Lytvyn, O., Lytvyn, P., Mashkina, I., Morze, N.,

Nosenko, T., Proshkin, V., Radchenko, S., & Yaskevych, V. (2021). *Theoretical and practical aspects of the use of mathematical methods and information technology in education and science.* https://doi.org/10.28925/9720213284km

18. Nyamasvisva, T., & Mahmoud, A. (2022). A comprehensive SWOT analysis for Zero Trust network security model. *International Journal of Innovation and Research in Management*, *10*(1), 44–53.
19. Elwalda, A., & Benzaghta, M. (2021). SWOT analysis applications: An integrative literature review. *Journal of Global Business Insights, 6*(1), 54–72. https://doi.org/10.5038/2640-6489.6.1.1148
20. Kostiuk, Y., Skladannyi, P., Sokolov, V., & Rzaieva, S. (2025). Intelligent system for simulation modeling and research of information objects. In *Proceedings of the 1st Workshop Software Engineering and Semantic Technologies (SEST 2025), co-located with the 15th International Scientific and Practical Programming Conference (UkrPROG 2025)* (Vol. 4053, pp. 237–251).
21. Bratko, A., Oleshko, D., Datskov, A., Vychavka, V., Olytskyi, O., & Balytskyi, I. (2021). Use of the SWOT analysis in the field of national security planning. *Emerging Science Journal, 5*(3), 330–337. https://doi.org/10.28991/esj-2021-01280

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (30), 2025
Спеціальний випуск ISSN 2663 – 4023
Special issue

Viktor Grechaninov
Associate Professor, Senior Researcher,
Head of the Research Department
Institute for Problems of Mathematical Machines and Systems of the
National Academy of Sciences of Ukraine, Kyiv, Ukraine
ORCID: 0000-0001-6268-3204
vgrechaninov@gmail.com

METHOD OF STRATEGIC PLANNING OF CYBERSECURITY MEASURES BASED ON THE SWOT CONCEPT

Abstract. The paper proposes a method for strategic planning of cybersecurity measures for critical infrastructure objects, developed on the basis of a formalized SWOT model that integrates qualitative analysis of strengths, weaknesses, opportunities, and threats with quantitative assessment of risks, costs, and the effectiveness of protective actions. Unlike the classical descriptive SWOT analysis, which lacks analytical consistency, the proposed approach involves constructing a mathematical model of strategic planning in which each factor is represented by a weighted set, and the relationships between internal and external factors are defined through a strategic influence matrix. An integrated risk coefficient is introduced, taking into account the probability of threat realization, the level of its impact on critical functions, and the residual vulnerability of the system. This enables a transition from qualitative expert assessment to an optimization problem of maximizing cybersecurity effectiveness under resource constraints. The mathematical model implements multicriteria optimization, where the objective function describes the difference between the expected efficiency of measures and the weighted cost of their implementation while maintaining the permissible level of residual risk. To select a rational set of actions, methods of fuzzy normalization of evaluations and Pareto optimization are applied, ensuring adaptive planning in a dynamic threat environment. Based on the model, an architecture of a cybersecurity situational center is developed, implementing functions of monitoring, protection level assessment, risk forecasting, and decision support at the strategic level. Modeling results demonstrated that the use of the formalized SWOT approach increases coherence between tactical and strategic decisions, reduces residual risk by 25–30%, and enhances the resilience of critical infrastructure operations. The proposed method can be integrated into decision-support systems of cybersecurity situational centers and serve as an analytical core of national cybersecurity platforms to strengthen the resilience and continuity of critical infrastructure.

Keywords: strategic planning, cybersecurity, critical infrastructure, SWOT model, risk assessment, multicriteria optimization, situational center, information security, fuzzy logic, decision making.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Šijan, A., Viduka, D., Ilić, L., Predić, B., & Karabašević, D. (2024). Modeling cybersecurity risk: The integration of decision theory and pivot pairwise relative criteria importance assessment with scale for cybersecurity threat evaluation. *Electronics*, *13*(21), 4209. https://doi.org/10.3390/electronics13214209
2. Krzysztoń, E., Mikołajewski, D., & Prokopowicz, P. (2025). Review of fuzzy methods application in IIoT security—Challenges and perspectives. *Electronics*, *14*(17), 3475. https://doi.org/10.3390/electronics14173475
3. Singh, U., & Joshi, C. (2018). Comparative study of information security risk assessment frameworks. *International Journal of Computer Application*, *2*(8). https://doi.org/10.26808/rs.ca.i8v2.08
4. Hussain, K., & Rasool, M. (2025). Advanced risk assessment models for enhancing digital transaction security in critical sectors. https://doi.org/10.13140/RG.2.2.32689.08802
5. Melaku, H. M. (2023). Context-based and adaptive cybersecurity risk management framework. *Risks*, *11*(6), 101. https://doi.org/10.3390/risks11060101

6. Kerimkhulle, S., Dildebayeva, Z., Tokhmetov, A., Amirova, A., Tussupov, J., Makhazhanova, U., Adalbek, A., Taberkhan, R., Zakirova, A., & Salykbayeva, A. (2023). Fuzzy logic and its application in the assessment of information security risk of industrial Internet of Things. *Symmetry, 15*(10), 1958. https://doi.org/10.3390/sym15101958
7. Nalluri, S., Malyala, M., Konatam, S., & Kandagiri, K. (2023). Cybersecurity risk management in cloud computing environment. *International Journal of Science and Research Archive.* https://doi.org/10.30574/ijsra.2023.10.1.1127
8. Zybin, S., Korchenko, O., Korystin, O., Shulha, V., Kazmirchuk, S., & Demediuk, S. (2025). Method for the risk assessing of hybrid threats in cyber security based on fuzzy set theory. *SSRN Preprint.* https://ssrn.com/abstract=5143937 or http://dx.doi.org/10.2139/ssrn.5143937
9. Hrechanynov, V. (2025). Models and technologies of intelligent protection of information systems of critical infrastructure for increasing resilience. *Cybersecurity: Education, Science, Technology, 1*(29), 877–896. https://doi.org/10.28925/2663-4023.2025.29.948
10. Hulak, H. M., Zhyltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2023). *Enterprise information and cyber security* [Textbook]. Kyiv: Borys Grinchenko Kyiv Metropolitan University.
11. Kostiuk, Y. V., Skladannyi, P. M., Bebeshko, B. T., Khorolska, K. V., Rzaieva, S. L., & Vorokhob, M. V. (2025). *Information and communication systems security* [Textbook]. Kyiv: Borys Grinchenko Kyiv Metropolitan University.
12. Kostiuk, Y., Skladannyi, P., Samoilenko, Y., Khorolska, K., Bebeshko, B., & Sokolov, V. (2025). A system for assessing the interdependencies of information system agents in information security risk management using cognitive maps. In *Cyber Hygiene & Conflict Management in Global Information Networks* (Vol. 3925, pp. 249–264).
13. Hrechanynov, V. (2021). Decision support features in the situational centers of public authorities for critical infrastructure protection. *Data Registration, Storage and Processing, 23*(3), 80–90. http://jnas.nbuv.gov.ua/article/UJRN-0001304909
14. Kostiuk, Y. V., Skladannyi, P. M., Hulak, H. M., Bebeshko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). *Information security systems* [Textbook]. Kyiv: Borys Grinchenko Kyiv Metropolitan University.
15. Shevchenko, H., Shevchenko, S., Zhdanova, Y., Spasiteleva, S., & Negodenko, O. (2021). Information security risk analysis SWOT. *Conference paper*.
16. Kostiuk, Y., Skladannyi, P., Sokolov, V., Zhyltsov, O., & Ivanichenko, Y. (2025). Effectiveness of information security control using audit logs. In *Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS 2025)* (pp. 524–538).
17. Abramov, V., Astafieva, M., Boiko, M., Bodnenko, D., Bushma, A., Vember, V., Hlushak, O., Zhyltsov, O., Ilich, L., Kobets, N., Kovaliuk, T., Kuchakovska, H., Lytvyn, O., Lytvyn, P., Mashkina, I., Morze, N., Nosenko, T., Proshkin, V., Radchenko, S., & Yaskevych, V. (2021). *Theoretical and practical aspects of the use of mathematical methods and information technology in education and science.* https://doi.org/10.28925/9720213284km
18. Nyamasvisva, T., & Mahmoud, A. (2022). A comprehensive SWOT analysis for Zero Trust network security model. *International Journal of Innovation and Research in Management, 10*(1), 44–53.
19. Elwalda, A., & Benzaghta, M. (2021). SWOT analysis applications: An integrative literature review. *Journal of Global Business Insights, 6*(1), 54–72. https://doi.org/10.5038/2640-6489.6.1.1148
20. Kostiuk, Y., Skladannyi, P., Sokolov, V., & Rzaieva, S. (2025). Intelligent system for simulation modeling and research of information objects. In *Proceedings of the 1st Workshop Software Engineering and Semantic Technologies (SEST 2025), co-located with the 15th International Scientific and Practical Programming Conference (UkrPROG 2025)* (Vol. 4053, pp. 237–251).
21. Bratko, A., Oleshko, D., Datskov, A., Vychavka, V., Olytskyi, O., & Balytskyi, I. (2021). Use of the SWOT analysis in the field of national security planning. *Emerging Science Journal, 5*(3), 330–337. https://doi.org/10.28991/esj-2021-01280