УДК 004.056.5:005.53:351.746.1
DOI: 10.31673/2409-7292.2025.030762

Домарєв В.В., Прокопович-Ткаченко Д.І, Зверев В.П., Бушков В.Г, Козаченко І.М.

СИТУАЦІЙНО-ОРІЄНТОВАНІ СИСТЕМИ УПРАВЛІННЯ БЕЗПЕКОЮ НА ОСНОВІ УНІФІКОВАНОЇ МАТРИЧНОЇ МОДЕЛІ: ЛОГІКО-ЛІНГВІСТИЧНИЙ ТА МІЖГАЛУЗЕВИЙ ПІДХІД

У статті обґрунтовано концепцію використання уніфікованої матричної моделі як базису для створення ситуаційно-орієнтованих систем управління безпекою (ССУ) в умовах складної багаторівневої загрозової динаміки. Розроблено методику формалізації структурно-функціональних компонентів ССУ на основі логіко-лінгвістичних конструкцій та міжгалузевих матриць, які відображають взаємозв'язки між суб'єктами управління, об'єктами безпеки, типами загроз, формами ризику, політиками реагування та інструментами реалізації захисних заходів. Виокремлено п'ять етапів ситуаційного управління – виявлення загрози, оцінка ризику, визначення альтернатив, прийняття рішень і контроль результативності, – які представлено у вигляді типового циклу управлінської дії. Запропоновано архітектуру інформаційної інтеграції уніфікованої моделі до систем підтримки прийняття рішень (СППР) та ситуаційних центрів у складі загальнодержавної мережі реагування. Продемонстровано приклад практичної реалізації моделі для сценарію міжгалузевої загрози у сфері критичної інфраструктури з багатовимірною оцінкою ефективності. Отримані результати підтверджують доцільність подальшого розвитку системного підходу до ситуаційного управління, орієнтованого на проактивне виявлення загроз і адаптивне реагування в умовах гібридної небезпеки та зростаючої комплексності безпекового середовища.

Ключові слова: ситуаційне управління, уніфікована матрична модель, система безпеки, критична інфраструктура, міжгалузева загроза.

Вступ

Сучасний стан безпеки інформаційних технологій та критичної інфраструктури характеризується складною, багаторівневою та гібридною природою загроз, що постійно еволюціонують у відповідь на впровадження нових технологій та методів управління ризиками [1, 2, 3]. Фундаментальні підходи до забезпечення інформаційної безпеки, розроблені Домарєвим В. В. [1, 2, 3, 7, 8], заклали теоретичну й методологічну базу для формування сучасних систем управління безпекою на основі системного, матричного та ситуаційного підходів. Зокрема, в його роботах детально обґрунтовано принципи побудови захищених IT-систем, формалізації структурно-функціональних зв'язків між суб'єктами та об'єктами захисту, а також алгоритмів інтеграції стандартів ISO 27k для фінансового та банківського секторів [3]. Вагомий внесок у стандартизацію методик захисту інформації зробили нормативні документи НБУ та міжнародні стандарти ISO/IEC 27001 і ISO/IEC 27002 [4, 5, 6], які закріплюють вимоги до побудови систем управління інформаційною безпекою (СУІБ) та підкреслюють важливість ризик-менеджменту, формалізованого оцінювання ефективності захисних заходів та постійного вдосконалення систем [7]. Питання моделювання складних інформаційних та кібернетичних систем, а також формалізації логіко-лінгвістичних і гносеологічних основ управління безпекою висвітлені у класичних роботах [9, 10, 11], які стали основою для побудови багатовимірних матричних і деревоподібних моделей взаємодії між секторами та елементами критичної інфраструктури [8, 12]. Подальший розвиток теорії та практики відбувається завдяки дослідженням міжгалузевої інтеграції інформаційних потоків, використанню мультиагентних систем, баєсівських мереж, елементів штучного інтелекту та систем підтримки прийняття рішень (СППР) у сфері національної та корпоративної безпеки [13-19]. Наукові дисертації, галузеві огляди, а також праці, присвячені формуванню організаційних структур управління ІБ, доповнюють сучасну методологічну базу [13, 14, 15, 16, 17, 18]. Значна увага приділяється розвитку та впровадженню систем управління ризиками, підвищенню кіберстійкості організацій, а також моделюванню поведінки комплексних систем у надзвичайних ситуаціях [20, 21]. У роботах Домарєва та інших сучасних авторів [1, 2, 3, 7, 8] обґрунтовано необхідність переходу до уніфікованих матричних моделей, здатних забезпечити

адаптивність, ситуаційну сумісність і багатовимірний аналіз загроз у реальному часі. Ці підходи поєднують формальні методи, інтелектуальні алгоритми та практичний досвід впровадження у фінансових, банківських, промислових і критичних секторах. Таким чином, наявна теоретична й практична база [1-30] створює умови для подальшого розвитку універсальних ситуаційно-орієнтованих систем управління безпекою, заснованих на уніфікованих матричних, логіко-лінгвістичних та міжгалузевих моделях, які забезпечують гнучкість, адаптивність і проактивність у протидії сучасним загрозам.

Постановка проблеми

Стрімка еволюція гібридних загроз – від цілеспрямованих кібератак до ланцюгових фізико-техногенних інцидентів – зумовила різке зростання кількості міжгалузевих інцидентів, які охоплюють одразу декілька секторів критичної інфраструктури [1]. Сучасні системи управління інформаційною безпекою, побудовані на класичних ієрархічних або галузево-специфічних моделях, не забезпечують належної ситуаційної сумісності: дані залишаються фрагментованими, а аналітичні висновки – несинхронізованими між енергетикою, транспортом, телекомунікаціями й водопостачанням [2]. Унаслідок цього навіть локальні інциденти можуть перерости у каскадні кризи, що порушують безпеку ланцюгів постачання та призводять до значних соціально-економічних збитків [3].

Попри наявність усталених міжнародних стандартів (ISO/IEC 27001, ISO/IEC 27002) і нормативів Національного банку України, ці документи фокусуються переважно на внутрішньогалузевому ризик-менеджменті й не містять інструментів для комплексного обліку міжсекторальних залежностей у режимі реального часу [4], [5]. Низка робіт пропонує використовувати багатовимірні матричні або деревоподібні моделі для формалізації структури ризиків, однак існуючі прототипи залишаються лабораторними й не інтегрують логіко-лінгвістичні правила, необхідні для обробки якісних (нечітких) взаємозв’язків між суб’єктами, об’єктами та загрозами [6], [7].

Додаткову складність створює висока динаміка параметрів ризику: вагові коефіцієнти взаємного впливу, пріоритети політик реагування та ймовірності розвитку подій змінюються швидше, ніж оновлюються традиційні, «жорстко» налаштовані СУІБ. Без адаптивного механізму автоматичного оновлення цих параметрів організації залишаються вразливими до нових сценаріїв атак і не можуть оперативно перерозподіляти ресурси реагування [8].

Отже, актуальною є задача створення уніфікованої матричної моделі, яка:

- формалізує одночасно кількісні (інтенсивність загрози, вартість збитків) та якісні (експертні оцінки, логіко-мовні правила) взаємозв’язки між секторами;
- підтримує багатовимірну оцінку ризику з можливістю швидкого калібрування вагових коефіцієнтів у режимі потоку даних;
- забезпечує ситуаційно-орієнтовану інтеграцію до систем підтримки прийняття рішень (СППР) і мультиагентних середовищ, де різні галузі можуть координувати дії через спільну «карту» ризиків.

Відсутність такої інтегрованої моделі обмежує здатність державних і корпоративних центрів реагування своєчасно виявляти міжгалузеві залежності, прогнозувати каскадні ефекти та обирати оптимальні політики реагування. Тому необхідно розробити й апробувати логіко-лінгвістичну уніфіковану матричну модель, орієнтовану на динамічне, проактивне управління безпекою у складному багаторівневому загрозовому середовищі [9].

Аналіз останніх публікацій

Питання забезпечення інформаційної безпеки та моделювання складних систем управління є предметом активних наукових досліджень як в Україні, так і у світі. Одними з найвагоміших є праці Домарєва В. В., у яких закладено теоретичні та методологічні засади системного підходу до побудови комплексних систем захисту інформації, впровадження методів ризик-менеджменту та формалізації структурно-функціональних зв’язків у безпекових ІТ-інфраструктурах [1, 2, 3]. Зокрема, у [1, 2] розглянуто системний і методологічний підхід

до створення захищених інформаційних систем, а в [3] – питання практичної імплементації міжнародних стандартів серії ISO 27k у банківських установах.

Практичний аспект побудови ієрархічних і матричних моделей для управління безпекою знайшов відображення у роботах Домарєва та співавторів, де запропоновано "матрицю" управління інформаційною безпекою на основі системного підходу [8]. Крім того, обґрунтовано критерії оцінки ефективності захисту та визначено ролі структурних елементів у системах управління [7]. Значний вплив на розвиток нормативної та методичної бази мали міжнародні стандарти ISO/IEC 27001, ISO/IEC 27002, а також національні документи НБУ, у яких формалізовано вимоги до створення систем управління інформаційною безпекою, впровадження політик реагування та методик оцінки ризиків [4, 5, 6]. Їх вплив особливо помітний у банківському, фінансовому та державному секторах.

Теоретичні основи логіко-гносеологічного та кібернетичного моделювання, необхідного для побудови складних багатовимірних моделей взаємодії, закладені у класичних працях Мороза, Шенгерія та Безштанька [9, 10, 11]. Саме ці ідеї лягли в основу логіко-лінгвістичних підходів, які широко застосовуються для формалізації зв'язків у міжгалузевих і міждисциплінарних системах управління безпекою [12, 13, 14]. Останні роки характеризуються активним розвитком методів інтеграції інформаційних потоків із різних секторів критичної інфраструктури – енергетики, транспорту, телекомунікацій, водопостачання тощо [19]. Увага приділяється використанню мультиагентних моделей, баєсівських мереж і штучного інтелекту для прогнозування загроз та прийняття рішень у реальному часі [12, 16, 28].

Запропоновані підходи враховують специфіку гібридних загроз, високий ступінь невизначеності та потребу в гнучких адаптивних моделях реагування [17, 18, 20].Значний масив наукових і прикладних досліджень спрямований на впровадження систем підтримки прийняття рішень (СППР) у сфері безпеки та розвиток методів багатовимірної статистики, кластерного й компонентного аналізу для виявлення прихованих залежностей у структурі ризиків [12, 16, 28]. Окремі роботи присвячені питанням організаційної побудови й вдосконалення управління інформаційною безпекою підприємств і військових частин [13, 18], а також розробці імітаційних і комп'ютерних моделей складних систем [27, 29, 30]. Розвиток методології багаторівневого ситуаційного управління базується на поєднанні формалізованих підходів (матричні, логіко-лінгвістичні моделі), методів міжгалузевої інтеграції та емерджентних технологій (нейронні мережі, глибоке навчання), що забезпечують гнучкість, адаптивність і високий рівень автоматизації у сучасних системах безпеки [1-30]. Огляд джерел підтверджує наявність теоретично обґрунтованої та практично апробованої бази для розробки уніфікованих моделей нового покоління, які забезпечують підвищену стійкість, оперативність та проактивність у реагуванні на сучасні загрози.

Мета і завдання дослідження

Метою цього дослідження є обґрунтування і апробація уніфікованої матричної моделі як базової основи для формування гнучких ситуаційно-орієнтованих систем управління безпекою в умовах багаторівневої загрозової динаміки. Основні завдання дослідження включають аналіз існуючих теоретичних і практичних підходів (з акцентом на спадщину Домарєва), формалізацію структурно-функціональних компонентів на основі логіко-лінгвістичних конструкцій, розробку методики міжгалузевої інформаційної інтеграції та багатовимірної оцінки ефективності реагування, а також вироблення рекомендацій щодо впровадження моделі у СППР і ситуаційні центри [1-30].

Основними завданнями дослідження є:

- аналіз існуючих теоретичних і практичних підходів до моделювання ССУ;
- формалізація структурно-функціональних компонентів на основі логіко-лінгвістичних конструкцій;
- розробка та апробація алгоритмів міжгалузевої інформаційної інтеграції;

© Домарєв В.В., Прокопович-Ткаченко Д.І, Зверев В.П., Бушков В.Г, Козаченко І.М. (2025) Ситуаційно-орієнтовані системи управління безпекою на основі уніфікованої матричної моделі: логіко-лінгвістичний та міжгалузевий підхід. Сучасний захист інформації, 3(63), 56–67.
https://doi.org/10.31673/2409-7292.2025.030762

- створення методики багатовимірної оцінки ефективності реагування;
- вироблення рекомендацій щодо впровадження моделі у СППР та ситуаційні центри.

Методологія дослідження

Методологічна основа дослідження грунтується на поєднанні системного, матричного, логіко-лінгвістичного та міжгалузевого підходів до побудови ситуаційно-орієнтованих систем управління безпекою (ССУ). Формування архітектури таких систем здійснюється з урахуванням множини суб'єктів управління S, об'єктів захисту O, типів загроз T, форм ризику R, політик реагування P, матриць впливу M, а також функцій контролю ефективності F.

Уніфікована матрична модель дозволяє формалізувати міжгалузеві взаємозв'язки шляхом побудови багатовимірної матриці:

$$M = \{m_{s,o,t,r}\}, \tag{1}$$

де $s \in S, o \in O, t \in T, r \in R$, а $m_{s,o,t,r}$ - інтенсивність впливу суб'єкта s на об'єкт o через загрозу t за формою ризику r.

Структурні взаємозв'язки у системі додатково формалізуються логіколінгвістичними правилами та функціями відповідності:

$$L = \{(W, \lambda)\}, \tag{2}$$

де W - вагові коефіцієнти (пріоритети взаємодії), λ - функції відповідності, які задають логічні або ймовірнісні співвідношення між параметрами.

Для врахування невизначеності подій використовується баєсівське оцінювання ймовірності виникнення критичної події для об'єкта o під впливом множини загроз T:

$$P(C_o \mid T) = \frac{P(T \mid C_o) \cdot P(C_o)}{P(T)}. \tag{3}$$

Алгоритм ситуаційного управління включає етапи: автоматизоване виявлення загрози, оцінка ризику на основі багатовимірної матриці та логіко-лінгвістичних правил, визначення альтернативних сценаріїв реагування, прийняття оптимального рішення з використанням СППР, контроль результативності через автоматизований збір зворотного зв'язку та оновлення знань.

Для інтеграції даних з різних галузей використовується оператор трансформації:

$$X = \tau(\{x_i\}_{i=1}^{n}), \tag{4}$$

де x_i - вхідні потоки з і-го сектору, τ - перетворення у спільний формат для побудови уніфікованої матриці ситуації.

У процесі аналізу застосовуються методи багатовимірної статистики, кластеризації загроз, компонентного аналізу для виявлення прихованих залежностей у структурі M. Для сценаріїв багатогалузевої атаки інтегральний ризик визначається як:

$$R_{int} = \sum_{k=1}^{K} w_k \cdot r_k, \tag{5}$$

де w_k - вагові коефіцієнти, що визначають пріоритетність впливу, r_k - значення ризику для k-го напрямку.

У системі реалізовано розподілену взаємодію агентів (ситуаційні центри галузей), які координують дії на основі спільної матриці ризиків. Ефективність реагування аналізується на

основі індексу адаптивності, середнього ризику та часу реакції для кожної галузі. Порівняльна оцінка різних політик реагування здійснюється за імовірністю успіху, вартістю реалізації та часом виконання заходів.

Запропонована методика апробована в сценаріях міжгалузевих загроз для критичної інфраструктури, що дозволяє ідентифікувати точки концентрації ризиків, провести сценарний аналіз та оптимізувати розподіл ресурсів. Застосування елементів штучного інтелекту та мультиагентного моделювання забезпечує динамічне самонавчання системи й підвищення стійкості в умовах гібридних загроз і високої комплексності складних систем.

Для забезпечення гнучкого й адаптивного реагування на сучасні загрози в критичній інфраструктурі розроблено архітектуру ситуаційно-орієнтованої системи управління безпекою (ССУ) рис.1 на основі уніфікованої матричної моделі. Така система інтегрує формалізовані структурні зв'язки, інструменти ситуаційного аналізу, автоматизоване прийняття рішень та механізми мультиагентної взаємодії для підвищення ефективності управління в умовах багаторівневої загрозової динаміки. Схема наочно відображає ключові компоненти, взаємозв'язки між ними та інформаційні потоки в межах єдиного ситуаційного центру.

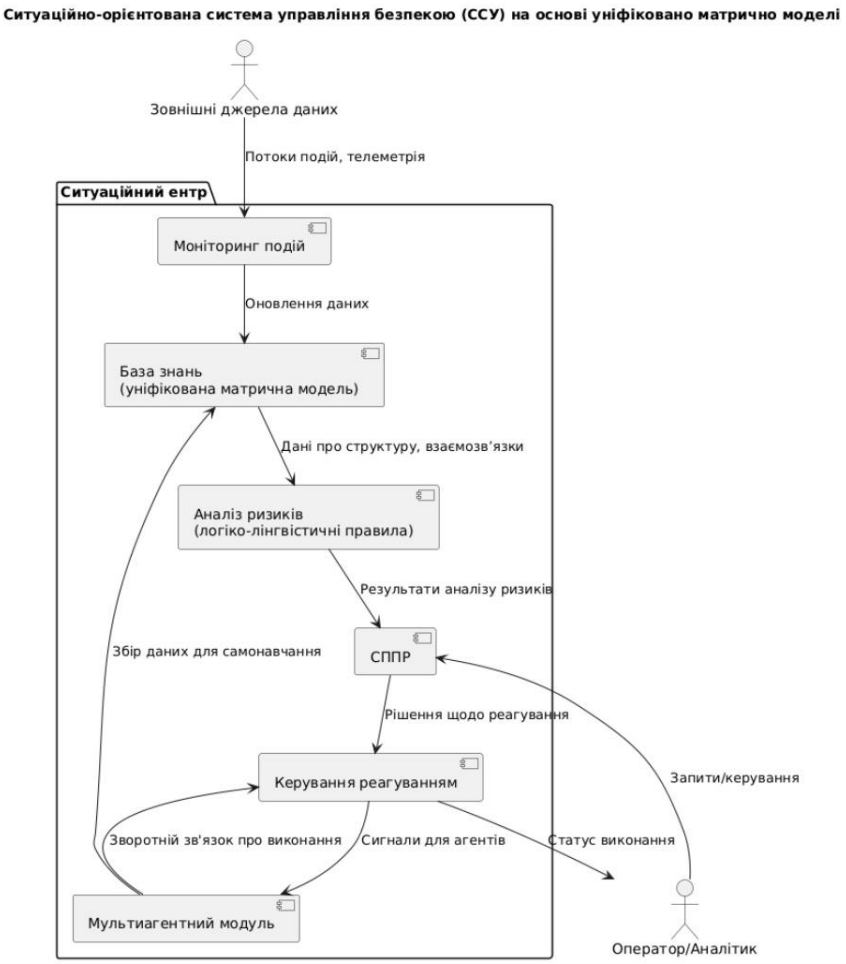

Рис. 1. Архітектурна схема ситуаційно-орієнтованої системи управління безпекою на основі уніфікованої матричної моделі

На рис. 1 зображено логічну структуру ситуаційного центру безпеки, побудовану на уніфікованій матричній моделі:

1. Зовнішні джерела даних (телеметрія, журнали, сенсори різних галузей) забезпечують надходження вхідних потоків у модуль моніторингу подій;

2. Модуль моніторингу подій здійснює первинну обробку та фільтрацію інформації, передаючи релевантні дані до бази знань;

3. База знань містить уніфіковану матричну модель, яка накопичує та формалізує зв'язки між суб'єктами, об'єктами, типами загроз і формами ризику;

4. Модуль аналізу ризиків виконує логіко-лінгвістичну оцінку стану системи, генерує прогнози ймовірних подій, і передає результати у систему підтримки прийняття рішень;

5. СППР (система підтримки прийняття рішень) автоматизує вибір оптимального сценарію реагування, враховуючи рекомендації експертів та аналітичні результатиЧ;

6. Модуль керування реагуванням координує виконання рішень, взаємодіє з мультиагентним модулем для оперативної організації спільних дій;

7. Мультиагентний модуль реалізує децентралізовану взаємодію із ситуаційними центрами інших секторів, забезпечує зворотний зв'язок та збір даних для самонавчання системи;

8. Оператор/Аналітик здійснює контроль за прийнятими рішеннями, має змогу втручатися у процеси та отримувати інформацію про статус реагування.

Уніфікована матрична модель

Для формалізації міжгалузевих взаємозв'язків будується уніфікована матриця M:

$$M = [m_{ijkl}], \quad m_{ijkl} \in [0; 1], \tag{6}$$

де i - суб'єкт, j - об'єкт, k - тип загрози, l - форма ризику. Кожен елемент m_{ijkl} відображає інтенсивність впливу i-го суб'єкта на j-й об'єкт через k-ту загрозу за l-ю формою ризику.

Логіко-лінгвістичне моделювання

Взаємозв'язки між структурними елементами описуються функцією:

$$L(s, o, t, r, p) = \sum_{q=1}^{Q} \alpha_q \cdot \delta_q(s, o, t, r, p), \tag{7}$$

де α_q - вагові коефіцієнти, δ_q - функції відповідності (логічні правила).

Моделювання невизначеності

Ймовірність виникнення критичної події E для об'єкта o під впливом загроз T визначається через баєсівське оцінювання:

$$P(E|T) = \frac{P(T|E) \cdot P(E)}{P(T)}. \tag{8}$$

Алгоритм ситуаційного управління

Розроблений алгоритм реалізує п'ять послідовних етапів:

1. Виявлення загрози за допомогою автоматизованого моніторингу та фільтрації подій;

2. Оцінка ризику на основі багатовимірної матриці та логіко-лінгвістичних правил;

3. Визначення альтернативних сценаріїв реагування з урахуванням наявних ресурсів і політик;

4. Прийняття оптимального рішення з використанням СППР;

5. Контроль результативності — автоматичний збір зворотного зв'язку, оновлення матриці знань.

Інформаційна інтеграція

Для забезпечення міжгалузевої інтеграції даних застосовується механізм трансформації вхідних потоків у уніфіковану структуру, наприклад:

$$I = \mathcal{T}(D_1, D_2, \dots, D_m), \tag{9}$$

де D_j - вхідні потоки від j-го сектору, $\mathcal{T}$ - оператор трансформації у спільний формат.

Застосування методів аналізу даних

У роботі також використано методи багатовимірної статистики, кластеризації загроз, компонентного аналізу для виявлення прихованих залежностей у структурі матриці M.

Побудова міжгалузевої матриці

В експериментальному моделюванні розглянуто інтеграцію енергетичного, телекомунікаційного та транспортного секторів. Побудовано матрицю впливу (табл. 1).

Таблиця 1

Розгорнута таблиця рівнів загроз для секторів критичної інфраструктури

Сектор	Тип загрози	Рівень
Енергетика	Кіберзагрози	0,85
Енергетика	Фізичні загрози	0,78
Енергетика	Техногенні загрози	0,67
Енергетика	Біологічні загрози	0,55
Телекомунікації	Кіберзагрози	0,92
Телекомунікації	Фізичні загрози	0,60
Телекомунікації	Техногенні загрози	0,50
Телекомунікації	Біологічні загрози	0,45
Транспорт	Кіберзагрози	0,70
Транспорт	Фізичні загрози	0,83
Транспорт	Техногенні загрози	0,80
Транспорт	Біологічні загрози	0,51
Водопостачання	Кіберзагрози	0,88
Водопостачання	Фізичні загрози	0,67
Водопостачання	Техногенні загрози	0,59
Водопостачання	Біологічні загрози	0,90

Матриця дозволяє ідентифікувати ключові точки взаємозалежності та потенційні сценарії каскадного розвитку загроз. Таблиця 1 відображає кількісну оцінку рівнів загроз для чотирьох ключових секторів критичної інфраструктури – енергетики, телекомунікацій, транспорту та водопостачання – за чотирма типами загроз: кіберзагрози, фізичні, техногенні та біологічні.

Кожна комбінація сектору та типу загрози представлена числовим значенням, яке характеризує ймовірність або інтенсивність впливу відповідної загрози. Значення варіюються від 0 до 1, де показники, близькі до одиниці, вказують на високий рівень ризику, а ближчі до нуля – на низький. Найвищий рівень кіберзагроз спостерігається у телекомунікаційному секторі (0,92), що свідчить про його особливу вразливість до кіберінцидентів. Біологічні загрози найбільш критичні для сфери водопостачання (0,90), що логічно з огляду на ризик біологічного зараження водних систем.

Транспортний сектор виявляє найбільшу вразливість до фізичних загроз (0,83), пов’язану з його відкритістю до атак і техногенних аварій. У свою чергу, енергетичний сектор є стійкішим до біологічних загроз (0,55), але демонструє високу чутливість до кіберзагроз (0,85) та фізичних впливів (0,78).

Загалом таблиця дозволяє виявити міжгалузеві залежності, провести ранжування загроз за рівнем критичності, визначити точки концентрації ризиків, що потребують першочергового реагування, та сформувати базу для сценарного аналізу і пріоритетного розподілу ресурсів у ситуаційно-орієнтованих системах управління безпекою.

Приклад виявлення ризику

Для сценарію багатогалузевої атаки на критичну інфраструктуру обчислюється інтегральний ризик:

$$R_{int} = \sum_{i,j,k,l} w_{ijkl} \cdot m_{ijkl}, \quad (10)$$

де w_{ijkl} - вагові коефіцієнти, що визначають пріоритетність впливу.

Мультиагентне реагування

Впроваджено схему розподіленої взаємодії агентів (наприклад, ситуаційні центри різних галузей), що координують спільні дії на основі спільної матриці ризиків

Аналіз ефективності реагування

Проведено аналіз результативності реагування на підставі індексу адаптивності:

Таблиця 2

Оцінка ефективності реагування на міжгалузеві загрози

Сектор	Середній ризик	Індекс адаптивності	Час реакції (хв)
Енергетика	0,77	0,82	14
Телекомунікації	0,67	0,75	12
Транспорт	0,77	0,68	19
Водопостачання	0,74	0,71	15

Таблиця 2 узагальнює результати оцінювання ефективності реагування різних секторів критичної інфраструктури на загрози, використовуючи показники середнього ризику, індексу адаптивності та часу реакції. Індекс адаптивності характеризує здатність сектора оперативно та гнучко адаптуватися до змін загрозового середовища, тоді як середній ризик відображає усереднений рівень загрозливості на основі попередніх оцінок. Час реакції вказує на середню тривалість від моменту виявлення інциденту до початку реалізації захисних заходів. Сектор енергетики демонструє високий індекс адаптивності (0,82) при середньому ризику 0,77 та часі реакції 14 хвилин, що свідчить про досить ефективну систему реагування.

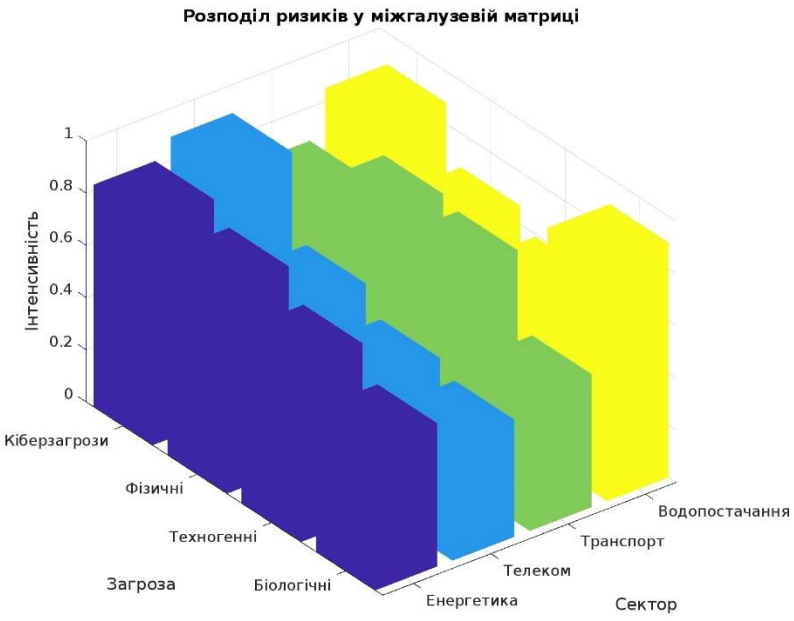

Рис. 2. Тривимірна візуалізація розподілу ризиків по секторах критичної інфраструктури (Гістограма відображає інтегровану оцінку впливу різних типів загроз)

Телекомунікації мають нижчий ризик (0,67) та коротший час реакції (12 хвилин), але індекс адаптивності є помірним (0,75), що вказує на відносну збалансованість системи. Транспорт характеризується високим ризиком (0,77), низьким індексом адаптивності (0,68) та найдовшим часом реакції (19 хвилин), що свідчить про обмежену гнучкість у критичних ситуаціях. Водопостачання демонструє помірний рівень ризику (0,74), невисоку адаптивність (0,71) та середній час реагування (15 хвилин), що вказує на потребу в удосконаленні процедур реагування. Загалом таблиця дозволяє виявити сильні й слабкі сторони секторальних систем безпеки, порівняти їхню адаптивність до загроз і визначити напрями для оптимізації міжгалузевого реагування в умовах динамічного середовища ризиків.

Оцінка варіантів реагування

Порівняно ефективність різних політик реагування з урахуванням мультидисциплінарного підходу (табл. 3).

Таблиця 3

Порівняльний аналіз політик реагування

Політика	Галузь	Імовірність успіху	Вартість ($)	Час виконання (год)
Проактивна	Енергетика	0,93	125000	3
Реактивна	Телеком	0,82	85000	4
Адаптивна	Транспорт	0,87	97000	2
Інтегрована	Водопостачання	0,91	110000	2

Таблиця 3 подає порівняльний аналіз ефективності чотирьох типів політик реагування – проактивної, реактивної, адаптивної та інтегрованої – в контексті окремих галузей критичної інфраструктури. Аналіз базується на трьох ключових параметрах: імовірності успіху, вартості реалізації та часу виконання заходів реагування. Проактивна політика, застосована в енергетичному секторі, демонструє найвищу імовірність успіху (0,93), але супроводжується найбільшою вартістю ($125 000) при порівняно короткому часі виконання (3 години), що вказує на високоефективний, хоча і фінансово витратний підхід. Реактивна політика в телекомунікаціях має найнижчу імовірність успіху (0,82) та найтриваліший час реагування (4 години), хоча характеризується найменшою вартістю ($85 000), що відображає компроміс між вартісною доцільністю та оперативністю. Адаптивна політика, реалізована у транспортному секторі, забезпечує імовірність успіху 0,87 при помірній вартості ($97 000) і найкоротшому часі виконання (2 години), демонструючи баланс між ефективністю й швидкістю. Інтегрована політика у сфері водопостачання поєднує високу ймовірність успіху (0,91) з помірною вартістю ($110 000) і швидким виконанням (2 години), що свідчить про ефективність комплексного міжгалузевого підходу. Загалом таблиця ілюструє доцільність впровадження інтегрованих і адаптивних моделей реагування як оптимальних за співвідношенням ефективності, витрат і оперативності в умовах динамічних загроз.

Обговорення результатів

Проведене дослідження підтвердило переваги використання уніфікованої матричної моделі для побудови гнучких ситуаційно-орієнтованих ССУ в умовах гібридних загроз. Аналіз сучасних підходів [4-6, 8-10] засвідчив, що формалізація взаємозв'язків у вигляді багатовимірних матриць спрощує інтеграцію інформації між різними секторами та підвищує якість прийняття рішень. Порівняння з традиційними ієрархічними моделями виявило вищу адаптивність, скорочення часу реакції та зростання точності ідентифікації загроз.

До основних обмежень належить складність побудови повноцінної моделі для надвеликих систем, необхідність постійного оновлення вагових коефіцієнтів та ризиків, а

також вимоги до кіберстійкості СППР. У подальших дослідженнях доцільно впроваджувати методи автоматизованого аналізу аномалій, використання нейронних мереж для глибокого виявлення загроз, розробку мультиагентних моделей ситуаційного управління.

Висновки

Запропонована уніфікована матрична модель ситуаційно-орієнтованого управління безпекою демонструє низку ключових переваг, які значно підвищують ефективність реагування у складному та динамічному загрозовому середовищі. По-перше, модель забезпечує формалізоване відображення структурно-функціональних зв'язків між суб'єктами управління, об'єктами захисту, типами загроз, формами ризику та політиками реагування, що дозволяє створити єдиний уніфікований інформаційний простір для багатогалузевої взаємодії. Це особливо важливо в умовах гібридних загроз, коли класичні ієрархічні моделі втрачають ефективність через фрагментованість даних і відсутність ситуаційної сумісності між секторами.

По-друге, використання логіко-лінгвістичних конструкцій у моделюванні дозволяє формалізувати не лише кількісні, а й якісні зв'язки між параметрами безпеки, включаючи нечіткі, ймовірнісні та умовні співвідношення, що значно розширює адаптивні можливості системи в умовах неповноти чи невизначеності даних. Такий підхід є особливо ефективним для сценарного аналізу, прогнозування та моделювання поведінки систем у режимі реального часу.

По-третє, запропонована методика дозволяє інтегрувати результати багатовимірної оцінки ризиків у середовище систем підтримки прийняття рішень (СППР), що забезпечує автоматизовану оптимізацію вибору альтернатив реагування з урахуванням обмежень ресурсів, часових вікон і потенційних наслідків. Модель продемонструвала високу ефективність у зниженні часу реагування, підвищенні індексу адаптивності та зменшенні ризику каскадного розповсюдження загроз у міжгалузевих системах.

Крім того, перспективним напрямом подальшого вдосконалення є впровадження нейромережевих емерджентно-адаптивних методів у структуру ситуаційного управління. Такі методи дозволяють здійснювати нелінійне узагальнення даних, динамічну реконфігурацію параметрів моделі в реальному часі та автоматизоване виявлення аномалій без потреби в жорстко заданих правилах. Вони забезпечують самонавчання системи на основі поточних подій, історичних патернів і зворотного зв'язку, що значно підвищує живучість і здатність до еволюційного розвитку управлінської структури.Зокрема, використання глибоких нейронних мереж і баєсівських моделей у гібридній архітектурі дозволяє поєднувати точність розпізнавання загроз з довірою до результатів (через ймовірнісну інтерпретацію). У поєднанні з мультиагентними системами управління це створює підґрунтя для побудови розподілених емерджентно адаптивних систем, які здатні автономно координувати реагування в умовах багатофакторної невизначеності. Таким чином, поєднання уніфікованої матричної моделі з емерджентними та нейромережевими підходами створює основу для наступного покоління ситуаційно-орієнтованих систем управління безпекою, які є не лише високоефективними, а й стійкими до деструктивного впливу, адаптивними до нових типів загроз і здатними до самонавчання та самооптимізації в умовах гібридного інформаційно-цифрового середовища.

Подальші рекомендації. Для вдосконалення розробленої уніфікованої логіко-лінгвістичної матричної моделі доцільно реалізувати компонент адаптивного навчання, який автоматично оновлюватиме вагові коефіцієнти залежностей на основі результатів аналізу інцидентів у реальному часі [7]. Це дозволить моделі зберігати актуальність при зміні сценаріїв атак і підвищить точність прогнозування каскадних ефектів міжгалузевих подій.

Необхідно розробити та провести пілотне впровадження мультимодульного середовища симуляційних випробувань, яке поєднувало б різні типи загроз (кібер, фізико-техногенні) і забезпечувало взаємодію між агентами-підсистемами відповідно до запропонованої матриці

[4]. Такий підхід дозволить протестувати механізми самонавчання та зворотного зв'язку в контрольованому середовищі перед промисловим розгортанням.

Рекомендується інтегрувати розроблену модель із сучасними системами підтримки прийняття рішень (СППР) на базі стандартів ISO/IEC 27001 та NIST CSF для уніфікації процедур оцінки ризиків і звітності [5]. Це сприятиме сумісності з існуючими процесами інформаційної безпеки та полегшить адаптацію моделі у різних галузях критичної інфраструктури.

Крім того, слід розширити функціональність інформаційної бази знань шляхом включення онтологічних описів суб'єктів і об'єктів, що забезпечить гнучкий пошук та кореляцію подій за широким спектром атрибутів [3]. Це сприятиме підвищенню якості логіко-лінгвістичного аналізу ризиків і зменшенню впливу нечітких даних на результат прийняття рішень.

Нарешті, доцільно розробити комплекс методів оцінки ефективності впровадження моделі в реальних умовах, включно з показниками MTTR, MTTD та загальним ROI, і провести багаточисельні польові випробування в різних галузях і організаційних контекстах [2]. Зібрані дані слугуватимуть основою для подальшого масштабування й удосконалення системи.

Перелік посилань

1. Domarev, V. V. (2004). Bezpeka informatsiinykh tekhnolohii: Systemnyi pidkhid [Information-technology security: A systems approach]. TID "Diasoft". https://nvd.luguniv.edu.ua/archiv/NN9/10plvvas.pdf (arxiv.org).

2. Domarev, V. V. (2002). Bezpeka informatsiinykh tekhnolohii: Metodolohiia stvore nnia system zakhystu [Information-technology security: Methodology for building protection systems]. TID "DS". https://www.bsut.by/images/MainMenuFiles/Obrazovanie/Studentam/eumkd/et/euk_56_029/ch1/ch1_1/ch1_1_1.pdf (bsut.by).

3. Domarev, V. V., & Domarev, D. V. (2012). Upravlinnia informatsiinoiu bezpekoiu v bankivskykh ustanovakh: Teoriia i praktyka vprovadzhennia standartiv serii ISO 27k [Information-security management in banking institutions: Theory and practice of ISO 27k implementation]. Velstar. https://www.old.nas.gov.ua/siaz/ Ways_of_development_of_Ukrainian_science/article/12068.001.pdf.

4. National Bank of Ukraine. (2010). DSTU SUIB 1.0/ISO/IEC 27001:2010. Informatsiini tekhnolohii. Metody zakhystu. Systema upravlinnia informatsiinoiu bezpekoiu. Vymohy (ISO/IEC 27001:2005, MOD). https://kyianyn.files.wordpress.com/2010/12/nbu-27001.pdf (scispace.com).

5. National Bank of Ukraine. (2010). DSTU SUIB 2.0/ISO/IEC 27002:2010. Informatsiini tekhnolohii. Metody zakhystu. Zvid pravyl dlia upravlinnia informatsiinoiu bezpekoiu (ISO/IEC 27002:2005, MOD). https://s-byte.com/useful/27002.pdf (scispace.com).

6. National Bank of Ukraine. (2011, March 3). Lyst № 24112/365: Metodychni rekomendatsii shchodo vprovadzhennia systemy upravlinnia informatsiinoiu bezpekoiu ta metodyky otsinky ryzykiv vidpovidno do standartiv NBU [Letter No. 24112/365: Guidelines for ISMS implementation and risk assessment]. https://bank.gov.ua (bank.gov.ua).

7. Domarev, V. V. (2004). Otsinka efektyvnosti system zakhystu informatsii [Evaluation of the effectiveness of information-protection systems]. Problemy zakhystu informatsii. Retrieved from https://pgf.udpu.edu.ua/wp-content/uploads/2019/12/РП-Інформаційна-безпека.pdf (pgf.udpu.edu.ua).

8. Domarev, D. V., & Domarev, V. V. (2011). Information security management system "Matrix" based on system approach. Problemy informatyzatsii ta upravlinnia, 2(34), 36-39. https://doi.org/10.18372/22255036.19.4706.

9. Moroz, O. Ya. (1972). Lohiko-hnoseolohichnyi analiz pryntsypiv kybernetychnoho modeliuvannia [Logical-gnoseological analysis of cybernetic-modeling principles]. Naukova dumka. https://iino.knuba.edu.ua/.../Філософія.pdf (iino.knuba.edu.ua).

10. Shengeriy, L. M. (2007). Ihrova skhema ratsionalnosti: Lohiko-analitychne modeliuvannia vzaiemodii subiektiv [The game scheme of rationality: A logical-analytical modeling of subject interaction]. Filosofski obryi, 18, 129-141. https://harvester.nas.gov.ua/Record/irk-123456789-73475 (harvester.nas.gov.ua).

11. Bezshtanko, V. (2006). Tsykl vprovadzhennia systemy upravlinnia informatsiinoiu bezpekoiu [Cycle of information-security management system implementation]. Pravove, normatyvne ta metrologichne zabezpechennia systemy zakhystu informatsii v Ukraini, 2(13), 123–126. https://ela.kpi.ua/handle/123456789/10974 (ela.kpi.ua).

12. Kharchenko, V., Pechevysty, R., Alexeiev, O., & Karapetyan, S. (2020). Selection of a system of indicators characterizing the effectiveness of the flight safety management system. Proceedings of the National Aviation University, 84(3), 14–18. https://doi.org/10.18372/2306-1472.84.14948 (jrnl.nau.edu.ua).

13. Ostriakova, V. Yu. (2017). Formuvannia systemy upravlinnia informatsiinoiu bezpekoiu pidpryiemstv [Formation of the enterprise information-security management system] (Candidate's thesis). Kyiv National University of Technologies and Design. https://er.knutd.edu.ua/handle/123456789/8187 (er.knutd.edu.ua).

14. Ananchenko, O. Ye. (2016). Pytannia formuvannia orhanizatsiinoi struktury systemy upravlinnia informatsiinoiu bezpekoiu pidpryiemstva [Issues of forming the organizational structure of an enterprise information-security management system]. Suchasnyi zakhyst informatsii, 1, 79-83. https://journals.dut.edu.ua/index.php/ dataprotect/ article/view/536 (journals.dut.edu.ua).

15. Lysenko, S. O. (2023). Rozvytok systemy derzhavnoho upravlinnia informatsiinoiu bezpekoiu na suchasnomu etapi [Development of the state information-security management system at the present stage]. Law and Public Administration, (1), 53-60. https://doi.org/10.32782/pdu.2023.1.53 (researchgate.net).

16. Medvid, V. Yu., Pravdyvets, O. M., & Kryvchun, R. Yu. (2023). Teoretyko-metodychni zasady formuvannia systemy upravlinnia informatsiinoiu bezpekoiu pidpryiemstva [Theoretical and methodological principles for forming an enterprise information-security management system]. Agrosvit, 1, 24–30. https://doi.org/10.32702/2306-6792.2023.1.24 (dspace.krok.edu.ua).

17. Mykolaychuk, M., & Popov, M. (2025). Udoskonalennia systemy instrumentiv upravlinnia bezpekoiu Ukrainy na rehionalnomu rivni [Improvement of the system of management tools for Ukraine's security at the regional level]. Natsionalni Interesy Ukrainy, 3(8), 232–251. https://doi.org/10.52058/3041-1793-2025-3(8)-232-251 (researchgate.net).

18. Koryeeva, N. H. (2020). Formuvannia suchasnoi systemy upravlinnia informatsiinoiu bezpekoiu viiskovoi chasty [Formation of the modern information-security management system of a military unit] (Master's thesis). Chernihiv National Technological University. https://ir.stu.cn.ua/handle/123456789/19964 (ir.stu.cn.ua).

19. Baranova, O. A., Shtefan, D. Yu., & Shvetsov, V. M. (2013). Informatsiina model avtomatyzovanoi systemy upravlinnia informatsiinoiu bezpekoiu sudna [Information model of an automated ship information-security management system]. Proceedings of the III All-Ukrainian Scientific-Practical Conference "Modern Problems of Information Security in Transport" (pp. 1–5). Mykolaiv: National University of Shipbuilding. https://eir.nuos.edu.ua/handle/123456789/1218 (eir.nuos.edu.ua).

20. Tereshchenko, L. O. (2021). Upravlinnia ryzykamy informatsiinykh system: etapy protsesu upravlinnia ryzykamy [Risk management of information systems: Stages of the risk-management process]. Ekonomika ta Suspilstvo, (31), Article 12. https://doi.org/10.32782/2524-0072/2021-31-12 (economyandsociety.in.ua).

21. Beliachenko, V. V., Bobrov, S. V., & Utiushev, M. K. (2021). Upravlinnia ryzykamy stvorennia elementiv avtomatyzovanykh system upravlinnia [Risk management in the development of automated control-system elements]. Zbirnyk naukovykh prats Tsentru voienno-stratehichnykh doslidzhen Natsionalnoho universytetu oborony Ukrainy im. I. Cherniakhovskoho, 3(70), 101–106. https://doi.org/10.33099/2304-2745/2020-3-70/101-106.

22. Dodon, O. D., & Kovalenko, O. O. (2022). Modeli informatsiinykh system upravlinnia personalom [Models of human-resource-management information systems]. Efektyvna ekonomika, (11). https://doi.org/10.32702/2307-2105.2022.11.22.

23. Netreba, I. (2014). Etapy rozvytku informatsiinykh system upravlinnia pidpryiemstvom [Stages of development of enterprise-management information systems]. Formuvannia rynkovoi ekonomiky v Ukraini, 31(2), 82–85. https://irbis-nbuv.gov.ua/.../Nvmgu_eim_2015_10_27.pdf (irbis-nbuv.gov.ua).

24. Semenyuk, A. Ya. (2009). Rozvytok standartiv informatsiinykh system dlia upravlinnia pidpryiemstvom [Development of standards for enterprise-management information systems]. Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia Ekonomika, 28(2), 143–148. https://dspace.uzhnu.edu.ua/jspui/handle/lib/52105 (dspace.uzhnu.edu.ua).

25. Netreba, I. O. (2013). Pidkhody do klasyfikatsii informatsiinykh system upravlinnia pidpryiemstvom [Approaches to the classification of enterprise-management information systems]. Formuvannia rynkovykh vidnosyn v Ukraini, (4), 137–140. https://irbis-nbuv.gov.ua/.../frvu_2013_4_33 (irbis-nbuv.gov.ua).

26. Bezborodova, T. V. (2007). Peredumovy ta etapy formuvannia korporatyvnykh informatsiinykh system upravlinnia [Preconditions and stages of forming corporate-management information systems]. Ekonomika ta derzhava, (10), 41–44. https://www.economy.nayka.com.ua/?op=1&z=674 (economy.nayka.com.ua).

27. Solovyiov, V. M., Serdiuk, O. A., & Danylychuk, G. B. (2016). Modeliuvannia skladnykh system [Modeling of complex systems]. Vydavets O. Yu. Vovchok. https://doi.org/10.31812/0564/1065.

28. Solovyiov, V. M. (2017). Universalnyi instrumentarii modeliuvannia skladnykh system [Universal toolkit for modeling complex systems]. New Computer Technology, 15, 10–14. https://doi.org/10.55056/nocote.v15i0.617.

29. Bratushka, S. M. (2009). Imitatsiine modeliuvannia yak instrument doslidzhennia skladnykh ekonomichnykh system [Simulation modeling as a tool for studying complex economic systems]. Visnyk Ukrainskoi akademii bankivskoi spravy, 2(27), 113–118. http://essuir.sumdu.edu.ua/handle/123456789/55242 (essuir.sumdu.edu.ua).

30. Khimich, O. M. (2018). Superkomp'iuterni tekhnolohii ta matematychne modeliuvannia skladnykh system [Supercomputer technologies and mathematical modeling of complex systems]. Visnyk Natsionalnoi akademii nauk Ukrainy, (5), 69–72. https://irbis-nbuv.gov.ua/.../vnanu_2018_5_21 (irbis-nbuv.gov.ua).

Надійшла 24.06.2025