КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.34.1272
УДК 004.89:004.056:005.53

Гречанінов Віктор Федорович
аспірант
Інститут проблем математичних машин і систем НАН України, м. Київ, Україна
ORCID:0009-0002-8400-6401
vgrechaninov@gmail.com

МЕТОД ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ТА ЗАБЕЗПЕЧЕННЯ ГАРАНТОЗДАТНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ СИТУАЦІЙНИХ ЦЕНТРІВ

Анотація. У статті розглянуто проблему підтримки прийняття рішень щодо забезпечення гарантоздатності інформаційних систем ситуаційних центрів в умовах зростання складності інформаційно-комунікаційної інфраструктури, збільшення кількості дестабілізуючих впливів та підвищення вимог до безперервності функціонування критично важливих сервісів. Актуальність дослідження обумовлена необхідністю підвищення обґрунтованості рішень, які приймаються під час управління станом інформаційних систем ситуаційних центрів, а також потребою врахування великої кількості взаємопов'язаних параметрів функціонування, ризиків і можливих наслідків реалізації загроз. Метою роботи є розроблення методу підтримки прийняття рішень та забезпечення гарантоздатності інформаційних систем ситуаційних центрів на основі комплексного аналізу стану системи, оцінювання ризиків і багатокритеріального вибору альтернатив. Формалізовано процес підтримки прийняття рішень щодо забезпечення гарантоздатності інформаційних систем ситуаційних центрів та розроблено математичну модель, яка враховує поточний стан системи, рівень ризику, доступні ресурси та можливі наслідки реалізації дестабілізуючих впливів. Запропоновано метод, що забезпечує формування множини допустимих альтернатив, їх багатокритеріальне оцінювання та вибір найбільш доцільного рішення з урахуванням впливу на показники гарантоздатності. Розроблено архітектуру інтелектуальної системи підтримки прийняття рішень, яка забезпечує накопичення знань, адаптацію до зміни умов функціонування та підвищення якості прийнятих рішень. На відміну від існуючих підходів, запропонований метод поєднує оцінювання стану інформаційної системи, аналіз ризиків, формування альтернатив та підтримку прийняття рішень у межах єдиного процесу забезпечення гарантоздатності. Результати моделювання підтвердили підвищення обґрунтованості прийнятих рішень, скорочення часу вибору альтернатив та покращення показників гарантоздатності інформаційної системи. Практична цінність роботи полягає у можливості використання запропонованого методу в інформаційних системах ситуаційних центрів для підвищення ефективності управління, стійкості функціонування та забезпечення безперервності надання інформаційних сервісів.

Ключові слова: гарантоздатність; інформаційні системи; ситуаційні центри; підтримка прийняття рішень; інтелектуальні технології; багатокритеріальне оцінювання; управління ризиками; база знань; адаптивне прийняття рішень; кібербезпека.

ВСТУП

Стрімкий розвиток інформаційно-комунікаційних технологій, цифровізація управління та зростання кількості кіберзагроз зумовлюють необхідність підвищення ефективності функціонування інформаційних систем ситуаційних центрів [1, 3]. Такі системи забезпечують моніторинг обстановки, координацію дій та підтримку прийняття рішень у складних і динамічних умовах [2-6, 13]. Особливого значення набуває забезпечення їх гарантоздатності, оскільки порушення функціонування може призвести до втрати актуальності інформації, затримки прийняття рішень та зниження ефективності реагування на кризові ситуації.

Сучасні інформаційні системи ситуаційних центрів функціонують під впливом кібератак, технічних відмов, програмних помилок, перевантаження ресурсів і людського фактора [21, 23]. Водночас ускладнення архітектури систем та необхідність оброблення значних обсягів різнорідних даних суттєво ускладнюють процес прийняття рішень щодо забезпечення необхідного рівня гарантоздатності [15, 26-27]. За таких умов актуальним є застосування інтелектуальних технологій, здатних підтримувати

прийняття рішень на основі аналізу стану системи, оцінювання ризиків і вибору найбільш доцільних альтернатив.

Існуючі підходи переважно орієнтовані на оцінювання окремих показників, прогнозування їх зміни або реагування на інциденти [7-9, 17]. Проте вони недостатньо враховують необхідність комплексного обґрунтування рішень з урахуванням поточного стану системи, рівня ризику, ресурсних обмежень та можливих наслідків управлінських впливів [25, 27]. Це обумовлює необхідність розроблення нових методів підтримки прийняття рішень щодо забезпечення гарантоздатності інформаційних систем ситуаційних центрів.

Наукова новизна роботи полягає у розробленні методу підтримки прийняття рішень щодо забезпечення гарантоздатності інформаційних систем ситуаційних центрів, який, на відміну від існуючих підходів, забезпечує інтеграцію процедур формування множини допустимих альтернатив, їх багатокритеріального оцінювання та адаптивного вибору рішень на основі коригування ваг критеріїв з урахуванням поточного стану системи, рівня ризику та ресурсних обмежень.

Теоретичне значення дослідження полягає у розвитку науково-методичних засад підтримки прийняття рішень щодо забезпечення гарантоздатності інформаційних систем ситуаційних центрів шляхом формалізації процесу вибору альтернатив та розроблення математичних моделей їх оцінювання.

Практичне значення отриманих результатів полягає у можливості використання запропонованого методу під час проєктування, модернізації та експлуатації інформаційних систем ситуаційних центрів для підвищення обґрунтованості рішень, забезпечення необхідного рівня гарантоздатності та підтримання безперервності функціонування інформаційних сервісів.

Постановка проблеми. Інформаційні системи ситуаційних центрів є складними системами, призначеними для збору, оброблення, аналізу та візуалізації інформації з метою підтримки управлінської діяльності в умовах невизначеності та динамічної зміни обстановки [6, 21, 23]. Ефективність їх функціонування залежить від здатності підтримувати необхідний рівень гарантоздатності, що визначається показниками доступності, надійності, безпеки, цілісності та безперервності надання інформаційних сервісів.

Сучасні інформаційні системи ситуаційних центрів функціонують під впливом різноманітних дестабілізуючих факторів, зокрема кібератак, технічних відмов, програмних помилок, перевантаження ресурсів, порушення мережевої взаємодії та людського фактора [13, 27]. Їх реалізація може призводити до зниження рівня гарантоздатності та ефективності функціонування системи, що обумовлює необхідність своєчасного прийняття рішень щодо підтримання або відновлення її працездатності [23].

Існуючі підходи до забезпечення гарантоздатності переважно орієнтовані на моніторинг стану системи, оцінювання ризиків або реагування на окремі інциденти [17, 19]. Водночас прийняття рішень щодо забезпечення гарантоздатності потребує врахування поточного стану системи, рівня ризику, ресурсних обмежень, можливих альтернатив та очікуваного результату їх реалізації [15, 25]. За таких умов значна залежність від експертних оцінок може призводити до суб’єктивності рішень і зниження ефективності управління.

Таким чином, актуальним науково-практичним завданням є розроблення методу підтримки прийняття рішень щодо забезпечення гарантоздатності інформаційних систем ситуаційних центрів, який забезпечуватиме формування множини допустимих альтернатив, їх багатокритеріальне оцінювання та вибір найбільш доцільного рішення з урахуванням поточного стану системи, рівня ризику, ресурсних обмежень і очікуваного впливу на показники гарантоздатності.

Аналіз останніх досліджень і публікацій. Забезпечення гарантоздатності інформаційних систем ситуаційних центрів та підтримка прийняття рішень в умовах динамічних загроз є одним із пріоритетних напрямів сучасних досліджень у галузі комп’ютерних наук, кібербезпеки та критичної інфраструктури.

У роботі Ajayi, Kurien, Djouani та Dieng [1] досліджено можливості використання штучного інтелекту для підвищення стійкості інфраструктурних систем. Авторами обґрунтовано доцільність застосування інтелектуальних технологій для аналізу ризиків, прогнозування загроз і підтримки управлінських процесів. Водночас питання забезпечення гарантоздатності інформаційних систем та вибору рішень щодо її підтримання залишаються поза межами дослідження.

Leyli-Abadi та співавтори [2] запропонували концептуальну модель систем підтримки прийняття рішень на основі штучного інтелекту для критичної інфраструктури. Автори визначили основні компоненти таких систем та принципи їх функціонування, проте не розглянули механізми оцінювання альтернатив і вибору рішень щодо забезпечення гарантоздатності інформаційних систем.

У роботі Järveläinen, Dang, Mekkanen та Vartiainen [3] розроблено підхід до підвищення кіберстійкості критичної інфраструктури на основі концепції динамічних можливостей. Отримані результати демонструють важливість адаптивного управління та своєчасного прийняття рішень, однак не

містять формалізованих методів багатокритеріального вибору альтернатив для забезпечення гарантоздатності інформаційних систем.

Jovanović [4] досліджує підходи до оцінювання стійкості критичної інфраструктури в умовах комплексних ризиків та кризових ситуацій. Запропоновані моделі дозволяють аналізувати вплив зовнішніх факторів на функціонування інфраструктурних об'єктів, проте питання підтримки прийняття рішень щодо забезпечення гарантоздатності інформаційних систем залишаються недостатньо розкритими.

У роботі Pasić [5] розглянуто проблеми кризового управління та забезпечення стійкості критичної інфраструктури. Автор акцентує увагу на необхідності використання сучасних підходів до управління ризиками та прийняття рішень, однак не пропонує математичного апарату для оцінювання альтернатив та вибору найбільш доцільних рішень.

Bîlbîie та Ciolponea [6] дослідили теоретичні засади ситуаційної обізнаності та моделі її реалізації у кіберпросторі. Отримані результати підтверджують важливість своєчасного отримання та аналізу інформації для підтримки прийняття рішень, проте не враховують вплив управлінських рішень на показники гарантоздатності інформаційних систем.

У роботі Kramer та співавторів [7] проаналізовано можливості інтеграції великих мовних моделей у процеси реагування на інциденти інформаційної безпеки. Автори продемонстрували потенціал використання сучасних інтелектуальних технологій для підтримки фахівців під час прийняття рішень, однак питання формування множини альтернатив та оцінювання їх ефективності не розглядаються.

Hammar, Alpcan та Lupu [8] запропонували підхід до планування реагування на інциденти із застосуванням великої мовної моделі зі зменшеним рівнем галюцинацій. Запропоноване рішення підвищує якість рекомендацій для операторів, проте не враховує комплексне оцінювання стану системи, ресурсних обмежень та впливу прийнятих рішень на гарантоздатність.

Отже, проведений аналіз показав, що сучасні дослідження зосереджені переважно на забезпеченні стійкості критичної інфраструктури, підвищенні ситуаційної обізнаності, використанні штучного інтелекту та інтелектуальній підтримці прийняття рішень [1-8]. Водночас недостатньо дослідженими залишаються питання розроблення методів підтримки прийняття рішень щодо забезпечення гарантоздатності інформаційних систем ситуаційних центрів, які б поєднували формування множини альтернатив, їх багатокритеріальне оцінювання та адаптивний вибір найбільш доцільного рішення з урахуванням поточного стану системи, рівня ризику, ресурсних обмежень і очікуваного впливу на показники гарантоздатності. Саме усунення зазначених недоліків становить наукову задачу даного дослідження.

Мета статті. Метою статті є розробка методу підтримки прийняття рішень щодо забезпечення гарантоздатності інформаційних систем ситуаційних центрів, який забезпечує формування множини допустимих альтернатив, їх багатокритеріальне оцінювання та вибір найбільш доцільного рішення з урахуванням поточного стану системи, рівня ризику, ресурсних обмежень і очікуваного впливу на показники гарантоздатності.

Для досягнення поставленої мети у роботі необхідно вирішити такі завдання:

- провести аналіз сучасних підходів до забезпечення гарантоздатності інформаційних систем ситуаційних центрів та підтримки прийняття рішень в умовах дестабілізуючих впливів;
- визначити фактори та критерії, що впливають на прийняття рішень щодо забезпечення гарантоздатності інформаційних систем ситуаційних центрів;
- формалізувати процес підтримки прийняття рішень щодо забезпечення гарантоздатності інформаційних систем ситуаційних центрів;
- розробити математичну модель подання стану інформаційної системи, ризиків, ресурсних обмежень та можливих альтернатив рішень;
- розробити метод багатокритеріального оцінювання альтернатив щодо забезпечення гарантоздатності інформаційної системи;
- розробити метод підтримки прийняття рішень, який забезпечує адаптивний вибір найбільш доцільної альтернативи з урахуванням поточного стану системи та рівня ризику;
- розробити архітектуру інтелектуальної системи підтримки прийняття рішень щодо забезпечення гарантоздатності інформаційних систем ситуаційних центрів;
- провести моделювання та оцінити ефективність запропонованого методу за показниками якості прийнятих рішень, часу вибору альтернатив та рівня гарантоздатності інформаційної системи.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Для розроблення методу підтримки прийняття рішень щодо забезпечення гарантоздатності інформаційних систем ситуаційних центрів необхідно формалізувати процес вибору альтернатив, визначити критерії їх оцінювання, ресурсні обмеження та механізм адаптивного прийняття найбільш доцільного рішення [15, 25]. У межах дослідження інформаційна система ситуаційного центру розглядається як об'єкт управління, стан якого змінюється під впливом дестабілізуючих факторів, а підтримка прийняття рішень спрямована на забезпечення необхідного рівня гарантоздатності [21].

Формалізація процесу підтримки прийняття рішень щодо забезпечення гарантоздатності інформаційних систем ситуаційних центрів. Підтримка прийняття рішень щодо забезпечення гарантоздатності інформаційних систем ситуаційних центрів є складним процесом, який передбачає аналіз поточного стану системи, оцінювання можливих варіантів дій та вибір найбільш доцільного рішення з урахуванням визначених критеріїв і наявних ресурсних обмежень [2, 13]. Особливістю таких систем є необхідність функціонування в умовах динамічної зміни середовища, наявності значної кількості взаємопов'язаних компонентів та постійного впливу дестабілізуючих факторів, що ускладнює процес прийняття рішень.

Для формалізації процесу підтримки прийняття рішень введемо модель задачі у вигляді:

$$D = \langle S, K, A, R \rangle, \tag{1}$$

де S − множина можливих станів інформаційної системи ситуаційного центру, K − множина критеріїв оцінювання альтернатив, A − множина допустимих альтернативних рішень, R − множина ресурсних обмежень. Модель описує процес підтримки прийняття рішень як задачу вибору найбільш доцільної альтернативи із множини допустимих рішень з урахуванням поточного стану системи, критеріїв оцінювання та ресурсних обмежень.

Множина станів інформаційної системи визначається як:

$$S = \{s_1, s_2, \dots, s_m\}, \tag{2}$$

де s_i − окремий стан інформаційної системи, m − кількість можливих станів. Залежно від значень параметрів функціонування інформаційної системи стани можуть відповідати нормальному, деградованому, критичному або аварійному режиму функціонування.

Кожний стан характеризує рівень функціонування інформаційної системи в певний момент часу та відображає сукупність параметрів, що визначають її працездатність, захищеність і здатність забезпечувати необхідний рівень гарантоздатності.

Для опису поточного стану системи використаємо вектор параметрів:

$$s(t) = \{x_1(t), x_2(t), \dots, x_n(t)\}, \tag{3}$$

де $s(t)$ − вектор поточного стану інформаційної системи у момент часу t, $x_i(t)$ − значення і-го параметра функціонування системи, n − кількість параметрів, що контролюються. До складу вектора стану можуть входити показники завантаження процесорних ресурсів, використання оперативної пам'яті, доступності сервісів, інтенсивності мережевого трафіку, кількості зареєстрованих подій безпеки, часу відгуку інформаційних сервісів та інші параметри, що характеризують поточний стан інформаційної системи.

Таким чином, формули (1)-(3) дозволяють формалізувати задачу підтримки прийняття рішень щодо забезпечення гарантоздатності інформаційних систем ситуаційних центрів та визначають основу для подальшого опису критеріїв оцінювання, формування множини альтернатив і розроблення методу вибору найбільш доцільного рішення. Отримане формальне представлення процесу підтримки прийняття рішень дозволяє перейти до побудови математичної моделі подання стану інформаційної системи та факторів впливу, які використовуються під час оцінювання альтернатив і вибору найбільш доцільного рішення.

Математична модель подання стану інформаційної системи та факторів впливу. Для забезпечення обґрунтованого прийняття рішень щодо підтримання гарантоздатності інформаційної системи ситуаційного центру необхідно забезпечити єдине подання різнорідних параметрів її функціонування [13, 15, 21]. Оскільки значення показників можуть вимірюватися в різних одиницях та мати різні діапазони зміни, перед проведенням їх аналізу виконується процедура нормалізації.

Нормалізоване значення (і)-го показника визначається за формулою:

$$x_i^* = \frac{x_i - x_i^{min}}{x_i^{max} - x_i^{min}}, \quad (4)$$

де x_i^* − нормалізоване значення показника, x_i − поточне значення показника, x_i^{min} та x_i^{max} – відповідно мінімальне та максимальне допустимі значення показника. Застосування процедури нормалізації дозволяє привести всі параметри до єдиної шкали оцінювання в діапазоні від 0 до 1 та забезпечити їх подальше порівняння під час вибору управлінських рішень. Це забезпечує коректне порівняння показників різної природи та виключає домінування критеріїв, значення яких мають більший числовий діапазон.

Для оцінювання альтернатив щодо забезпечення гарантоздатності інформаційної системи введемо множину критеріїв:

$$K = \{k_1, k_2, k_3, k_4, k_5\}, \quad (5)$$

де k_1 − рівень гарантоздатності інформаційної системи після реалізації альтернативи, k_2 − рівень ризику функціонування системи, k_3 − ресурсомісткість реалізації альтернативи, k_4 − час реалізації рішення, k_5 − очікувана ефективність запропонованих заходів. Зазначені критерії охоплюють основні аспекти прийняття рішень щодо забезпечення гарантоздатності інформаційної системи та дозволяють оцінювати альтернативи як з технічної, так і з організаційно-економічної точки зору. Обрана множина критеріїв забезпечує комплексне врахування як технічних, так і організаційних аспектів функціонування інформаційної системи ситуаційного центру. На відміну від підходів, орієнтованих виключно на мінімізацію ризику або максимізацію окремих показників ефективності, запропонована модель дозволяє одночасно враховувати декілька взаємопов'язаних факторів під час прийняття рішень.

Рівень гарантоздатності інформаційної системи визначається як інтегральний показник:

$$G = \sum_{=1}^{l} \beta_i \, g_i, \ \sum_{=1}^{l} \beta_i = 1 \quad (6)$$

де G − інтегральний рівень гарантоздатності, g_i − нормалізоване значення і-го показника гарантоздатності, β_i − ваговий коефіцієнт показника, l − кількість показників гарантоздатності. Інтегральний показник гарантоздатності враховує сукупний вплив основних характеристик функціонування інформаційної системи, зокрема доступності, надійності, безпеки, цілісності та безперервності надання сервісів. Чим більше значення показника GGG, тим вищим є рівень гарантоздатності інформаційної системи та її здатність забезпечувати стабільне функціонування в умовах дестабілізуючих впливів.

Для подальшого аналізу сформуємо матрицю оцінювання альтернатив:

$$M = \begin{pmatrix} m_{11} & m_{12} & \cdots & m_{1m} \\ m_{21} & m_{22} & \cdots & m_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n1} & m_{n2} & \cdots & m_{nm} \end{pmatrix} \quad (7)$$

де m_{ij} − оцінка альтернативи a_i за критерієм k_j, n − кількість альтернативних рішень, m − кількість критеріїв оцінювання. Кожний рядок матриці відповідає окремій альтернативі забезпечення гарантоздатності, а кожний стовпець характеризує значення відповідного критерію оцінювання. Таким чином, матриця M є основою для подальшого багатокритеріального оцінювання альтернатив та визначення найбільш доцільного рішення.

Рядки матриці відповідають альтернативним рішенням щодо забезпечення гарантоздатності інформаційної системи, а стовпці − критеріям їх оцінювання. Елементи матриці можуть визначатися на основі результатів моніторингу, аналітичних розрахунків, статистичних даних або експертних оцінок [21-22, 26]. Таким чином, математична модель подання стану інформаційної системи та факторів впливу забезпечує формування єдиного інформаційного простору для подальшого оцінювання альтернатив, визначення їх переваг і недоліків та вибору найбільш доцільного рішення щодо забезпечення гарантоздатності інформаційної системи ситуаційного центру.

Формування множини допустимих альтернатив забезпечення гарантоздатності. Одним із ключових етапів підтримки прийняття рішень є формування множини допустимих альтернатив, реалізація яких дозволяє підтримувати або підвищувати рівень гарантоздатності інформаційної системи ситуаційного центру [23-25]. До таких альтернатив можуть належати переналаштування ресурсів, резервування сервісів, ізоляція окремих компонентів, зміна політик безпеки, запуск процедур відновлення або комбіновані заходи забезпечення функціонування системи.

Множина допустимих альтернатив визначається як:

$$A = \{a_1, a_2, \dots, a_p\}, \tag{8}$$

де a_i – окрема альтернатива забезпечення гарантоздатності, p – загальна кількість допустимих альтернатив. Залежно від поточного стану системи до множини A можуть включатися альтернативи резервування сервісів, перерозподілу ресурсів, зміни конфігурації засобів захисту, ізоляції окремих компонентів або запуску процедур відновлення.

Кожна альтернатива повинна відповідати встановленим ресурсним обмеженням. Умова допустимості альтернативи визначається співвідношенням:

$$C(a_i) \le C_{max}, \tag{9}$$

де $C(a_i)$ – витрати ресурсів на реалізацію альтернативи a_i, C_{max} – максимально допустимий обсяг ресурсів.

Крім ресурсних обмежень, кожна альтернатива повинна забезпечувати мінімально допустимий рівень гарантоздатності інформаційної системи:

$$G(a_i) \ge G_{min}, \tag{10}$$

де $G(a_i)$ – очікуваний рівень гарантоздатності після реалізації альтернативи a_i, G_{min} – мінімально допустиме значення гарантоздатності.

Таким чином, до подальшого аналізу допускаються лише ті альтернативи, які одночасно задовольняють умови (9) та (10), що дозволяє виключити неефективні або недопустимі варіанти ще на етапі формування множини рішень [15, 22, 24]. Сформована множина допустимих альтернатив є основою для їх подальшого багатокритеріального оцінювання та вибору найбільш доцільного рішення щодо забезпечення гарантоздатності інформаційної системи ситуаційного центру.

Метод багатокритеріального оцінювання альтернатив. Після формування множини допустимих альтернатив необхідно виконати їх порівняльне оцінювання за сукупністю критеріїв. Для цього вводиться вектор вагових коефіцієнтів критеріїв:

$$W = \{w_1, w_2, \dots, w_m\}, \tag{11}$$

де w_i – ваговий коефіцієнт j-го критерію, m – кількість критеріїв оцінювання. Для ваг повинна виконуватися умова:

$$\sum_{j=1}^{m} w_j = 1, \tag{12}$$

тобто сума всіх ваг дорівнює одиниці.

Нормована оцінка альтернативи:

$$q_{ij} = \frac{m_{ij}}{\max(m_j)}, \tag{13}$$

де q_{ij} – нормована оцінка, m_{ij} – значення оцінки альтернативи, $\max(m_j)$ – максимальне значення за критерієм j. Нормалізація дозволяє привести значення різних критеріїв до єдиної шкали оцінювання та забезпечити можливість їх подальшого агрегування. Для критеріїв, що підлягають мінімізації (ризик, ресурсомісткість та час реалізації), нормалізація виконується оберненим способом.

Інтегральна корисність альтернативи:

$$U(a_i) = \sum_{j=1}^{m} w_j \, q_{ij}, \tag{14}$$

де $U(a_i)$ – інтегральна корисність альтернативи a_i. Отримане значення функції корисності характеризує ступінь доцільності реалізації відповідної альтернативи. Чим більше значення $U(a_i)$, тим вищою є пріоритетність альтернативи з точки зору забезпечення гарантоздатності інформаційної системи ситуаційного центру.

Отримані значення функції корисності використовуються під час вибору найбільш доцільної альтернативи, що розглядається у наступному підрозділі.

Метод підтримки прийняття рішень. Вибір рішення здійснюється на основі максимізації функції корисності серед усіх допустимих альтернатив. Оптимальна альтернатива визначається за формулою

$$a^* = arg \max_{a_i \in A} U(a_i), \quad (15)$$

де a^* − оптимальна альтернатива забезпечення гарантоздатності інформаційної системи. Тобто обирається альтернатива, для якої функція корисності має найбільше значення.

Для врахування результатів попередніх рішень та адаптації системи до змін умов функціонування використовується механізм коригування ваг критеріїв:

$$w_j(t+1) = w_j(t) + \alpha(E_f - E_p), \quad (16)$$

де $w_j(t)$ − поточне значення вагового коефіцієнта, $w_j(t+1)$ − оновлене значення ваги, E_f − фактичний результат реалізації рішення, E_p − прогнозований результат, α − коефіцієнт адаптації. Якщо фактичний результат перевищує прогнозований, ваговий коефіцієнт відповідного критерію збільшується. У протилежному випадку його значення зменшується, що забезпечує адаптацію системи до зміни умов функціонування. Процес адаптації дозволяє враховувати результати попередніх управлінських впливів та забезпечує самоудосконалення системи підтримки прийняття рішень у процесі її експлуатації.

Запропонований механізм дозволяє накопичувати досвід функціонування системи та підвищувати якість прийняття рішень у процесі експлуатації інформаційної системи ситуаційного центру [20, 22-23]. У результаті формується адаптивний метод підтримки прийняття рішень, який враховує поточний стан системи, ресурсні обмеження, рівень ризику та очікуваний вплив альтернатив на показники гарантоздатності.

Реалізація запропонованого методу підтримки прийняття рішень потребує створення відповідної інтелектуальної системи, архітектура якої наведена у наступному підрозділі.

Архітектура інтелектуальної системи підтримки прийняття рішень. Для реалізації запропонованого методу розроблено архітектуру інтелектуальної системи підтримки прийняття рішень, яка забезпечує збір та оброблення інформації про стан інформаційної системи, аналіз факторів впливу, формування та оцінювання альтернатив і вибір найбільш доцільного рішення щодо забезпечення гарантоздатності.

Рис. 1 ілюструє архітектуру інтелектуальної системи підтримки прийняття рішень щодо забезпечення гарантоздатності інформаційних систем ситуаційних центрів. Архітектура об'єднує модулі моніторингу стану системи, оцінювання параметрів функціонування, аналізу ризиків, формування альтернатив, багатокритеріального оцінювання та вибору рішень [21-22]. Важливими складовими є база знань і механізм адаптації, які забезпечують накопичення досвіду функціонування системи та коригування параметрів процесу прийняття рішень на основі результатів попередніх управлінських впливів [2, 9, 17]. Це дозволяє підвищити обґрунтованість рішень і забезпечити необхідний рівень гарантоздатності в умовах дії дестабілізуючих факторів.

Рис. 1. Архітектура інтелектуальної системи підтримки прийняття рішень щодо забезпечення гарантоздатності інформаційних систем ситуаційних центрів

Архітектура побудована за модульним принципом та включає модуль моніторингу стану системи, модуль оцінювання параметрів функціонування, модуль аналізу ризиків і дестабілізуючих факторів, модуль формування альтернатив, модуль багатокритеріального оцінювання, модуль вибору рішення, базу знань та модуль зворотного зв'язку й адаптації.

Модуль моніторингу забезпечує збір інформації про використання ресурсів, доступність сервісів, мережеву активність і події безпеки [6, 10]. Отримані дані передаються до модуля оцінювання, де виконуються їх нормалізація та підготовка до аналізу.

Модуль аналізу ризиків здійснює виявлення дестабілізуючих факторів та оцінювання їх впливу на гарантоздатність системи [13, 20]. На основі результатів аналізу формуються обмеження, які враховуються під час прийняття рішень.

Модуль формування альтернатив генерує допустимі варіанти підтримання або підвищення гарантоздатності, зокрема перерозподіл ресурсів, резервування сервісів, зміну конфігурації засобів захисту, ізоляцію компонентів та запуск процедур відновлення [9].

Модуль багатокритеріального оцінювання визначає корисність кожної альтернативи за встановленими критеріями, а модуль вибору рішення визначає найбільш доцільний варіант [25-26]. База знань накопичує інформацію про попередні стани системи, прийняті рішення та результати їх реалізації, що дозволяє використовувати попередній досвід під час подальшого функціонування.

Модуль зворотного зв'язку та адаптації аналізує результати реалізації обраного рішення та коригує параметри системи підтримки прийняття рішень. Подібні механізми адаптивного управління та навчання на основі накопиченого досвіду розглядаються у роботах [12, 14, 18].

Таким чином, запропонована архітектура інтегрує процеси моніторингу, аналізу, оцінювання та вибору рішень у межах єдиного інформаційного середовища, що сприяє підвищенню обґрунтованості управлінських рішень та забезпеченню гарантоздатності інформаційних систем ситуаційних центрів.

Алгоритм функціонування методу. Алгоритм функціонування запропонованого методу підтримки прийняття рішень щодо забезпечення гарантоздатності інформаційних систем ситуаційних центрів реалізує послідовність етапів, спрямованих на аналіз стану системи, оцінювання альтернатив та вибір найбільш доцільного рішення [21, 26]. Робота методу розпочинається зі збору та нормалізації даних моніторингу, на основі яких формується вектор поточного стану інформаційної системи.

Далі виконується аналіз ризиків і дестабілізуючих факторів, результати якого використовуються для визначення обмежень та формування множини можливих альтернатив забезпечення гарантоздатності [13, 23]. До таких альтернатив можуть належати резервування сервісів, перерозподіл ресурсів, зміна конфігурації засобів захисту, ізоляція окремих компонентів або запуск процедур відновлення [9].

Сформовані альтернативи перевіряються на відповідність ресурсним обмеженням і вимогам щодо мінімально допустимого рівня гарантоздатності. Для допустимих варіантів виконується багатокритеріальне оцінювання за показниками гарантоздатності, рівня ризику, ресурсомісткості, часу реалізації та очікуваної ефективності [15, 25]. На основі отриманих оцінок розраховується інтегральна функція корисності кожної альтернативи.

Після оцінювання здійснюється вибір рішення з максимальним значенням функції корисності та його реалізація в інформаційній системі ситуаційного центру. Отримані результати порівнюються з прогнозованими значеннями, що дозволяє оцінити ефективність прийнятого рішення та виявити можливі відхилення.

На завершальному етапі виконується коригування вагових коефіцієнтів критеріїв та оновлення бази знань, що забезпечує накопичення досвіду й адаптацію системи до зміни умов функціонування [17, 20]. Таким чином, запропонований алгоритм реалізує безперервний цикл моніторингу, аналізу, оцінювання та адаптивного прийняття рішень, спрямованих на підтримання необхідного рівня гарантоздатності інформаційних систем ситуаційних центрів.

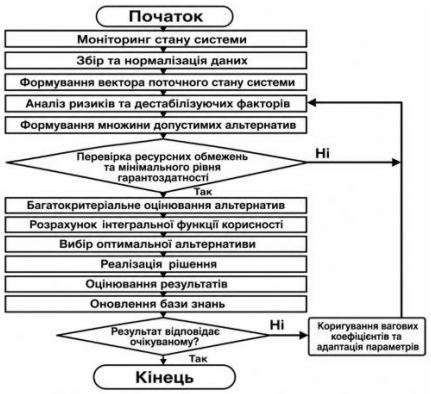

Рис. 2. Алгоритм функціонування методу підтримки прийняття рішень щодо забезпечення гарантоздатності інформаційних систем ситуаційних центрів

На рис. 2 представлено послідовність етапів запропонованого методу, що включає моніторинг стану системи, аналіз ризиків, формування та оцінювання альтернатив, вибір оптимального рішення, його реалізацію та оцінювання результатів. У разі невідповідності отриманих результатів очікуваним значенням здійснюється коригування параметрів методу та повторний аналіз стану системи, що забезпечує адаптивне управління рівнем гарантоздатності інформаційної системи.

Результати моделювання та оцінювання ефективності. Для оцінювання ефективності запропонованого методу підтримки прийняття рішень щодо забезпечення гарантоздатності інформаційних систем ситуаційних центрів проведено моделювання процесу вибору альтернатив в умовах різного рівня дестабілізуючих впливів. Під час дослідження розглядалися чотири сценарії функціонування системи: S1 – штатний режим функціонування, S2 – підвищений рівень ризику, S3 – відмова критичного сервісу, S4 – комплексний дестабілізуючий вплив.

Ефективність запропонованого методу оцінювалася за показниками рівня гарантоздатності, часу прийняття рішень, точності вибору альтернатив та частки успішних рішень.

Таблиця 1

Результати функціонування системи в різних сценаріях

Сценарій	Рівень ризику	Гарантоздатність до прийняття рішення	Гарантоздатність після прийняття рішення	Час прийняття рішення, с
S1	0,12	0,91	0,95	4,1
S2	0,34	0,78	0,89	4,8
S3	0,57	0,65	0,84	5,3
S4	0,76	0,51	0,79	6,1

Як видно з табл. 1, зі зростанням рівня ризику відбувається зниження початкового рівня гарантоздатності інформаційної системи. Водночас застосування запропонованого методу дозволяє підвищити показники гарантоздатності в усіх розглянутих сценаріях, включаючи сценарій комплексного дестабілізуючого впливу S4, де рівень гарантоздатності збільшився з 0,51 до 0,79, що свідчить про ефективність запропонованого методу навіть у найбільш складних умовах функціонування системи.

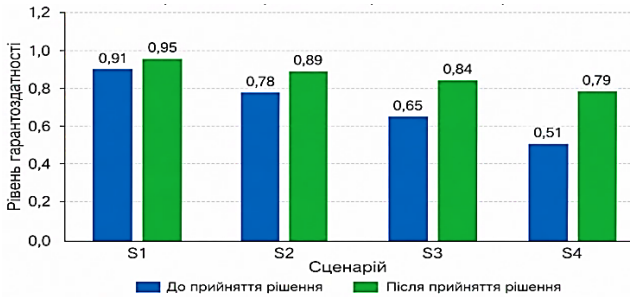

Рис. 3. Зміна рівня гарантоздатності до та після прийняття рішення в різних сценаріях

На рис. 3 наведено порівняння рівня гарантоздатності інформаційної системи до та після застосування запропонованого методу підтримки прийняття рішень для різних сценаріїв функціонування. Отримані результати свідчать про підвищення рівня гарантоздатності в усіх розглянутих сценаріях. Найбільший приріст спостерігається у сценарії S4, де показник гарантоздатності зріс з 0,51 до 0,79. Це підтверджує ефективність запропонованого методу в умовах високого рівня ризику та комплексних дестабілізуючих впливів.

Для сценарію S4 подальший аналіз альтернатив наведено в табл. 2.

Таблиця 2

Результати багатокритеріального оцінювання альтернатив для сценарію S4

Альтернатива	Рівень гарантоздатності	Рівень ризику	Ресурсомісткість	Час реалізації, хв	Функція корисності
a_1	0,71	0,52	0,43	18	0,72
a_2	0,75	0,47	0,51	15	0,76
a_3	0,82	0,38	0,48	14	0,84
a_4	0,79	0,41	0,56	17	0,80

Як видно з табл. 2, найбільше значення функції корисності отримала альтернатива a_3, яка забезпечує найкраще співвідношення між рівнем гарантоздатності, ризиком, ресурсомісткістю, функція корисності та часом реалізації. Саме ця альтернатива була обрана системою як оптимальне рішення для сценарію комплексного дестабілізуючого впливу.

На рис. 4 наведено результати порівняння значень функції корисності для альтернатив сценарію S4. Аналіз показує, що найбільше значення функції корисності має альтернатива a_3 (0,84), яка забезпечує найкраще співвідношення між рівнем гарантоздатності, ризиком, ресурсомісткістю та часом реалізації. Отримані результати підтверджують доцільність вибору альтернативи a_3 як оптимального рішення в умовах комплексного дестабілізуючого впливу.

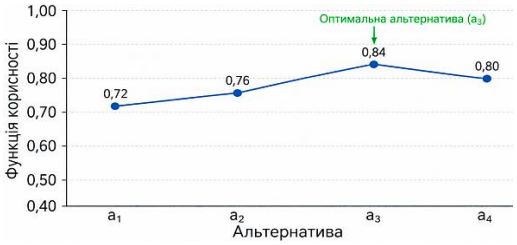

Рис. 4. Порівняння значень функції корисності для альтернатив сценарію S4

Результати табл. 3 свідчать, що запропонований метод забезпечує найкращі показники серед розглянутих підходів за рівнем гарантоздатності, точністю вибору альтернатив, часткою успішних рішень та середнім значенням функції корисності, одночасно скорочуючи час прийняття рішень.

Таблиця 3

Порівняння методів підтримки прийняття рішень

Метод	Рівень гарантоздатності	Час, с	Точність	Частка успішних рішень	Середня функція корисності
Експертний	0,81	15,2	0,79	0,82	0,74
Правило-орієнтований	0,86	9,8	0,85	0,88	0,81
Запропонований	0,93	5,4	0,94	0,96	0,89

Порівняно з правило-орієнтованим підходом запропонований метод забезпечив підвищення рівня гарантоздатності на 8,1 %, скорочення часу прийняття рішення на 44,9 %, збільшення точності вибору альтернатив на 10,6 % та підвищення частки успішних рішень на 9,1 %. Це пояснюється використанням багатокритеріального оцінювання альтернатив і механізму адаптивного коригування ваг критеріїв. Отримані результати підтверджують ефективність використання багатокритеріального оцінювання та адаптивного коригування вагових коефіцієнтів під час підтримки прийняття рішень щодо забезпечення гарантоздатності інформаційних систем ситуаційних центрів.

На рис. 5 наведено порівняльну оцінку ефективності експертного, правило-орієнтованого та запропонованого методів за ключовими показниками: рівнем гарантоздатності, точністю, часткою успішних рішень, середньою функцією корисності та нормалізованим часом прийняття рішення. Отримані результати свідчать, що запропонований метод демонструє найкращі значення за всіма розглянутими критеріями, що підтверджує його перевагу та ефективність під час підтримки прийняття рішень щодо забезпечення гарантоздатності інформаційних систем ситуаційних центрів.

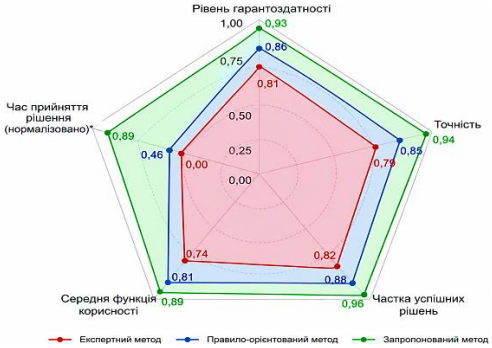

Рис. 5. Порівняння ефективності методів підтримки прийняття рішень

Для додаткового аналізу оцінено вплив адаптивного механізму коригування вагових коефіцієнтів на якість прийнятих рішень.

Таблиця 4

Вплив адаптації вагових коефіцієнтів на ефективність прийняття рішень

Кількість циклів адаптації	Точність вибору рішення	Середнє значення функції корисності
0	0,84	0,78
5	0,88	0,82
10	0,91	0,85
15	0,93	0,87
20	0,94	0,89

Отримані результати демонструють поступове підвищення точності прийняття рішень у міру накопичення досвіду функціонування системи. Аналогічний позитивний вплив адаптивного коригування параметрів та використання інтелектуальних моделей на якість прийняття рішень відзначається також у роботах [16-18]. Найбільший приріст спостерігається на початкових етапах адаптації, після чого показники стабілізуються, що свідчить про збіжність процесу налаштування вагових коефіцієнтів та підвищення якості прийняття рішень [9, 17].

На рис. 6 показано залежність точності вибору рішення та середнього значення функції корисності від кількості циклів адаптації вагових коефіцієнтів. Отримані результати свідчать про поступове зростання обох показників у процесі адаптації системи: точність вибору рішення збільшилася з 0,84 до 0,94, а середнє значення функції корисності – з 0,78 до 0,89. Найбільший приріст спостерігається на початкових етапах адаптації, після чого показники наближаються до стабільних значень, що підтверджує збіжність адаптивного механізму та підвищення ефективності підтримки прийняття рішень.

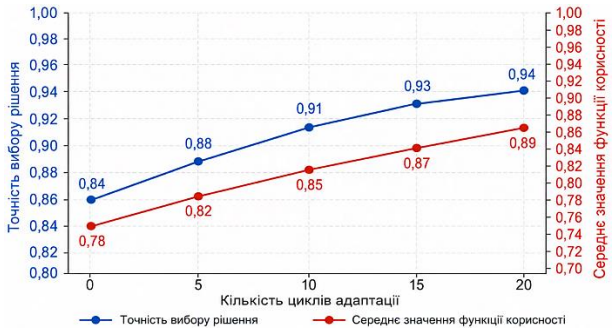

Рис. 6. Вплив адаптації вагових коефіцієнтів на якість прийняття рішень

Найбільший ефект спостерігається у сценаріях S3 та S4, де необхідно одночасно враховувати значну кількість критеріїв, альтернатив та ресурсних обмежень, що підтверджує доцільність використання багатокритеріального підходу до підтримки прийняття рішень.

Узагальнюючи результати моделювання, можна зробити висновок, що запропонований метод забезпечує ефективне формування та оцінювання альтернатив, скорочує час прийняття рішень і підвищує рівень гарантоздатності інформаційних систем ситуаційних центрів. Запропонований адаптивний механізм дозволяє враховувати результати попередніх рішень та підвищувати якість функціонування системи підтримки прийняття рішень у процесі експлуатації.

Обговорення. Отримані результати підтверджують ефективність запропонованого методу підтримки прийняття рішень щодо забезпечення гарантоздатності інформаційних систем ситуаційних центрів. На відміну від існуючих підходів [1-8, 11], метод поєднує аналіз стану системи, оцінювання ризиків, формування множини допустимих альтернатив, їх багатокритеріальне оцінювання та адаптивний вибір рішення в межах єдиного процесу підтримки прийняття рішень.

Дослідження [1-3, 11] підтверджують доцільність використання інтелектуальних технологій для підвищення стійкості критичної інфраструктури, однак не містять формалізованого механізму вибору альтернатив щодо підтримання гарантоздатності інформаційних систем. На відміну від підходів, орієнтованих переважно на оцінювання ризиків і ситуаційну обізнаність [4-6, 21, 23], запропонований метод забезпечує вибір оптимальної альтернативи на основі інтегральної функції корисності.. Порівняно з сучасними рішеннями для реагування на інциденти [9, 19], метод додатково враховує ресурсні обмеження, вплив рішень на гарантоздатність та результати попередніх управлінських впливів.

Важливою особливістю запропонованого підходу є використання адаптивного механізму коригування ваг критеріїв та накопичення знань про результати реалізації управлінських рішень. Подібні принципи адаптивного управління та інтелектуального аналізу даних розглядаються у роботах [12, 14, 16, 18], однак запропонований метод інтегрує їх у єдину процедуру забезпечення гарантоздатності інформаційних систем ситуаційних центрів.

Результати моделювання показали, що застосування запропонованого методу дозволяє підвищити рівень гарантоздатності навіть за умов зростання рівня ризику. Найбільший ефект спостерігається у сценаріях S3 та S4, де необхідно враховувати значну кількість взаємопов'язаних факторів, альтернатив та ресурсних обмежень. Отримані результати також підтверджують позитивний вплив адаптивного коригування ваг критеріїв на якість прийняття рішень. Аналогічні тенденції щодо підвищення ефективності управління на основі інтелектуального аналізу ризиків та використання когнітивних механізмів підтримки прийняття рішень відзначаються у роботах [22, 26, 28].

Водночас дослідження має певні обмеження. Отримані результати базуються на імітаційному моделюванні та потребують подальшої перевірки на реальних даних функціонування інформаційних систем ситуаційних центрів. Крім того, у роботі не розглядалися питання автоматичного формування критеріїв оцінювання та використання методів машинного навчання для прогнозування зміни показників гарантоздатності. Перспективним напрямом подальших досліджень є інтеграція технологій штучного інтелекту, прогнозної аналітики та моделей пояснюваного прийняття рішень, які активно розвиваються в сучасних системах кібербезпеки [29-30].

Загалом отримані результати підтверджують доцільність використання запропонованого методу як складової інтелектуальних систем підтримки прийняття рішень щодо забезпечення гарантоздатності інформаційних систем ситуаційних центрів та створюють підгрунтя для подальших досліджень у цьому напрямі.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті вирішено актуальне науково-практичне завдання розроблення методу підтримки прийняття рішень щодо забезпечення гарантоздатності інформаційних систем ситуаційних центрів в умовах дестабілізуючих впливів та ресурсних обмежень. Проведено аналіз сучасних підходів до забезпечення гарантоздатності інформаційних систем і підтримки прийняття рішень в умовах динамічних загроз, формалізовано процес прийняття рішень з урахуванням поточного стану системи, рівня ризику, ресурсних обмежень та множини можливих альтернатив.

Розроблено математичну модель подання стану інформаційної системи, критеріїв оцінювання та множини допустимих альтернатив. Запропоновано метод багатокритеріального оцінювання альтернатив і адаптивного вибору рішень на основі інтегральної функції корисності та механізму коригування вагових коефіцієнтів критеріїв. Також розроблено архітектуру інтелектуальної системи підтримки прийняття рішень, яка інтегрує процеси моніторингу, аналізу ризиків, формування альтернатив, оцінювання рішень та накопичення знань.

Результати моделювання підтвердили ефективність запропонованого методу. Порівняно з правило-орієнтованим підходом забезпечено підвищення рівня гарантоздатності на 8,1 %, збільшення точності вибору альтернатив на 10,6 %, підвищення частки успішних рішень на 9,1 % та скорочення часу прийняття рішень на 44,9 %.

Наукова новизна полягає у розробленні методу підтримки прийняття рішень щодо забезпечення гарантоздатності інформаційних систем ситуаційних центрів, який, на відміну від існуючих підходів, інтегрує формування множини допустимих альтернатив, їх багатокритеріальне оцінювання та адаптивний вибір рішень з урахуванням поточного стану системи, рівня ризику та ресурсних обмежень.

Перспективи подальших досліджень полягають у розробленні методів прогнозування показників гарантоздатності на основі технологій машинного навчання, удосконаленні механізмів автоматичного налаштування вагових коефіцієнтів критеріїв та апробації запропонованого методу на реальних інформаційних системах ситуаційних центрів і об'єктах критичної інфраструктури.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ajayi, O. O., Kurien, A., Djouani, K., & Dieng, L. (2025). Artificial intelligence for infrastructure resilience: Transportation systems as a strategic case for policy and practice. *Sustainability, 17*(20), Article 8992. https://doi.org/10.3390/su17208992

2. Leyli-Abadi, M., Bessa, R. J., Viebahn, J., Boos, D., Borst, C., Castagna, A., & Yagoubi, M. (2025). A conceptual framework for AI-based decision systems in critical infrastructures. In *2025 IEEE International Conference on Systems, Man, and Cybernetics (SMC)* (pp. 5799-5806). IEEE.
3. Järveläinen, J., Dang, D., Mekkanen, M., & Vartiainen, T. (2025). Towards a framework for improving cybersecurity resilience of critical infrastructure against cyber threats: A dynamic capabilities approach. *Journal of Decision Systems, 34*(1). https://doi.org/10.1080/12460125.2025.2479546
4. Jovanović, A. S. (2025). Stress-testing the resilience of critical infrastructures exposed to polycrises triggered by emerging risks. *International Journal of Disaster Risk Science, 16*, 594-617. https://doi.org/10.1007/s13753-025-00663-0
5. Pasic, A. (2025). Crisis management and resilience of critical infrastructure: SUNRISE project insights. *Crisis Management Days*. https://ojs.vvg.hr/index.php/DKU/article/view/673
6. Bîlbîie, I., & Ciolponea, C.-A. (2025). Considerations on cyber situational awareness: Theoretical fundamentals and implementation models. *Land Forces Academy Review, 30*, 445-453. https://doi.org/10.2478/raft-2025-0043
7. Kramer, D., Rosique, L., Narotam, A., Bursztein, E., Kelley, P. G., Thomas, K., & Woodruff, A. (2025). Integrating large language models into security incident response. In *Proceedings of the Twenty-First USENIX Conference on Usable Privacy and Security (SOUPS '25)* (Article 8, pp. 133-148). USENIX Association.
8. Hammar, K., Alpcan, T., & Lupu, E. C. (2025). *Incident response planning using a lightweight large language model with reduced hallucination* (arXiv:2508.05188). arXiv.
9. Ren, S., Jin, J., Niu, G., & Liu, Y. (2025). ARCS: Adaptive reinforcement learning framework for automated cybersecurity incident response strategy optimization. *Applied Sciences, 15*(2), Article 951. https://doi.org/10.3390/app15020951
10. Kostiuk, Y., Skladannyi, P., & Rzaieva, S. (2026). Quality management of SIEM alerts based on risk-oriented assessment and SOC feedback. *Ukrainian Information Security Research Journal, 31*(3), 151-163. https://doi.org/10.18372/2225-5036.31.21161
11. Muñoz-Navarro, E., Hernández-Montesinos, J. J., Marqués-Moreno, A., Papadopoulos, L., Karteris, A., & Demestichas, K. (2025). PRAETORIAN: From protection to resilience of critical infrastructures. In I. Gkotsis, D. Kavallieros, N. Stoianov, S. Vrochidis, D. Diagourtas, & B. Akhgar (Eds.), *Paradigms on technology development for security practitioners* (Security Informatics and Law Enforcement). Springer. https://doi.org/10.1007/978-3-031-62083-6_13
12. Kostiuk, Y., Rzaieva, S., & Rzaiev, D. (2026). Intelligent analysis of network traffic for detecting information security incidents. *Science and Technology Today, 2*(56), 1909–1928. https://doi.org/10.52058/2786-6025-2026-2(56)-1909-1928
13. Dacorogna, M., Debbabi, N., & Kratz, M. (2023). Building up cyber resilience by better grasping cyber risk via a new algorithm for modelling heavy-tailed data. *European Journal of Operational Research, 311*(2), 707–721. https://doi.org/10.1016/j.ejor.2023.05.003
14. Kostiuk, Y., Skladannyi, P., Rzaieva, S., Samoilenko, Y., & Korshun, N. (2025). Intelligent control and protection systems in cyber-physical and cloud Smart Grid environments. *Cybersecurity: Education, Science, Technique, 2*(30), 125–156. https://doi.org/10.28925/2663-4023.2025.30.956
15. Yazo-Cabuya, E. J., Ibeas, A., & Rey-Caballero, R. (2025). Multi-criteria decision making for risk management in quality management systems. *Sustainability, 17*(3), Article 1092. https://doi.org/10.3390/su17031092
16. Dovzhenko, N., Ivanichenko, Y., & Kostiuk, Y. (2025). A methodology for detecting and localizing cyber threats in cloud environments with integrated IoT components based on graph models. *Cybersecurity: Education, Science, Technique, 1*(29), 762-776. https://doi.org/10.28925/2663-4023.2025.29.938
17. Klein, T., & Romano, G. (2025). Optimizing cybersecurity incident response via adaptive reinforcement learning. *Journal of Advances in Engineering and Technology, 2*(1). https://doi.org/10.62177/jaet.v2i1.212
18. Skladannyi, P., Kostiuk, Y., Rzaieva, S., Samoilenko, Y., & Savchenko, T. (2025). Development of modular neural networks for detecting different classes of network attacks. *Cybersecurity: Education, Science, Technique, 3*(27), 534-548. https://doi.org/10.28925/2663-4023.2025.27.772
19. Lin, X., Zhang, J., Deng, G., Liu, T., Zhang, T., Guo, Q., & Chen, R. (2025). *IRCopilot: Automated incident response with large language models* (arXiv:2505.20945). arXiv.
20. Rzaieva, S. L., Lytvyn, O. S., Skladannyi, P. M., Kostiuk, Y. V., & Rzaiev, D. O. (2026). A model of adaptive cybersecurity management for information and communication systems based on a risk-oriented

approach. *Mathematical Machines and Systems, 2*, 92-109. https://doi.org/10.34121/1028-9763-2026-2-92-109

21. Alavizadeh, H., Jang-Jaccard, J., Enoch, S. Y., Al-Sahaf, H., Welch, I., Camtepe, S. A., & Kim, D. S. (2022). A survey on threat situation awareness systems: Framework, techniques, and insights. *ACM Computing Surveys, 55*(5), Article 107. https://doi.org/10.1145/3530809
22. 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 on Software Engineering and Semantic Technologies (SEST 2025), co-located with the 15th International Scientific and Practical Programming Conference (UkrPROG 2025)* (CEUR Workshop Proceedings, Vol. 4053, pp. 237-251). CEUR-WS.org.
23. Aghazadeh Ardebili, A., Lezzi, M., & Pourmadadkar, M. (2024). Risk assessment for cyber resilience of critical infrastructures: Methods, governance, and standards. *Applied Sciences, 14*(24), Article 11807. https://doi.org/10.3390/app142411807
24. Kostiuk, Y. (2025). Multi-agent system for detecting and counteracting attacks on the enterprise information system. In *Insider threats and security in corporations* (pp. 205-232). https://doi.org/10.36690/ITSC-205-232
25. Maček, D., Magdalenić, I., & Begičević Ređep, N. (2021). A model for the evaluation of critical IT systems using multicriteria decision-making with elements for risk assessment. *Mathematics, 9*(9), Article 1045.
26. Kostiuk, Y., Skladannyi, P., Sokolov, V., & Vorokhob, M. (2025). Models and technologies of cognitive agents for decision-making with integration of artificial intelligence. In *Proceedings of the Modern Data Science Technologies Doctoral Consortium (MoDaST 2025)* (CEUR Workshop Proceedings, Vol. 4005, pp. 82-96). CEUR-WS.org.
27. Kure, H. I., Islam, S., & Mouratidis, H. (2022). An integrated cybersecurity risk management framework and risk prediction for critical infrastructure protection. *Neural Computing and Applications, 34*(18), 15241-15271.
28. Kostiuk, Y., Skladannyi, P., Sokolov, V., Hulak, H., & Korshun, N. (2024). Models and algorithms for analyzing information risks during the security audit of personal data information systems. In *Proceedings of the Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN'24)* (CEUR Workshop Proceedings, Vol. 3925, pp. 155-171). CEUR-WS.org.
29. Sarker, I. H. (2024). Introduction to AI-driven cybersecurity and threat intelligence. In *AI-driven cybersecurity and threat intelligence: Cyber automation, intelligent decision-making and explainability* (pp. 3-19). Springer Nature Switzerland.
30. Pliekhov, O. (2026). *AI-driven message prioritization for offline BLE mesh networks in disaster response scenarios* [Preprint]. SSRN. https://doi.org/10.2139/ssrn.6428398

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023

Victor Hrechaninov
postgraduate
Institute of Mathematical Machines and Systems Problems, Kyiv, Ukraine
ORCID: 0009-0002-8400-6401
vgrechaninov@gmail.com

METHOD FOR DECISION SUPPORT AND DEPENDABILITY ASSURANCE OF INFORMATION SYSTEMS OF SITUATIONAL CENTERS

Abstract. The paper addresses the problem of decision support for ensuring the dependability of information systems of situational centers under conditions of increasing complexity of information and communication infrastructures, a growing number of destabilizing influences, and rising requirements for the continuity of critical service operation. The relevance of the study is determined by the need to improve the validity of decisions made during the management of situational center information systems, as well as the necessity to consider a large number of interrelated operational parameters, risks, and potential consequences of threat realization. The aim of the study is to develop a method for decision support and dependability assurance of situational center information systems based on comprehensive system state analysis, risk assessment, and multicriteria selection of alternatives. The decision-support process for ensuring the dependability of situational center information systems is formalized, and a mathematical model is developed that takes into account the current system state, risk level, available resources, and possible consequences of destabilizing influences. A method is proposed that enables the generation of a set of feasible alternatives, their multicriteria evaluation, and the selection of the most appropriate decision considering its impact on dependability indicators. An architecture of an intelligent decision support system is developed, providing knowledge accumulation, adaptation to changing operating conditions, and improvement of decision quality. Unlike existing approaches, the proposed method integrates information system state assessment, risk analysis, alternative generation, and decision support within a unified dependability assurance process. Simulation results confirmed improved decision validity, reduced time required for alternative selection, and enhanced dependability indicators of the information system. The practical significance of the study lies in the possibility of applying the proposed method in situational center information systems to improve management efficiency, operational resilience, and continuity of information service provision.

Keywords: dependability; information systems; situational centers; decision support; intelligent technologies; multicriteria evaluation; risk management; knowledge base; adaptive decision-making; cybersecurity.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Ajayi, O. O., Kurien, A., Djouani, K., & Dieng, L. (2025). Artificial intelligence for infrastructure resilience: Transportation systems as a strategic case for policy and practice. *Sustainability*, *17*(20), Article 8992. https://doi.org/10.3390/su17208992
2. Leyli-Abadi, M., Bessa, R. J., Viebahn, J., Boos, D., Borst, C., Castagna, A., & Yagoubi, M. (2025). A conceptual framework for AI-based decision systems in critical infrastructures. In *2025 IEEE International Conference on Systems, Man, and Cybernetics (SMC)* (pp. 5799-5806). IEEE.
3. Järveläinen, J., Dang, D., Mekkanen, M., & Vartiainen, T. (2025). Towards a framework for improving cybersecurity resilience of critical infrastructure against cyber threats: A dynamic capabilities approach. *Journal of Decision Systems*, *34*(1). https://doi.org/10.1080/12460125.2025.2479546
4. Jovanović, A. S. (2025). Stress-testing the resilience of critical infrastructures exposed to polycrises triggered by emerging risks. *International Journal of Disaster Risk Science*, *16*, 594-617. https://doi.org/10.1007/s13753-025-00663-0
5. Pasic, A. (2025). Crisis management and resilience of critical infrastructure: SUNRISE project insights. *Crisis Management Days*. https://ojs.vvg.hr/index.php/DKU/article/view/673
6. Bîlbîie, I., & Ciolponea, C.-A. (2025). Considerations on cyber situational awareness: Theoretical fundamentals and implementation models. *Land Forces Academy Review*, *30*, 445-453. https://doi.org/10.2478/raft-2025-0043

7. Kramer, D., Rosique, L., Narotam, A., Bursztein, E., Kelley, P. G., Thomas, K., & Woodruff, A. (2025). Integrating large language models into security incident response. In *Proceedings of the Twenty-First USENIX Conference on Usable Privacy and Security (SOUPS '25)* (Article 8, pp. 133-148). USENIX Association.
8. Hammar, K., Alpcan, T., & Lupu, E. C. (2025). *Incident response planning using a lightweight large language model with reduced hallucination* (arXiv:2508.05188). arXiv.
9. Ren, S., Jin, J., Niu, G., & Liu, Y. (2025). ARCS: Adaptive reinforcement learning framework for automated cybersecurity incident response strategy optimization. *Applied Sciences*, *15*(2), Article 951. https://doi.org/10.3390/app15020951
10. Kostiuk, Y., Skladannyi, P., & Rzaieva, S. (2026). Quality management of SIEM alerts based on risk-oriented assessment and SOC feedback. *Ukrainian Information Security Research Journal*, *31*(3), 151-163. https://doi.org/10.18372/2225-5036.31.21161
11. Muñoz-Navarro, E., Hernández-Montesinos, J. J., Marqués-Moreno, A., Papadopoulos, L., Karteris, A., & Demestichas, K. (2025). PRAETORIAN: From protection to resilience of critical infrastructures. In I. Gkotsis, D. Kavallieros, N. Stoianov, S. Vrochidis, D. Diagourtas, & B. Akhgar (Eds.), *Paradigms on technology development for security practitioners* (Security Informatics and Law Enforcement). Springer. https://doi.org/10.1007/978-3-031-62083-6_13
12. Kostiuk, Y., Rzaieva, S., & Rzaiev, D. (2026). Intelligent analysis of network traffic for detecting information security incidents. *Science and Technology Today*, *2*(56), 1909–1928. https://doi.org/10.52058/2786-6025-2026-2(56)-1909-1928
13. Dacorogna, M., Debbabi, N., & Kratz, M. (2023). Building up cyber resilience by better grasping cyber risk via a new algorithm for modelling heavy-tailed data. *European Journal of Operational Research, 311*(2), 707–721. https://doi.org/10.1016/j.ejor.2023.05.003
14. Kostiuk, Y., Skladannyi, P., Rzaieva, S., Samoilenko, Y., & Korshun, N. (2025). Intelligent control and protection systems in cyber-physical and cloud Smart Grid environments. *Cybersecurity: Education, Science, Technique, 2*(30), 125–156. https://doi.org/10.28925/2663-4023.2025.30.956
15. Yazo-Cabuya, E. J., Ibeas, A., & Rey-Caballero, R. (2025). Multi-criteria decision making for risk management in quality management systems. *Sustainability*, *17*(3), Article 1092. https://doi.org/10.3390/su17031092
16. Dovzhenko, N., Ivanichenko, Y., & Kostiuk, Y. (2025). A methodology for detecting and localizing cyber threats in cloud environments with integrated IoT components based on graph models. *Cybersecurity: Education, Science, Technique, 1*(29), 762-776. https://doi.org/10.28925/2663-4023.2025.29.938
17. Klein, T., & Romano, G. (2025). Optimizing cybersecurity incident response via adaptive reinforcement learning. *Journal of Advances in Engineering and Technology*, *2*(1). https://doi.org/10.62177/jaet.v2i1.212
18. Skladannyi, P., Kostiuk, Y., Rzaieva, S., Samoilenko, Y., & Savchenko, T. (2025). Development of modular neural networks for detecting different classes of network attacks. *Cybersecurity: Education, Science, Technique, 3*(27), 534-548. https://doi.org/10.28925/2663-4023.2025.27.772
19. Lin, X., Zhang, J., Deng, G., Liu, T., Zhang, T., Guo, Q., & Chen, R. (2025). *IRCopilot: Automated incident response with large language models* (arXiv:2505.20945). arXiv.
20. Rzaieva, S. L., Lytvyn, O. S., Skladannyi, P. M., Kostiuk, Y. V., & Rzaiev, D. O. (2026). A model of adaptive cybersecurity management for information and communication systems based on a risk-oriented approach. *Mathematical Machines and Systems*, *2*, 92-109. https://doi.org/10.34121/1028-9763-2026-2-92-109
21. Alavizadeh, H., Jang-Jaccard, J., Enoch, S. Y., Al-Sahaf, H., Welch, I., Camtepe, S. A., & Kim, D. S. (2022). A survey on threat situation awareness systems: Framework, techniques, and insights. *ACM Computing Surveys, 55*(5), Article 107. https://doi.org/10.1145/3530809
22. 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 on Software Engineering and Semantic Technologies (SEST 2025), co-located with the 15th International Scientific and Practical Programming Conference (UkrPROG 2025)* (CEUR Workshop Proceedings, Vol. 4053, pp. 237-251). CEUR-WS.org.
23. Aghazadeh Ardebili, A., Lezzi, M., & Pourmadadkar, M. (2024). Risk assessment for cyber resilience of critical infrastructures: Methods, governance, and standards. *Applied Sciences*, *14*(24), Article 11807. https://doi.org/10.3390/app142411807

24. Kostiuk, Y. (2025). Multi-agent system for detecting and counteracting attacks on the enterprise information system. In *Insider threats and security in corporations* (pp. 205-232). https://doi.org/10.36690/ITSC-205-232
25. Maček, D., Magdalenić, I., & Begičević Ređep, N. (2021). A model for the evaluation of critical IT systems using multicriteria decision-making with elements for risk assessment. *Mathematics*, *9*(9), Article 1045.
26. Kostiuk, Y., Skladannyi, P., Sokolov, V., & Vorokhob, M. (2025). Models and technologies of cognitive agents for decision-making with integration of artificial intelligence. In *Proceedings of the Modern Data Science Technologies Doctoral Consortium (MoDaST 2025)* (CEUR Workshop Proceedings, Vol. 4005, pp. 82-96). CEUR-WS.org.
27. Kure, H. I., Islam, S., & Mouratidis, H. (2022). An integrated cybersecurity risk management framework and risk prediction for critical infrastructure protection. *Neural Computing and Applications*, *34*(18), 15241-15271.
28. Kostiuk, Y., Skladannyi, P., Sokolov, V., Hulak, H., & Korshun, N. (2024). Models and algorithms for analyzing information risks during the security audit of personal data information systems. In *Proceedings of the Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN'24)* (CEUR Workshop Proceedings, Vol. 3925, pp. 155-171). CEUR-WS.org.
29. Sarker, I. H. (2024). Introduction to AI-driven cybersecurity and threat intelligence. In *AI-driven cybersecurity and threat intelligence: Cyber automation, intelligent decision-making and explainability* (pp. 3-19). Springer Nature Switzerland.
30. Pliekhov, O. (2026). *AI-driven message prioritization for offline BLE mesh networks in disaster response scenarios* [Preprint]. SSRN. https://doi.org/10.2139/ssrn.6428398

Отримано редакцією журналу / Received: 22.01.26
Прорецензовано / Revised: 05.02.26
Схвалено до друку / Accepted: 24.09.26