

Гречанінов Віктор Федорович

аспірант

Інститут проблем математичних машин і систем НАН України, м. Київ, Україна

ORCID ID: 0009-0002-8400-6401

vgrechaninov@gmail.com

МЕТОД ОЦІНЮВАННЯ ТА ПРОГНОЗУВАННЯ СТАНУ ГАРАНТОЗДАТНОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Анотація. У статті розглянуто проблему оцінювання та прогнозування стану гарантоздатності об'єктів критичної інфраструктури в умовах зростання кількості кіберзагроз, технічних відмов та дестабілізуючих впливів. Актуальність дослідження зумовлена необхідністю забезпечення безперервності функціонування критично важливих систем шляхом своєчасного виявлення тенденцій погіршення їхнього стану та формування обґрунтованих управлінських рішень. Метою роботи є розроблення методу оцінювання та прогнозування гарантоздатності об'єктів критичної інфраструктури із застосуванням інтелектуальних технологій підтримки прийняття рішень. Запропоновано метод, який поєднує процедури збору та аналізу даних моніторингу, оцінювання ризиків, формування інтегрального показника гарантоздатності та прогнозування його зміни у часі. Розроблено математичну модель оцінювання гарантоздатності на основі сукупності показників кібербезпеки, надійності, доступності, живучості та відновлюваності об'єкта. Удосконалено підхід до підтримки прийняття рішень шляхом використання інтелектуальної технології, що поєднує оцінювання поточного стану гарантоздатності, прогнозування його зміни та застосування моделі машинного навчання для раннього виявлення критичних станів і вибору найбільш доцільних заходів реагування. Розроблено алгоритм визначення критичних станів об'єкта та формування рекомендацій щодо підвищення рівня його гарантоздатності. Для перевірки ефективності запропонованого підходу проведено моделювання чотирьох сценаріїв функціонування об'єкта критичної інфраструктури. Отримані результати показали підвищення точності прогнозування стану гарантоздатності до 92,4 %, зменшення середнього часу формування управлінських рішень на 31,7 % та зниження інтегрального рівня ризику на 28,5 % порівняно з традиційними підходами. Встановлено, що використання інтелектуальних технологій підтримки прийняття рішень забезпечує своєчасне виявлення потенційно небезпечних тенденцій та підвищує обґрунтованість вибору заходів реагування. Практична цінність роботи полягає у можливості використання запропонованого методу в ситуаційних центрах та інформаційно-аналітичних системах управління об'єктами критичної інфраструктури.

Ключові слова: гарантоздатність; об'єкти критичної інфраструктури; підтримка прийняття рішень; інтелектуальні технології; прогнозування стану; оцінювання ризиків; ситуаційний центр; кібербезпека; інформаційно-аналітична система; моніторинг.

Hrechaninov Victor

postgraduate

Institute of Mathematical Machines and Systems Problems, Kyiv, Ukraine

ORCID: 0009-0002-8400-6401

vgrechaninov@gmail.com

METHOD FOR ASSESSING AND FORECASTING THE DEPENDABILITY STATE OF CRITICAL INFRASTRUCTURE OBJECTS

Abstract. This paper addresses the problem of assessing and forecasting the dependability state of critical infrastructure objects under conditions of increasing cyber threats, technical failures, and destabilizing influences. The relevance of the study is determined by the need to ensure the continuity of operation of critical systems through the timely identification of trends indicating deterioration of their condition and the formation of well-grounded management decisions. The aim of the study is to develop a method for assessing and forecasting the dependability of critical infrastructure objects using intelligent decision-support technologies. A method is proposed that combines procedures for collecting and analyzing monitoring data, risk assessment, the formation of an integrated dependability indicator, and forecasting its changes over time. A mathematical model for dependability assessment based on a set of cybersecurity, reliability, availability, survivability, and recoverability indicators of the object has been developed. The decision-support approach has been improved through the use of an intelligent technology that integrates assessment of the current dependability state, forecasting of its changes, and the application of a machine learning model for the early detection of critical states and the selection of the most appropriate response measures. An algorithm for identifying critical states of a critical infrastructure object and generating recommendations for improving its dependability level has been developed. To validate the effectiveness of the proposed approach, simulation experiments were conducted for four operational scenarios of a critical infrastructure object. The obtained results demonstrated an increase in dependability forecasting accuracy to 92.4%, a reduction in the average time required for management decision-making by 31.7%, and a decrease in the integrated risk level by 28.5% compared to traditional approaches. It was established that the use of intelligent decision-support technologies ensures the timely detection of potentially dangerous trends and improves the justification of response measure selection. The practical value of the study lies in the possibility of applying the proposed method in situation centers and information-analytical management systems for critical infrastructure objects.

Keywords: dependability; critical infrastructure objects; decision support; intelligent technologies; state forecasting; risk assessment; situation center; cybersecurity; information and analytical system; monitoring.

© 2026 Гречанінов В.Ф.. Цей матеріал ліцензовано за умовами CC BY 4.0.

<https://creativecommons.org/licenses/by/4.0/>

1. Вступ

Сучасні об'єкти критичної інфраструктури функціонують в умовах постійного зростання кількості кіберзагроз, технічних відмов, інформаційних атак та інших дестабілізуючих впливів, здатних призвести до порушення безперервності надання життєво важливих послуг [1, 11]. Особливої актуальності ця проблема набуває в умовах цифрової трансформації суспільства, коли функціонування енергетичних, транспортних, телекомунікаційних, фінансових та державних інформаційних систем значною мірою залежить від складних програмно-технічних комплексів [7, 9, 13]. За таких умов забезпечення гарантоздатності об'єктів критичної інфраструктури стає одним із ключових завдань сучасних інформаційних технологій та систем підтримки прийняття рішень.

Традиційні підходи до оцінювання стану об'єктів критичної інфраструктури переважно орієнтовані на аналіз окремих характеристик, таких як надійність, доступність, кібербезпека або ризик виникнення інцидентів [8, 11, 26]. Проте вони не забезпечують комплексного врахування взаємозв'язків між різнорідними показниками функціонування об'єкта та не дозволяють своєчасно прогнозувати зміну рівня його гарантоздатності в умовах динамічного середовища [2-6, 21-22]. Крім того, більшість існуючих рішень не використовують повною мірою можливості інтелектуального аналізу даних і сучасних технологій підтримки прийняття рішень для формування обґрунтованих рекомендацій щодо реагування на потенційні загрози [17].

Наукова проблема полягає у необхідності розроблення методу, який забезпечуватиме комплексне оцінювання та прогнозування стану гарантоздатності об'єктів критичної інфраструктури на основі аналізу великої кількості різнорідних параметрів функціонування, оцінювання ризиків та використання інтелектуальних механізмів підтримки прийняття рішень.

Метою статті є розроблення методу оцінювання та прогнозування стану гарантоздатності об'єктів критичної інфраструктури із застосуванням інтелектуальних технологій підтримки прийняття рішень, який забезпечує підвищення точності оцінювання поточного стану об'єкта, прогнозування його зміни та формування рекомендацій щодо забезпечення безперервності функціонування.

Наукова новизна отриманих результатів полягає у розробленні методу оцінювання та прогнозування стану гарантоздатності об'єктів критичної інфраструктури, який, на відміну від існуючих підходів, поєднує інтегральне оцінювання показників кібербезпеки, доступності, надійності, живучості та відновлюваності з адаптивним прогнозуванням зміни гарантоздатності та інтелектуальною підтримкою прийняття рішень на основі аналізу даних моніторингу [10, 12, 23], що забезпечує своєчасне виявлення критичних станів та підвищення обґрунтованості управлінських рішень.

Теоретичне значення дослідження полягає у розвитку науково-методичних засад оцінювання гарантоздатності об'єктів критичної інфраструктури шляхом формалізації процесів аналізу стану системи, оцінювання ризиків та прогнозування можливих сценаріїв її функціонування.

Практичне значення роботи полягає у можливості використання запропонованого методу в інформаційно-аналітичних системах ситуаційних центрів, системах моніторингу кібербезпеки та системах підтримки прийняття рішень для підвищення стійкості, безперервності функціонування та ефективності управління об'єктами критичної інфраструктури [14, 16, 18].

2. Постановка проблеми.

Функціонування сучасних об'єктів критичної інфраструктури потребує забезпечення високого рівня гарантоздатності, яка визначає здатність системи безпечно, надійно та безперервно виконувати свої функції в умовах дестабілізуючих впливів, зокрема кібератак, технічних відмов, програмних помилок, людського фактора та порушень мережевої взаємодії.

Сучасні системи моніторингу накопичують значні обсяги даних про стан інформаційно-комунікаційної інфраструктури, однак їх використання здебільшого обмежується контролем окремих показників безпеки, продуктивності або надійності [10, 20]. Водночас оцінювання гарантоздатності потребує комплексного врахування взаємопов'язаних характеристик, таких як кібербезпека, доступність, живучість, відмовостійкість, відновлюваність і ризикостійкість [11, 21]. Існуючі підходи переважно аналізують окремі складові гарантоздатності та не забезпечують інтегрального оцінювання стану об'єкта з урахуванням прогнозованих змін його функціонування.

Особливо важливим є своєчасне прогнозування зниження рівня гарантоздатності, оскільки ефективність реагування залежить від можливості завчасного виявлення негативних тенденцій та прийняття обґрунтованих рішень [2-5]. Проте наявні методи недостатньо враховують взаємозв'язки між різнорідними параметрами функціонування об'єкта та обмежено використовують можливості інтелектуального аналізу даних [15, 24].

Тому актуальним науково-практичним завданням є розроблення методу оцінювання та прогнозування стану гарантоздатності об'єктів критичної інфраструктури, який забезпечує комплексний аналіз поточного стану, прогнозування його зміни на основі даних моніторингу та підтримку прийняття рішень щодо забезпечення необхідного рівня гарантоздатності.

3. Аналіз останніх досліджень і публікацій.

Питання забезпечення гарантоздатності та стійкості об'єктів критичної інфраструктури останніми роками набувають особливої актуальності у зв'язку зі зростанням складності кіберзагроз, взаємозалежності інфраструктурних систем та необхідності оперативного прийняття рішень в умовах невизначеності.

У роботі Muñoz-Navarro та ін. запропоновано концепцію переходу від традиційного захисту до забезпечення стійкості критичної інфраструктури на основі інтеграції механізмів моніторингу, аналізу подій безпеки та підтримки прийняття рішень [1]. Автори акцентують увагу на підвищенні ситуаційної обізнаності операторів, проте питання кількісного оцінювання та прогнозування гарантоздатності об'єктів не розглядаються.

У дослідженні Ren, Jin, Niu та Liu розроблено адаптивний підхід до реагування на кіберінциденти із застосуванням навчання з підкріпленням, що дозволяє автоматизувати вибір стратегій реагування залежно від поточного стану середовища [2]. Незважаючи на високу ефективність запропонованого підходу, він орієнтований переважно на реагування на інциденти та не враховує комплексне оцінювання гарантоздатності об'єкта.

Klein та Romano запропонували модель адаптивного управління процесами реагування на кіберінциденти на основі технологій машинного навчання [3]. Отримані результати демонструють підвищення ефективності реагування та оптимізацію використання ресурсів, однак довгострокове прогнозування стану об'єкта критичної інфраструктури залишається поза межами дослідження.

У роботі Lin та ін. представлено систему IRCopilot, яка використовує великі мовні моделі для автоматизації процесів реагування на інциденти кібербезпеки [4]. Запропонований підхід демонструє значний потенціал генеративного штучного інтелекту для підтримки прийняття рішень, проте не містить формалізованих механізмів оцінювання та прогнозування рівня гарантоздатності.

Liu досліджує застосування мультиагентних систем на основі великих мовних моделей для координації процесів реагування на інциденти [5]. Автором показано можливість підвищення ефективності колективного аналізу подій безпеки, однак питання інтегрального оцінювання стану критичної інфраструктури не розглядається.

У роботі Kramer та ін. проаналізовано можливості інтеграції великих мовних моделей у процеси реагування на інциденти інформаційної безпеки [6]. Результати дослідження підтверджують перспективність використання генеративного штучного інтелекту для підтримки фахівців з кібербезпеки, проте автори не приділяють уваги прогнозуванню зміни стану об'єкта на основі накопичених даних моніторингу.

Ajayi та ін. дослідили можливості використання технологій штучного інтелекту для забезпечення стійкості інфраструктурних систем та підтримки управлінських рішень [7]. Автори підкреслюють важливість прогнозувальної аналітики та машинного навчання для підвищення стійкості інфраструктури, однак не пропонують математичного апарату інтегрального оцінювання гарантоздатності.

У роботі Wang та ін. запропоновано підхід до аналізу стійкості взаємозалежних об'єктів критичної інфраструктури на основі методів глибокого навчання та теорії мереж [8]. Дослідження підтверджує ефективність використання інтелектуальних методів для аналізу складних інфраструктурних систем, проте основна увага зосереджена на оцінюванні стійкості мережевих структур, а не на прогнозуванні гарантоздатності окремих об'єктів.

Отже, проведений аналіз показав, що сучасні дослідження переважно спрямовані на забезпечення кіберстійкості, автоматизацію реагування на інциденти, застосування штучного інтелекту та аналіз складних інфраструктурних систем [1–8]. Водночас недостатньо дослідженою залишається проблема розроблення комплексного методу, який поєднує інтегральне оцінювання поточного стану гарантоздатності об'єкта критичної інфраструктури, прогнозування його зміни на основі даних моніторингу та формування рекомендацій для підтримки прийняття рішень. Саме розв'язанню зазначеної наукової проблеми присвячено дане дослідження.

Мета статті. Метою статті є розробка методу оцінювання та прогнозування стану гарантоздатності об'єктів критичної інфраструктури на основі інтелектуальних технологій підтримки прийняття рішень для підвищення точності оцінювання, своєчасного виявлення негативних тенденцій та обґрунтованого вибору заходів реагування.

Для досягнення поставленої мети у роботі необхідно вирішити такі завдання:

- проаналізувати сучасні підходи до оцінювання гарантоздатності об'єктів критичної інфраструктури та визначити їх переваги й обмеження;
- сформулювати систему показників оцінювання стану гарантоздатності об'єктів критичної інфраструктури з урахуванням характеристик кібербезпеки, доступності, надійності, живучості та відновлюваності;
- розробити математичну модель інтегрального оцінювання стану гарантоздатності об'єкта критичної інфраструктури;
- розробити метод прогнозування зміни рівня гарантоздатності на основі даних моніторингу та інтелектуального аналізу даних;
- розробити алгоритм підтримки прийняття рішень щодо забезпечення необхідного рівня гарантоздатності об'єкта;
- провести моделювання запропонованого методу та оцінити його ефективність за різних сценаріїв функціонування об'єкта критичної інфраструктури.

4. Виклад основного матеріалу дослідження

Для досягнення поставленої мети розроблено метод оцінювання та прогнозування стану гарантоздатності об'єктів критичної інфраструктури із застосуванням інтелектуальних технологій підтримки прийняття рішень [11, 22]. Запропонований метод базується на комплексному аналізі показників функціонування об'єкта, інтегральному оцінюванні його гарантоздатності, прогнозуванні зміни стану на основі даних моніторингу та формуванні рекомендацій щодо забезпечення безперервності функціонування [8, 13, 21]. Структура методу включає етапи формалізації процесу оцінювання гарантоздатності, побудови математичної моделі інтегрального оцінювання, прогнозування зміни стану об'єкта, реалізації інтелектуальної технології підтримки прийняття рішень та оцінювання ефективності запропонованого підходу.

Для наочного подання взаємозв'язків між основними компонентами запропонованого методу на рис. 1 наведено його структурну схему.

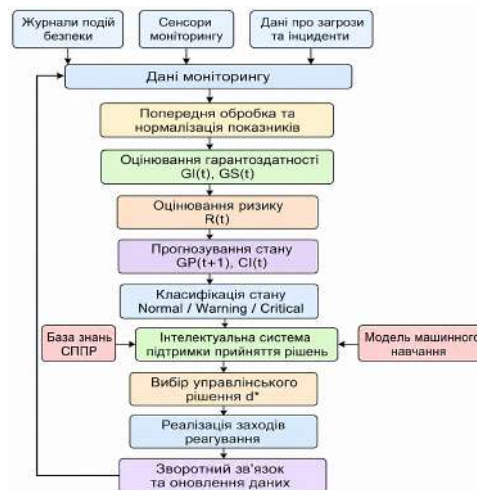


Рис. 1. Структурна схема методу оцінювання та прогнозування гарантоздатності об'єктів критичної інфраструктури

Рис. 1 ілюструє структурну схему запропонованого методу оцінювання та прогнозування гарантоздатності об'єктів критичної інфраструктури. Метод забезпечує послідовне виконання етапів збору та оброблення даних моніторингу, оцінювання гарантоздатності, аналізу ризиків, прогнозування стану об'єкта та формування управлінських рішень за допомогою інтелектуальної системи підтримки прийняття рішень [11, 15, 25]. Наявність зворотного зв'язку забезпечує адаптацію процесу оцінювання та підтримки прийняття рішень до змін умов функціонування об'єкта.

Формалізація процесу оцінювання гарантоздатності об'єктів критичної інфраструктури

Для оцінювання гарантоздатності об'єкта критичної інфраструктури необхідно враховувати сукупність характеристик, що визначають його здатність забезпечувати безперервне та безпечне функціонування в умовах дії дестабілізуючих факторів [13, 21, 26]. До основних складових гарантоздатності віднесемо кібербезпеку, доступність, надійність, живучість та відновлюваність.

Інтегральний стан об'єкта критичної інфраструктури подамо множиною:

$$G = \{C, A, R, V, D\}, \quad (1)$$

де C – показник кібербезпеки, A – показник доступності, R – показник надійності, V – показник живучості, D – показник відновлюваності.

Оскільки зазначені показники мають різні діапазони зміни та одиниці вимірювання, виконується їх нормалізація:

$$Z = \{z_1, z_2, \dots, z_n\}, \quad (2)$$

де z_i – нормалізоване значення i -го показника, n – кількість показників, що використовуються для оцінювання гарантоздатності.

Для врахування впливу кожного показника на загальний стан системи введемо множину вагових коефіцієнтів:

$$W = \{w_1, w_2, \dots, w_n\}, \quad (3)$$

де w_i – ваговий коефіцієнт i -го показника, $\sum w_i = 1$, $w_i \geq 0$.

Отримані нормалізовані параметри та вагові коефіцієнти використовуються для побудови математичної моделі інтегрального оцінювання гарантоздатності об'єкта критичної інфраструктури.

Математична модель інтегрального оцінювання стану гарантоздатності

Для комплексного оцінювання гарантоздатності об'єкта критичної інфраструктури необхідно враховувати сукупний вплив усіх складових множини G , визначеної у (1). Інтегральний показник гарантоздатності визначається як:

$$GI(t) = \sum w_i \cdot z_i(t), \quad i = 1, n, \quad (4)$$

де $GI(t)$ – інтегральний показник гарантоздатності в момент часу t , w_i – ваговий коефіцієнт i -го показника, $z_i(t)$ – нормалізоване значення i -го показника, n – кількість показників оцінювання.

Оскільки різні складові гарантоздатності можуть мати неоднаковий рівень узгодженості, введемо коефіцієнт структурної збалансованості системи:

$$KB(t) = 1 - \sqrt{\frac{1}{n} \cdot \sum (z_i(t) - GI(t))^2}, \quad i = 1, n \quad (5)$$

де $KB(t)$ – коефіцієнт збалансованості; величина під коренем характеризує ступінь розкиду окремих показників відносно інтегрального значення гарантоздатності.

На функціонування об'єкта впливає множина загроз $T = \{t_1, t_2, \dots, t_m\}$, кожна з яких характеризується імовірністю виникнення та рівнем впливу. Інтегральний рівень загроз визначається як:

$$TL(t) = \sum (p_j \cdot i_j \cdot \lambda_j), \quad j = 1, m, \quad (6)$$

де p_j – імовірність реалізації j -ї загрози, i_j – інтенсивність впливу, λ_j – коефіцієнт критичності загрози, m – кількість виявлених загроз.

Для врахування нелінійного впливу загроз на стан об'єкта визначимо коефіцієнт деградації гарантоздатності:

$$KD(t) = \exp(-TL(t)), \quad (7)$$

де $KD(t) \in [0; 1]$ – коефіцієнт деградації стану об'єкта, $\exp(\cdot)$ – експоненціальна функція.

Тоді фактичний рівень гарантоздатності об'єкта визначається як:

$$GS(t) = GI(t) \cdot KB(t) \cdot KD(t), \quad (8)$$

де $GS(t)$ – скоригований показник гарантоздатності, що враховує поточний стан системи, узгодженість її складових та вплив дестабілізуючих факторів.

Для оцінювання ризику втрати гарантоздатності введемо функцію ризику:

$$R(t) = 1 - GS(t)^\beta, \quad (9)$$

де $R(t)$ – інтегральний рівень ризику, β – коефіцієнт чутливості моделі до зміни гарантоздатності. При $\beta > 1$ підвищується чутливість моделі до критичних станів об'єкта.

Таким чином, запропонована математична модель дозволяє здійснювати інтегральне оцінювання гарантоздатності об'єкта критичної інфраструктури з урахуванням значущості окремих показників, рівня їх збалансованості та впливу зовнішніх і внутрішніх загроз. Отримані значення $GI(t)$, $GS(t)$ та $R(t)$ використовуються на наступному етапі для прогнозування зміни стану гарантоздатності та підтримки прийняття рішень щодо забезпечення безперервності функціонування об'єкта.

Метод прогнозування зміни стану гарантоздатності

Для забезпечення своєчасного виявлення негативних тенденцій функціонування об'єкта критичної інфраструктури необхідно прогнозувати зміну рівня гарантоздатності на основі накопичених даних моніторингу [2-5, 11]. В основу прогнозування покладено аналіз часових рядів значень показника гарантоздатності $GS(t)$, отриманого відповідно до (8).

Прогнозоване значення гарантоздатності визначається як:

$$GP(t+1) = \alpha \cdot GS(t) + (1 - \alpha) \cdot GP(t), \quad (10)$$

де $GP(t+1)$ – прогнозоване значення гарантоздатності на наступний момент часу, $GS(t)$ – поточне значення гарантоздатності, $GP(t)$ – попереднє прогнозне значення, α – коефіцієнт адаптації моделі, що визначає вплив нових даних на результат прогнозування, $0 < \alpha < 1$.

Для оцінювання швидкості зміни стану гарантоздатності введемо показник динаміки:

$$\Delta G(t) = GP(t+1) - GS(t), \quad (11)$$

де $\Delta G(t)$ – прогнозована зміна рівня гарантоздатності. Додатне значення свідчить про покращення стану об'єкта, а від'ємне – про його погіршення.

На основі прогнозованого значення гарантоздатності та поточного рівня ризику формується індекс критичності стану:

$$CI(t) = R(t) \cdot (1 - GP(t+1)), \quad (12)$$

де $CI(t)$ – індекс критичності, $R(t)$ – інтегральний рівень ризику, визначений згідно з (9). Зростання значення $CI(t)$ свідчить про підвищення ймовірності переходу об'єкта до небезпечного або критичного стану.

Для інтерпретації результатів оцінювання та прогнозування стан об'єкта критичної інфраструктури класифікується як нормальний, небезпечний або критичний залежно від значення індексу критичності

$$S(t) = \{Normal, CI(t) < 0.2 \text{ Warning}, 0.2 \leq CI(t) < 0.5 \text{ Critical}, CI(t) \geq 0.5\}, \quad (13)$$

Нормальний стан характеризує відсутність суттєвих загроз функціонуванню об'єкта, небезпечний стан свідчить про наявність негативних тенденцій та необхідність посиленого моніторингу, а критичний стан потребує негайного реагування для запобігання втраті гарантоздатності.

Для підтримки прийняття рішень прогнозований стан об'єкта використовується для вибору найдоцільнішої альтернативи реагування за критерієм:

$$d^* = \arg U(d_i), \quad U(d_i) = \omega_1 GP(t+1) + \omega_2 (1 - CI(t)), \quad (14)$$

де $D = \{d_1, d_2, \dots, d_k\}$ – множина можливих управлінських рішень щодо забезпечення гарантоздатності об'єкта, d^* – найдоцільніше рішення, $U(d_i)$ – функція корисності i -ї альтернативи, $GP(t+1)$ – прогнозований рівень гарантоздатності, $CI(t)$ – індекс критичності стану, ω_1, ω_2 – вагові коефіцієнти важливості критеріїв, для яких виконується умова $\omega_1 + \omega_2 = 1$, $\omega_1 \geq 0$, $\omega_2 \geq 0$. Оператор $\arg \max$ забезпечує вибір альтернативи, що має найбільшу очікувану корисність з урахуванням прогнозованого стану об'єкта та рівня критичності.

Рис. 2 демонструє поверхню функції корисності $U(d_i)$, яка використовується для вибору оптимального управлінського рішення. Аналіз поверхні показує, що значення корисності зростає зі збільшенням прогнозованого рівня гарантоздатності $GP(t+1)$ та зменшенням індексу критичності $CI(t)$ [15, 23, 25]. Це дозволяє обирати рішення, які забезпечують найвищий рівень гарантоздатності об'єкта критичної інфраструктури.

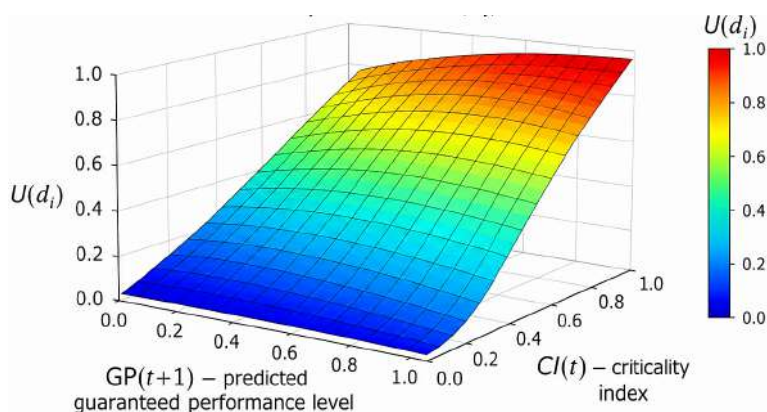


Рис. 2. Поверхня функції корисності $U(d_i)$ для вибору управлінського рішення

Таким чином, запропонований метод прогнозування дозволяє не лише оцінювати майбутній стан гарантоздатності об'єкта критичної інфраструктури, а й своєчасно виявляти потенційно небезпечні тенденції його функціонування та формувати рекомендації для підтримки прийняття управлінських рішень [15, 23-24]. Завдяки використанню адаптивного прогнозування, оцінювання динаміки зміни стану та індексу критичності забезпечується підвищення обґрунтованості рішень щодо підтримання необхідного рівня гарантоздатності об'єкта.

Інтелектуальна технологія підтримки прийняття рішень

Ефективність забезпечення гарантоздатності об'єктів критичної інфраструктури значною мірою залежить від своєчасності та обґрунтованості управлінських рішень. У зв'язку з цим запропонований метод оцінювання та прогнозування гарантоздатності інтегровано до інтелектуальної технології підтримки прийняття рішень, яка забезпечує автоматизований аналіз поточного стану об'єкта, прогнозування його зміни та формування рекомендацій щодо реагування на потенційні загрози.

Основою технології є поєднання засобів моніторингу, аналітичного оброблення даних, оцінювання ризиків, прогнозування стану гарантоздатності та інтелектуальної підтримки прийняття рішень [11, 15, 22, 24]. Вхідними даними системи є результати моніторингу стану інформаційно-комунікаційної інфраструктури, показники функціонування програмно-апаратних компонентів, журнали подій безпеки, дані про виявлені загрози та інциденти, а також результати попередніх оцінювань гарантоздатності [12, 14, 18].

Функціонування технології реалізується у вигляді послідовності взаємопов'язаних етапів. На першому етапі здійснюється збір та попередня обробка даних моніторингу, включаючи перевірку повноти інформації, усунення аномальних значень та нормалізацію показників. На другому етапі виконується оцінювання поточного стану гарантоздатності об'єкта за допомогою математичної моделі. На третьому етапі визначається рівень ризику функціонування об'єкта та здійснюється прогнозування зміни гарантоздатності відповідно до розробленого методу.

Особливістю запропонованої технології є використання інтелектуального механізму підтримки прийняття рішень, який аналізує результати оцінювання та прогнозування, визначає найбільш критичні фактори впливу на гарантоздатність і формує перелік можливих керуючих впливів [2-6, 15, 24]. Для цього використовується база знань, що містить правила реагування на типові ситуації, сценарії розвитку інцидентів та рекомендації щодо підвищення рівня гарантоздатності об'єкта.

Інтелектуальний механізм підтримки прийняття рішень реалізується на основі бази знань, що містить множини продукційних правил типу «умова–дія», та аналізу прогнозованих значень показників гарантоздатності. Формування рекомендацій здійснюється шляхом аналізу поточного значення гарантоздатності $GS(t)$, прогнозованого рівня гарантоздатності $GP(t + 1)$, індексу критичності $CI(t)$ та рівня ризику $R(t)$ [11, 23, 25]. На основі отриманих результатів система формує множини альтернативних рішень, виконує їх ранжування відповідно до очікуваної ефективності реагування та автоматично обирає найбільш доцільний сценарій підтримки гарантоздатності об'єкта критичної інфраструктури.

Для забезпечення адаптивності підтримки прийняття рішень база знань містить набір типових сценаріїв функціонування об'єкта критичної інфраструктури, сформованих на основі попереднього досвіду реагування на інциденти, експертних знань та результатів моніторингу [1, 22, 24]. У процесі роботи система виконує ранжування можливих альтернатив за критеріями ефективності, швидкості реалізації та очікуваного впливу на рівень гарантоздатності. Це забезпечує автоматизоване формування найбільш доцільних рекомендацій щодо підтримання безперервності функціонування об'єкта критичної інфраструктури.

Для підвищення якості рекомендацій використовуються результати інтелектуального аналізу даних моніторингу, що дозволяє враховувати приховані закономірності зміни гарантоздатності та адаптувати процес прийняття рішень до поточного стану об'єкта критичної інфраструктури [27, 29].

Інтелектуальний механізм підтримки прийняття рішень використовує узагальнену модель машинного навчання для класифікації станів об'єкта критичної інфраструктури на нормальний, небезпечний та критичний [2-5, 17]. Модель навчається на історичних даних моніторингу та дозволяє виявляти приховані закономірності зміни показників гарантоздатності, прогнозувати ймовірність переходу об'єкта до критичного стану та визначати найбільш впливові фактори ризику [2-3, 28]. Для навчання моделі використовуються накопичені дані моніторингу, журнали подій безпеки, інформація про інциденти та результати попереднього оцінювання гарантоздатності [12, 20]. Отримані результати використовуються для адаптивного коригування вагових коефіцієнтів показників, ранжування альтернативних управлінських рішень та формування рекомендацій щодо забезпечення необхідного рівня гарантоздатності.

Використання моделі машинного навчання забезпечує адаптацію процесу підтримки прийняття рішень до змін умов функціонування об'єкта та підвищує точність прогнозування його гарантоздатності.

Приклади продукційних правил, що використовуються інтелектуальною технологією підтримки прийняття рішень, наведено в табл. 1.

Таблиця 1

Приклади правил підтримки прийняття рішень

Умова	Рішення
$GS(t) > 0,85$ та $CI(t) < 0,2$	Продовження штатного режиму функціонування
$0,7 < GS(t) \leq 0,85$	Посилення моніторингу та контроль критичних сервісів
$0,5 < GS(t) \leq 0,7$	Активізація резервних ресурсів та додаткових засобів захисту
$GS(t) \leq 0,5$ або $CI(t) \geq 0,5$	Виконання аварійних процедур та негайне реагування

Наведені правила у табл. 1 є прикладом реалізації механізму інтелектуальної підтримки прийняття рішень. У реальній системі кількість правил може змінюватися залежно від особливостей об'єкта критичної інфраструктури, наявних загроз та вимог до рівня гарантоздатності.

На основі результатів аналізу система формує рекомендації для операторів ситуаційного центру або автоматизованої системи управління [15, 23, 25]. Залежно від поточного та прогнозованого стану гарантоздатності можуть бути запропоновані такі заходи, як посилення механізмів кіберзахисту, резервування ресурсів, зміна конфігурації мережевої інфраструктури, перерозподіл навантаження між компонентами системи, активація процедур аварійного відновлення або проведення додаткового моніторингу.

Запропонована інтелектуальна технологія підтримки прийняття рішень забезпечує перехід від реактивного до проактивного управління гарантоздатністю об'єктів критичної інфраструктури [24-26]. Це дозволяє не лише оперативно реагувати на поточні загрози, але й завчасно виявляти тенденції погіршення стану об'єкта, оцінювати можливі наслідки їх реалізації та обирати найбільш ефективні стратегії забезпечення безперервності функціонування критично важливих систем.

Алгоритм реалізації методу

Розроблений метод оцінювання та прогнозування стану гарантоздатності об'єктів критичної інфраструктури реалізується у вигляді послідовності взаємопов'язаних етапів, що забезпечують отримання даних моніторингу, оцінювання поточного стану системи, прогнозування його зміни та формування рекомендацій щодо підтримки прийняття рішень. Алгоритм функціонування методу наведено на рис. 3.

На рис. 3 наведено алгоритм реалізації запропонованого методу. Алгоритм включає етапи збору та попередньої обробки даних моніторингу, оцінювання гарантоздатності й ризику функціонування об'єкта,

прогнозування його стану, визначення рівня критичності на основі індексу $CI(t)$, класифікації стану об'єкта та формування рекомендацій щодо вибору найбільш доцільних управлінських рішень.

На першому етапі здійснюється збір даних із джерел моніторингу об'єкта критичної інфраструктури, зокрема журналів подій безпеки, мережевих сенсорів, засобів моніторингу обладнання та інших інформаційних систем.

Другий етап передбачає попередню обробку даних: перевірку їх повноти, усунення аномалій, фільтрацію шумів і нормалізацію показників відповідно до формули (3). У результаті формується множина параметрів, придатних для подальшого аналізу.

На третьому етапі оцінюється поточний рівень гарантоздатності шляхом визначення показників кібербезпеки, доступності, надійності, живучості та відновлюваності з подальшим розрахунком інтегрального показника за формулою (4).

Четвертий етап полягає в оцінюванні загроз і ризиків функціонування об'єкта. На основі виявлених загроз визначаються інтегральний рівень загроз, коефіцієнт деградації та скоригований показник гарантоздатності відповідно до формул (6)–(9).

На п'ятому етапі виконується прогнозування зміни стану гарантоздатності. На основі поточних і попередніх оцінок визначаються прогнозований рівень гарантоздатності, тенденція його зміни та індекс критичності згідно з формулами (10)–(13).

Шостий етап реалізує інтелектуальну підтримку прийняття рішень. З урахуванням поточного стану, результатів прогнозування та накопичених знань формуються альтернативні управлінські рішення на основі продукційних правил бази знань і результатів аналізу даних моніторингу.

На сьомому етапі відповідно до критерію (14) обирається найбільш доцільне рішення, яке передається оператору ситуаційного центру або автоматизованій системі управління.

Заклучний етап передбачає оновлення бази знань на основі інформації про прийняті рішення, їх ефективність та фактичні зміни стану гарантоздатності.

Таким чином, алгоритм забезпечує повний цикл управління гарантоздатністю об'єкта критичної інфраструктури – від збору й аналізу даних до прогнозування стану та формування рекомендацій щодо підтримання його функціональної стійкості.



Рис. 3. Алгоритм реалізації методу оцінювання та прогнозування гарантоздатності об'єктів критичної інфраструктури

Результати моделювання та оцінювання ефективності

Для перевірки ефективності запропонованого методу було проведено моделювання процесів функціонування об'єкта критичної інфраструктури в умовах різних рівнів дестабілізуючих впливів [1, 11, 21-22]. Моделювання виконувалося для чотирьох сценаріїв, що відображають типові режими функціонування сучасних інформаційно-комунікаційних систем критичної інфраструктури. Основні параметри сформованих сценаріїв наведено в табл. 2.

Таблиця 2

Параметри сценаріїв моделювання

Сценарій	Кількість загроз	Середня імовірність загрози	Середній рівень впливу	Кількість інцидентів	Рівень навантаження системи, %
S1	3	0,12	0,15	2	35

S2	8	0,27	0,32	7	52
S3	15	0,48	0,61	14	73
S4	25	0,71	0,84	22	91

Як видно з табл. 2, кожний наступний сценарій характеризується збільшенням кількості загроз, інцидентів та навантаження на інформаційно-комунікаційну інфраструктуру, що дозволяє оцінити роботу методу в умовах поступового погіршення стану об'єкта.

На основі параметрів сценаріїв було визначено значення основних складових гарантоздатності об'єкта критичної інфраструктури, які характеризують рівень його кібербезпеки, доступності, надійності, живучості та відновлюваності. Результати оцінювання наведено в табл. 3.

Таблиця 3

Результати оцінювання складових гарантоздатності об'єкта критичної інфраструктури

Сценарій	Кібербезпека (С)	Доступність (А)	Надійність (R)	Живучість (V)	Відновлюваність (D)
S1	0,97	0,95	0,96	0,93	0,94
S2	0,89	0,87	0,86	0,84	0,85
S3	0,78	0,75	0,77	0,73	0,76
S4	0,62	0,58	0,61	0,54	0,57

Дані табл. 3 демонструють зміну основних складових гарантоздатності залежно від рівня дестабілізуючих впливів [13, 21]. Для сценарію S1 усі показники перевищують значення 0,93, що відповідає високому рівню гарантоздатності об'єкта. У сценаріях S2 та S3 спостерігається поступове зниження показників кібербезпеки, доступності, надійності, живучості та відновлюваності внаслідок збільшення кількості загроз та інцидентів. Найгірші результати отримано для сценарію S4, де значення окремих складових гарантоздатності знижуються до 0,54–0,62, що свідчить про суттєве погіршення стану об'єкта та необхідність реалізації додаткових заходів захисту.

На основі отриманих значень складових гарантоздатності було виконано розрахунок інтегрального показника гарантоздатності, скоригованого показника гарантоздатності, прогнозованого стану об'єкта та відповідного рівня ризику. Результати розрахунків наведено в табл. 4.

Таблиця 4

Результати оцінювання та прогнозування гарантоздатності

Сценарій	Інтегральний показник гарантоздатності $GI(t)$	Скоригований показник гарантоздатності $GS(t)$	Прогнозований рівень гарантоздатності $GP(t+1)$	Рівень ризику $R(t)$
S1	0,95	0,93	0,94	0,07
S2	0,88	0,82	0,80	0,18
S3	0,76	0,68	0,64	0,37
S4	0,61	0,49	0,44	0,58

Аналіз результатів табл. 4 показує, що зі зростанням рівня загроз спостерігається поступове зниження інтегрального показника гарантоздатності та збільшення рівня ризику функціонування об'єкта. Найбільше погіршення стану зафіксовано для сценарію S4, де прогнозований рівень гарантоздатності знижується до 0,44, а ризик досягає значення 0,58. Це свідчить про здатність запропонованого методу своєчасно виявляти тенденції погіршення стану системи ще до переходу об'єкта у критичний режим функціонування [11, 24].

На рис. 4 наведено залежність скоригованого показника гарантоздатності $GS(t)$ та рівня ризику $R(t)$ від сценарію функціонування об'єкта критичної інфраструктури. Аналіз отриманих результатів свідчить, що зі зростанням рівня дестабілізуючих впливів від сценарію S1 до сценарію S4 спостерігається поступове зниження показника гарантоздатності з 0,93 до 0,49 та одночасне зростання рівня ризику з 0,07 до 0,58. Найбільш суттєві зміни зафіксовано для сценаріїв S3 та S4, що характеризуються високою інтенсивністю загроз та інцидентів. Отримані результати підтверджують наявність оберненої залежності між рівнем гарантоздатності та ризиком функціонування об'єкта, а також демонструють здатність запропонованого методу своєчасно виявляти тенденції погіршення стану системи. Особливої уваги заслуговує зближення кривих у сценарії S4, що свідчить про досягнення критичного рівня ризику та необхідність реалізації додаткових заходів щодо підтримання гарантоздатності об'єкта.

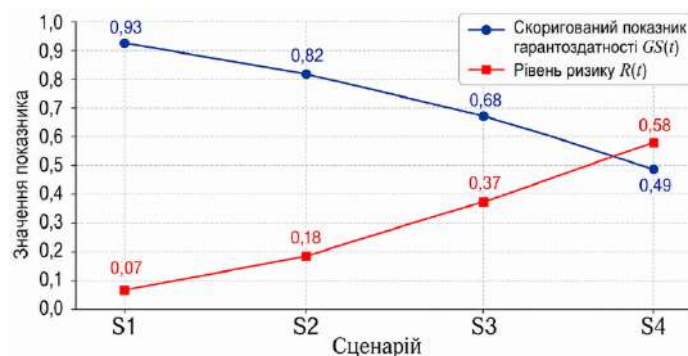


Рис. 4. Залежність інтегрального показника гарантоздатності та рівня ризику від сценарію функціонування

Для визначення переваг запропонованого методу було проведено його порівняння з існуючими підходами, що використовуються для оцінювання та прогнозування стану об'єктів критичної інфраструктури. Порівняння здійснювалося за показниками точності прогнозування, часу формування управлінських рішень, рівня зниження ризику та значення F1-міри. Отримані результати наведено в табл. 5.

Таблиця 5

Порівняння запропонованого методу з існуючими підходами

Метод	Точність прогнозування, %	Час прийняття рішення, с	Зниження ризику, %	F1-міра
Статичне оцінювання	78,3	12,6	9,4	0,76
Правилоорієнтований	84,7	9,8	17,2	0,83
Машинне навчання	89,1	8,1	23,6	0,88
Запропонований метод	92,4	6,7	28,5	0,92

Для оцінювання точності прогнозування використовувалася середня частка правильно визначених станів гарантоздатності на тестовій вибірці сценаріїв моделювання. Значення F1-міри обчислювалися за результатами класифікації станів об'єкта на нормальні, небезпечні та критичні. Результати табл. 5 демонструють переваги запропонованого методу над альтернативними підходами. Зокрема, точність прогнозування стану гарантоздатності досягає 92,4 %, що на 3,3 % перевищує результат методу машинного навчання та на 14,1 % – статичного підходу. Крім того, використання інтелектуальної технології підтримки прийняття рішень дозволило скоротити середній час формування управлінського рішення до 6,7 с, що відповідає зменшенню на 31,7 % порівняно з правилоорієнтованими системами [17, 24, 28]. Одночасно забезпечено зниження інтегрального рівня ризику на 28,5 % завдяки можливості раннього виявлення негативних тенденцій та своєчасного формування рекомендацій щодо реагування.

Узагальнюючи результати табл. 2–5, можна зробити висновок, що запропонований метод забезпечує стабільне оцінювання поточного стану гарантоздатності, своєчасне прогнозування його зміни та ефективну підтримку прийняття рішень навіть в умовах високого рівня дестабілізуючих впливів. Найбільший ефект досягається в сценаріях S3 та S4, де раннє виявлення тенденцій погіршення стану дозволяє зменшити ризик втрати гарантоздатності та скоротити час реагування на інциденти.

Для додаткового оцінювання впливу системи підтримки прийняття рішень (СППР) на оперативність реагування було проведено порівняльний аналіз часу прийняття управлінських рішень за умови використання та без використання СППР. Результати дослідження наведено в табл. 6.

Таблиця 6

Аналіз ефективності системи підтримки прийняття рішень (СППР)

Сценарій	Час реагування без СППР, с	Час реагування із СППР, с	Скорочення часу, %
S1	7.4	5.9	20.3
S2	9.8	7.0	28.6
S3	12.7	8.1	36.2
S4	16.5	10.9	33.9

Аналіз результатів табл. 6 свідчить, що використання інтелектуальної технології підтримки прийняття рішень дозволяє суттєво скоротити час реагування на інциденти в усіх досліджуваних сценаріях. Найбільший ефект досягнуто для сценарію S3, де скорочення часу реагування становить 36,2 %, що пояснюється можливістю автоматизованого аналізу поточного стану гарантоздатності та оперативного формування рекомендацій. Для критичного сценарію S4 час реагування зменшується на 33,9 %, що підтверджує доцільність використання запропонованої технології в умовах підвищеного рівня загроз та необхідності швидкого прийняття управлінських рішень.

Оскільки ключовою особливістю запропонованого методу є використання інтелектуальних технологій підтримки прийняття рішень, доцільно окремо оцінити їх вплив на результати оцінювання та прогнозування гарантоздатності об'єктів критичної інфраструктури. На відміну від табл. 6, де оцінюється лише часовий аспект реагування, у табл. 7 наведено узагальнену оцінку впливу СППР на ключові показники ефективності запропонованого методу.

Таблиця 7

Вплив інтелектуальної СППР на ефективність оцінювання та прогнозування гарантоздатності

Показник	Без СППР	Із СППР	Покращення
Точність прогнозування, %	85,6	92,4	+6,8 %
F1-міра	0,84	0,92	+9,5 %
Середній час прийняття рішення, с	9,8	6,7	-31,7 %
Зниження інтегрального ризику, %	19,3	28,5	+47,7 %
Частка своєчасно виявлених критичних станів, %	81,2	93,7	+12,5 %

Результати табл. 7 свідчать, що використання інтелектуальної системи підтримки прийняття рішень дозволяє підвищити точність прогнозування стану гарантоздатності на 6,8 %, збільшити значення F1-міри до 0,92 та скоротити середній час формування управлінських рішень на 31,7 %. Крім того, застосування СППР забезпечує більш своєчасне виявлення критичних станів об'єкта та зменшення інтегрального рівня ризику функціонування.

На рис. 5 показано вплив СППР на ключові показники ефективності запропонованого методу. Використання СППР сприяє підвищенню точності прогнозування, якості класифікації та своєчасності виявлення критичних станів, а також забезпечує скорочення часу прийняття рішень і додаткове зниження ризику функціонування об'єкта.

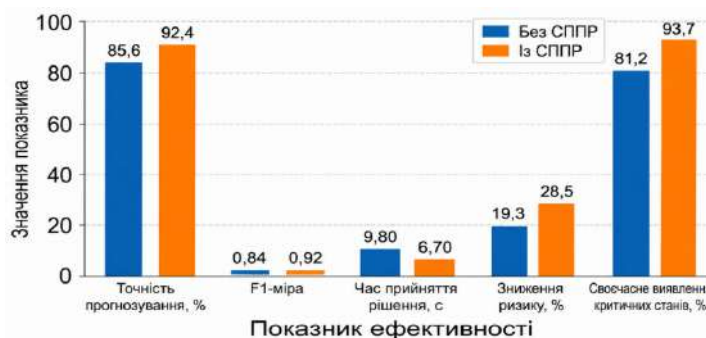


Рис. 5. Вплив СППР на ефективність оцінювання та прогнозування гарантоздатності

Отримані результати підтверджують ефективність запропонованого методу оцінювання та прогнозування гарантоздатності об'єктів критичної інфраструктури та доцільність його використання в інформаційно-аналітичних системах ситуаційних центрів і системах підтримки прийняття рішень.

Обговорення. Отримані результати підтверджують ефективність запропонованого методу в умовах різного рівня дестабілізуючих впливів. На відміну від існуючих підходів, метод поєднує інтегральне оцінювання показників гарантоздатності, прогнозування зміни стану об'єкта та інтелектуальну підтримку прийняття рішень, що забезпечує своєчасне виявлення негативних тенденцій і формування обґрунтованих рекомендацій щодо реагування [15, 22-25].

Результати моделювання показали, що зі зростанням кількості загроз та інцидентів відбувається зниження рівня гарантоздатності та збільшення ризику функціонування об'єкта. Запропонований метод забезпечує можливість раннього виявлення критичних станів ще до переходу системи до аварійного режиму функціонування. Важливу роль у цьому відіграє інтелектуальна СППР, яка використовує результати оцінювання та прогнозування для автоматизованого формування рекомендацій, підвищення точності прогнозування, скорочення часу прийняття рішень і зниження ризику [2-6, 15, 23]. Отримані результати узгоджуються з сучасними дослідженнями у сфері застосування штучного інтелекту та машинного навчання для підвищення стійкості й гарантоздатності критичної інфраструктури [7, 17, 24].

Обмеженням дослідження є використання сценарного моделювання, що не дозволяє повною мірою врахувати особливості реальних об'єктів критичної інфраструктури. Крім того, у роботі застосовано узагальнену модель машинного навчання без деталізації конкретного алгоритму, а також не враховано міжгалузеві залежності та каскадні ефекти поширення інцидентів, які є характерними для сучасних взаємопов'язаних інфраструктурних систем [1, 8, 21, 22]. Перспективним напрямом подальших досліджень є використання реальних даних моніторингу критичної інфраструктури, розширення набору факторів оцінювання гарантоздатності та застосування спеціалізованих моделей машинного навчання для підвищення точності прогнозування.

Незважаючи на зазначені обмеження, отримані результати підтверджують перспективність використання запропонованого методу в ситуаційних центрах, системах моніторингу кібербезпеки та інтелектуальних системах підтримки прийняття рішень [14, 16, 23, 25]. Запропонований підхід може бути використаний як складова інформаційно-аналітичних систем управління критичною інфраструктурою для підвищення стійкості, безперервності функціонування та обґрунтованості управлінських рішень в умовах зростання кіберзагроз і дестабілізуючих впливів.

5. Висновки та перспективи подальших досліджень

У роботі розв'язано актуальне науково-практичне завдання розроблення методу оцінювання та прогнозування стану гарантоздатності об'єктів критичної інфраструктури із застосуванням інтелектуальних технологій підтримки прийняття рішень. Запропонований метод поєднує інтегральне оцінювання показників гарантоздатності, прогнозування зміни стану об'єкта та інтелектуальну підтримку прийняття рішень. Розроблено математичну модель оцінювання гарантоздатності, удосконалено процес підтримки прийняття рішень на основі аналізу даних моніторингу та моделі машинного навчання, а також розроблено алгоритм реалізації методу, який забезпечує повний цикл оброблення даних – від моніторингу до вибору управлінських рішень.

Результати моделювання підтвердили ефективність запропонованого підходу: точність прогнозування стану гарантоздатності досягла 92,4 %, а середній час прийняття рішень скоротився на 31,7 % порівняно з традиційними підходами. Це підтверджує доцільність використання методу в ситуаційних центрах та інформаційно-аналітичних системах управління об'єктами критичної інфраструктури.

Перспективи подальших досліджень полягають в апробації запропонованого методу на реальних даних моніторингу, розширенні можливостей інтелектуальної системи підтримки прийняття рішень за рахунок сучасних алгоритмів машинного навчання та врахуванні міжгалузевих взаємозв'язків і каскадних ефектів поширення інцидентів

Декларація про штучний інтелект

Під час підготовки цієї роботи автор використовував програму штучного інтелекту Grammarly Pro для виправлення граматики тексту та систему Strike Plagiarism для пошуку можливих проявів плагиату. Після використання цих інструментів автор переглянув та відредагував зміст за потреби і несе повну відповідальність за зміст публікації.

Конфлікт інтересів

Автор заявляє про відсутність конфлікту інтересів та підтверджує, що під час підготовки цієї роботи не існувало жодних комерційних, фінансових чи інших взаємовідносин, які могли б бути розцінені як такі, що здатні вплинути на результати дослідження або їх інтерпретацію. Робота виконана відповідно до принципів академічної доброчесності, етичних норм проведення наукових досліджень та вимог редакційної політики щодо запобігання конфлікту інтересів.

Список використаних джерел

1. 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
2. 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>
3. 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>
4. Lin, X., Zhang, J., Deng, G., Liu, T., Zhang, T., Guo, Q., & Chen, R. (2025). IRCopilot: Automated incident response with large language models. arXiv. <https://arxiv.org/abs/2505.20945>
5. Liu, Z. (2024). Multi-agent collaboration in incident response with large language models. arXiv. <https://arxiv.org/abs/2412.00652>
6. 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)* (pp. 133–148). USENIX Association.
7. 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>
8. Wang, S., Gu, X., Luan, S., & Zhao, M. (2021). Resilience analysis of interdependent critical infrastructure systems considering deep learning and network theory. *International Journal of Critical Infrastructure Protection*, 35, Article 100459. <https://doi.org/10.1016/j.ijcip.2021.100459>
9. Mentges, A., Halekotte, L., Schneider, M., Demmer, T., & Lichte, D. (2023). A resilience glossary shaped by context: Reviewing resilience-related terms for critical infrastructures. *International Journal of Disaster Risk Reduction*, 96, Article 103893. <https://doi.org/10.1016/j.ijdrr.2023.103893>
10. Kostiuk, Y. V., & Skladannyi, P. M. (2026). Cryptographic trust model for security events in SIEM for intelligent network incident generation. *Modern Information Protection*, 1(65), 103–118. <https://doi.org/10.31673/2409-7292.2026.011393>
11. 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>

12. Kostiuk, Y., Rzaieva, S., & Rzaiev, D. (2026). Intelligent network traffic analysis for information security incident detection. *Science and Technology Today*, 2(56), 1909–1928. [https://doi.org/10.52058/2786-6025-2026-2\(56\)-1909-1928](https://doi.org/10.52058/2786-6025-2026-2(56)-1909-1928)
13. Lin, J.-H., & Wu, Y.-K. (2024). Review of power system resilience concept, assessment, and enhancement measures. *Applied Sciences*, 14(4), Article 1428. <https://doi.org/10.3390/app14041428>
14. Rzaeva, S., Skladannyi, P., Kostiuk, Y., Abramov, V., & Kravchenko, V. (2025). Adaptive information security management in cloud-oriented intelligent transportation systems. *Ukrainian Scientific Journal of Information Security*, 31(1), 23–36. <https://doi.org/10.18372/2225-5036.31.20634>
15. Pudney, S., Mills, D., Alaei, A. R., Sellers, S., Dvorak, J., & Potluka, O. (2025). Evaluation of artificial intelligence-enhanced critical infrastructure systems: A conceptual framework. *Evaluation*, 31(3), 412–443.
16. Kostiuk, Y., Skladannyi, P., Rzaieva, S., Samoilenko, Y., & Korshun, N. (2025). Intelligent control and protection systems in cyber-physical and cloud-based Smart Grid environments. *Cybersecurity: Education, Science, Technology*, 2(30), 125–156. <https://doi.org/10.28925/2663-4023.2025.30.956>
17. Yigit, Y., Ferrag, M. A., Sarker, I. H., Maglaras, L. A., Chrysoulas, C., Moradpoor, N., & Janicke, H. (2024). *Critical infrastructure protection: Generative AI, challenges, and opportunities*. arXiv. <https://arxiv.org/abs/2405.04874>
18. Dovzhenko, N., Ivanichenko, Y., & Kostiuk, Y. (2025). Method for detecting and localizing cyber threats in cloud environments with integrated IoT components based on graph models. *Cybersecurity: Education, Science, Technology*, 1(29), 762–776. <https://doi.org/10.28925/2663-4023.2025.29.938>
19. Woods, W., Grushin, A., Khan, S., & Velasquez, A. (2024). Combining AI control systems and human decision support via robustness and criticality. In *Disruptive Technologies in Information Sciences VIII* (Vol. 13058, pp. 172–190). SPIE.
20. Skladannyi, P., Kostiuk, Y., Rzaieva, S., Samoilenko, Y., & Savchenko, T. (2025). Development of modular neural networks for detecting various classes of network attacks. *Cybersecurity: Education, Science, Technology*, 3(27), 534–548. <https://doi.org/10.28925/2663-4023.2025.27.772>
21. Rouholamini, M., Wang, C., Magableh, S., et al. (2025). Resiliency of electric power distribution networks: A review. *Journal of Infrastructure Preservation and Resilience*, 6, Article 39. <https://doi.org/10.1186/s43065-025-00154-y>
22. 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>
23. Rzaieva, S. L., Lytvyn, O. S., Skladannyi, P. M., Kostiuk, Y. V., & Rzaiev, D. O. (2026). Adaptive cybersecurity management model 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>
24. Crichton, K., Ji, J., Miller, K., Bansemer, J., et al. (2024). *Securing critical infrastructure in the age of AI*. Center for Security and Emerging Technology. <https://doi.org/10.51593/20240032>
25. Kostiuk, Y., Skladannyi, P., & Rzaieva, S. (2026). SIEM alert quality management based on risk-oriented assessment and SOC feedback. *Ukrainian Scientific Journal of Information Security*, 31(3), 151–163. <https://doi.org/10.18372/2225-5036.31.21161>
26. Zio, E. (2025). Advances in reliability analysis and risk assessment for enhanced safety. *Journal of Reliability Science and Engineering*, 1, Article 013002. <https://doi.org/10.1088/3050-2454/adb65>
27. Kostiuk, Y., Skladannyi, P., Samoilenko, Y., Khorolska, K., Bebashko, B., & Sokolov, V. (2024). A system for assessing the interdependencies of information system agents in information security risk management using cognitive maps. In *Proceedings of the Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN'24)* (Vol. 3925, pp. 249–264). CEUR Workshop Proceedings.
28. Cummins, L., Sommers, A., Ramezani, S. B., Mittal, S., Jabour, J., Seale, M., & Rahimi, S. (2024). Explainable predictive maintenance: A survey of current methods, challenges and opportunities. *IEEE Access*, 12, 57574–57602.
29. 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)* (Vol. 3925, pp. 155–171). CEUR Workshop Proceedings.

Надійшла до редакції: 14.04.2026

Прийнята до друку: 15.09.2026

Опубліковано: 30.09.2026