DOI: https://doi.org/10.36910/6775-2524-0560-2026-64-17
УДК 004.056
Костюк Юлія Володимирівна, PhD
https://orcid.org/0000-0001-5423-0985
Складанний Павло Миколайович, к.т.н, доцент
https://orcid.org/0000-0002-7775-6039
Довженко Надія Михайлівна, к.т.н, доцент
https://orcid.org/0000-0003-4164-0066
Коршун Наталія Володимирівна, д.т.н, професор
https://orcid.org/0000-0003-2908-970X
Київський столичний університет імені Бориса Грінченка, м. Київ, Україна

ІНТЕЛЕКТУАЛЬНИЙ МЕТОД ВИБОРУ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ В РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ НА ОСНОВІ БАГАТОКРИТЕРІАЛЬНОЇ ОПТИМІЗАЦІЇ ТА ТЕОРІЇ ІГОР

Костюк Ю. В., Складанний П. М., Довженко Н. М., Коршун Н. В. Інтелектуальний метод вибору засобів захисту інформації в розподілених інформаційних системах на основі багатокритеріальної оптимізації та теорії ігор. У статті розроблено інтелектуальний метод вибору засобів захисту інформації в розподілених інформаційних системах на основі багатокритеріальної оптимізації та теорії ігор. Актуальність дослідження зумовлена зростанням кількості кіберзагроз, ускладненням архітектури розподілених систем та необхідністю адаптивного керування засобами кіберзахисту в умовах динамічного мережевого середовища. Показано, що традиційні методи вибору засобів захисту інформації орієнтовані переважно на статичні критерії оцінювання та недостатньо враховують поведінку порушника, взаємозалежність компонентів системи й ризики кіберзагроз. У роботі проведено аналіз попередніх досліджень у сфері кіберзахисту розподілених інформаційних систем, багатокритеріальної оптимізації, теорії ігор та моделей стратегічної протидії. Визначено недоліки існуючих підходів, серед яких недостатня адаптивність, неврахування невизначеності параметрів кіберсередовища та відсутність комплексного механізму вибору засобів захисту інформації. Запропонований метод базується на поєднанні математичного апарату багатокритеріальної оптимізації, ігрових моделей та оцінювання ризику кіберзагроз. У статті сформовано модель стратегічної взаємодії між системою кіберзахисту та порушником, побудовано функцію виграшу сторін і розроблено інтегральний критерій оцінювання ефективності засобів захисту інформації. Розроблено архітектуру інтелектуальної системи підтримки прийняття рішень, яка включає модулі моніторингу мережевого середовища, аналізу кіберзагроз, оцінювання ризику та формування стратегій захисту. Проведене експериментальне моделювання підтвердило ефективність запропонованого методу щодо зниження очікуваних втрат від кібератак, скорочення часу реагування на інциденти безпеки та підвищення адаптивності системи кіберзахисту. Результати підтвердили ефективність методу для захисту розподілених інформаційних систем і мереж.
Ключові слова: розподілені інформаційні системи; кіберзахист; засоби захисту інформації; інтелектуальний метод вибору; система підтримки прийняття рішень; багатокритеріальна оптимізація; теорія ігор; ігрові моделі; стратегічна протидія; оцінювання ризику; кіберзагрози.

Kostiuk Y., Skladannyi P., Dovzhenko N. Korshun N. Intelligent Method for Selecting Information Protection Means in Distributed Information Systems Based on Multi-Criteria Optimization and Game Theory. This paper presents an intelligent method for selecting information protection means in distributed information systems based on multi-criteria optimization and game theory. The relevance of the study is determined by the growing number of cyber threats, the increasing complexity of distributed system architectures, and the need for adaptive management of cybersecurity measures in dynamic network environments. It is shown that traditional approaches to selecting information protection means are primarily focused on static evaluation criteria and insufficiently consider attacker behavior, interdependencies among system components, and cybersecurity risks. The study analyzes previous research in the fields of cybersecurity for distributed information systems, multi-criteria optimization, game theory, and strategic defense models. The limitations of existing approaches are identified, including insufficient adaptability, inadequate consideration of uncertainty in cyber environment parameters, and the absence of an integrated mechanism for selecting information protection means. The proposed method is based on the integration of multi-criteria optimization techniques, game-theoretic models, and cyber risk assessment mechanisms. A strategic interaction model between the cybersecurity system and an attacker is developed, payoff functions for both parties are formulated, and an integral criterion for evaluating the effectiveness of information protection means is proposed. An architecture of an intelligent decision support system is designed, incorporating modules for network environment monitoring, cyber threat analysis, risk assessment, and protection strategy generation. Experimental modeling confirmed the effectiveness of the proposed method in reducing expected losses from cyberattacks, decreasing incident response time, and improving the adaptability of the cybersecurity system. The obtained results demonstrate the applicability and effectiveness of the proposed method for protecting distributed information systems and networks.
Keywords: distributed information systems; cybersecurity; information protection means; intelligent selection method; decision support system; multi-criteria optimization; game theory; game-theoretic models; strategic defense; risk assessment; cyber threats.

Постановка наукової проблеми. Розвиток хмарних платформ, розподілених сервісів і мережевих технологій супроводжується ускладненням архітектури розподілених інформаційних

систем, зростанням взаємозалежності їх компонентів та інтенсивності кіберзагроз [1, 8, 13]. Розподілений характер оброблення даних, гетерогенність програмно-апаратних платформ і динамічна зміна стану мережевого середовища ускладнюють забезпечення необхідного рівня захищеності. За таких умов ефективність кіберзахисту визначається не лише здатністю виявляти та блокувати загрози, а й обґрунтованістю вибору засобів захисту з урахуванням критичності ресурсів, поточного ризику, витрат, впливу на продуктивність і можливих сценаріїв атак.

Наукова проблема полягає у суперечності між необхідністю оперативного адаптивного вибору засобів захисту в умовах мінливого кіберсередовища та недостатньою здатністю існуючих підходів комплексно враховувати взаємопов'язані технічні, ризикові й стратегічні чинники такого вибору [2–3, 11, 27–28]. Переважання статичних моделей оцінювання та фіксованих правил прийняття рішень обмежує можливості адаптації захисту до зміни інтенсивності загроз, стану ресурсів і поведінки порушника. Особливої складності проблема набуває за одночасного існування кількох альтернатив захисту з різними показниками ефективності, вартості, продуктивності, часу реагування, стійкості та сумісності, коли вибір за окремим критерієм не забезпечує раціонального рішення для системи загалом.

Розв'язання цієї проблеми потребує переходу від статичного вибору окремих засобів до інтелектуального адаптивного прийняття рішень на основі спільного оцінювання кіберризику, багатокритеріальної оптимізації та моделювання стратегічної взаємодії системи кіберзахисту з порушником [1-3, 5, 6, 19]. Така інтеграція дає змогу пов'язати поточний стан системи та критичність її ресурсів із характеристиками доступних засобів захисту, можливими діями порушника й очікуваними наслідками прийнятих рішень.

Наукова новизна полягає у формуванні інтегрованого механізму стратегічного вибору засобів захисту, який поєднує ризик-орієнтоване оцінювання, багатокритеріальну оптимізацію та ігрову модель протидії й забезпечує адаптивне коригування захисту відповідно до поточного ризику, стану системи та поведінки порушника. На відміну від статичного вибору, такий підхід формує замкнений процес оцінювання стану, вибору захисної стратегії та її коригування при зміні кіберсередовища.

Теоретичне значення дослідження полягає у розвитку моделей багатокритеріального стратегічного вибору та адаптивного керування кіберзахистом розподілених інформаційних систем. Практичне значення визначається можливістю реалізації методу в інтелектуальних системах підтримки прийняття рішень для обґрунтованого вибору й адаптивного налаштування засобів захисту, зниження кіберризику та скорочення часу реагування на інциденти.

Метою статті є розробка інтелектуального методу вибору засобів захисту інформації в розподілених інформаційних системах на основі багатокритеріальної оптимізації та теорії ігор для підвищення ефективності стратегічної протидії кіберзагрозам в умовах динамічного кіберсередовища.

Для досягнення поставленої мети у роботі необхідно вирішити такі завдання:

- провести аналіз сучасних підходів до забезпечення кібербезпеки розподілених інформаційних систем та методів вибору засобів захисту в умовах динамічних кіберзагроз;
- дослідити особливості використання багатокритеріальної оптимізації та теорії ігор у задачах кіберзахисту;
- розробити модель стратегічної взаємодії між системою кіберзахисту та потенційним порушником;
- сформувати інтегральний критерій оцінювання ефективності засобів захисту інформації;
- розробити інтелектуальний метод вибору засобів захисту інформації для розподілених інформаційних систем;

провести експериментальне моделювання ефективності запропонованого методу в умовах динамічних кіберзагроз.

Аналіз останніх досліджень і публікацій. Сучасні дослідження вибору засобів захисту інформації в розподілених інформаційних системах охоплюють застосування теорії ігор, багатокритеріальної оптимізації, оцінювання ризику та інтелектуальних систем підтримки прийняття рішень. У роботах [1–3] ігрові та оптимізаційні моделі використовуються для формування стратегій кіберзахисту в умовах обмежених ресурсів, невизначеності та зміни поведінки порушника. Підходи [4, 5] орієнтовані на багатокритеріальне оцінювання, аналіз кіберризику та адаптивне формування керуючих рішень, тоді як у [6, 7] досліджено використання

методів дослідження операцій, ігрових моделей та інтелектуальних агентів для адаптивної протидії кіберзагрозам. Особливості розподілених інформаційних систем як об'єкта кіберзахисту та доцільність поєднання теорії ігор із багатокритеріальною оптимізацією розглянуто у [8].

Водночас існуючі підходи недостатньо комплексно враховують багатокритеріальний характер вибору засобів захисту, динаміку кіберсередовища, взаємозалежність компонентів розподілених систем і адаптивну поведінку порушника [11, 21, 27]. Тому недостатньо дослідженим залишається інтегрований підхід до вибору засобів захисту на основі багатокритеріальної оптимізації, оцінювання кіберризику та теорії ігор, що визначає напрям цього дослідження.

Виклад основного матеріалу й обґрунтування отриманих результатів дослідження. Для розроблення інтелектуального методу вибору засобів захисту інформації необхідно формалізувати структуру розподіленої інформаційної системи, визначити критерії оцінювання засобів кіберзахисту та побудувати модель стратегічної взаємодії між системою захисту та потенційним порушником [13, 20, 25]. Запропонований підхід базується на інтеграції методів багатокритеріальної оптимізації, оцінювання ризику кіберзагроз та теорії ігор, що дозволяє забезпечити адаптивне формування стратегій кіберзахисту в умовах динамічного кіберсередовища.

Формалізація структури розподіленої інформаційної системи. Розподілені інформаційні системи функціонують у динамічному кіберсередовищі зі змінною топологією, зростанням кількості взаємозалежних вузлів та інтенсивності кіберзагроз [21-22], що потребує оцінювання ризику, обґрунтованого вибору засобів захисту та адаптації до змін кіберсередовища.

Формально розподілену інформаційну систему подамо у вигляді множини:

$$DIS = \{N, C, S, R, T\}, \quad (1)$$

де $N = \{n_1, n_2, \dots, n_i\}$ – множина вузлів системи, $C = \{c_1, c_2, \dots, c_j\}$ – множина каналів передавання даних, $S = \{s_1, s_2, \dots, s_k\}$ – множина сервісів, $R = \{r_1, r_2, \dots, r_m\}$ – множина інформаційних ресурсів, $T = \{t_1, t_2, \dots, t_h\}$ – множина кіберзагроз. Вираз описує структуру розподіленої інформаційної системи та дозволяє визначити її основні компоненти під час побудови моделі кіберзахисту.

Кожен інформаційний ресурс характеризується інтегральним рівнем критичності:

$$Cr_i = aA_i + \beta I_i + \gamma C_i + \delta D_i, \quad (2)$$

де Cr_i – інтегральний рівень критичності ресурсу, A_i – показник важливості доступності ресурсу, I_i – показник важливості цілісності інформації, C_i – показник важливості конфіденційності, D_i – показник важливості достовірності інформації, a, β, γ, δ – вагові коефіцієнти критеріїв. Співвідношення визначає загальний рівень важливості інформаційного ресурсу для функціонування розподіленої інформаційної системи.

Для оцінювання рівня ризику використовується залежність:

$$Risk_i = P_i \cdot V_i \cdot Cr_i \cdot (1 - Sec_i), \quad (3)$$

де $Risk_i$ – рівень ризику інформаційного ресурсу, P_i – імовірність реалізації атаки, V_i – рівень уразливості ресурсу, Cr_i – рівень критичності ресурсу, Sec_i – рівень захищеності інформаційного ресурсу. Рівень ризику зростає зі збільшенням імовірності атаки, вразливості та критичності ресурсу й зменшується з підвищенням його захищеності.

Інтегральний рівень ризику розподіленої інформаційної системи визначається як:

$$Risk_{DIS} = \sum_{i=1}^{m} w_i Risk_i, \quad (4)$$

де $Risk_{DIS}$ – інтегральний ризик системи, w_i – коефіцієнт важливості інформаційного ресурсу, m – кількість інформаційних ресурсів. Рівняння дозволяє оцінити сумарний рівень небезпеки функціонування розподіленої інформаційної системи.

Багатокритеріальна модель вибору засобів захисту інформації. Вибір засобів захисту в розподілених інформаційних системах за умов обмежених ресурсів і динамічного кіберсередовища потребує врахування рівня захищеності, вартості, впливу на продуктивність, часу реагування та стійкості до кіберзагроз [11, 24].

Множину засобів захисту інформації подамо у вигляді:

$$Z = \{z_1, z_2, \dots, z_n\}, \quad (5)$$

де Z – множина засобів захисту інформації, z_i – окремий засіб захисту інформації, n – кількість доступних засобів захисту. Вираз визначає сукупність доступних механізмів кіберзахисту, серед яких виконується вибір оптимального рішення.

Для кожного засобу захисту формується вектор критеріїв оцінювання:

$$K(z_i) = (Sec_i, Cost_i, Perf_i, Resp_i, Res_i, Comp_i), \quad (6)$$

де Sec_i – рівень захищеності, який забезпечує засіб, $Cost_i$ – вартість впровадження та супроводу, $Perf_i$ – вплив на продуктивність системи, $Resp_i$ — час реагування на кіберінциденти, Res_i – стійкість до кіберзагроз, $Comp_i$ – рівень сумісності із компонентами розподіленої інформаційної системи. Співвідношення забезпечує комплексне оцінювання засобів захисту за сукупністю взаємопов'язаних критеріїв.

Інтегральну ефективність засобу захисту визначаємо за залежністю:

$$E(z_i) = \lambda_1 Sec_i - \lambda_2 Cost_i + \lambda_3 Perf_i - \lambda_4 Resp_i + \lambda_5 Res_i + \lambda_6 Comp_i,, \quad (7)$$

де $E(z_i)$ – інтегральний показник ефективності засобу захисту, $\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5, \lambda_6$ – вагові коефіцієнти критеріїв. Рівняння враховує позитивний вплив захищеності, стійкості й сумісності та негативний – вартості й часу реагування.

Оптимальний набір засобів захисту визначається як:

$$Z = \arg\max_{z_i \in Z} E(z_i), \quad (8)$$

де Z – оптимальний набір засобів захисту інформації. Умова описує задачу багатокритеріальної оптимізації, метою якої є вибір найбільш ефективного набору засобів кіберзахисту.

Загальний рівень захищеності системи оцінюємо інтегральним коефіцієнтом:

$$K_{sec} = \frac{\sum_{i=1}^{n} Sec_i w_i}{\sum_{i=1}^{n} w_i}, \quad (9)$$

де K_{sec} – інтегральний коефіцієнт захищеності системи, Sec_i – рівень захищеності, який забезпечує окремий засіб, w_i – коефіцієнт важливості засобу захисту. Вираз визначає узагальнений рівень захищеності системи з урахуванням ваг засобів кіберзахисту.

Економічну ефективність захисту оцінюємо співвідношенням ефективності та витрат:

$$K_{eff} = \frac{E(z_i)}{Cost_i}, \quad (10)$$

де K_{eff} – коефіцієнт економічної ефективності засобу захисту, $E(z_i)$ – інтегральна ефективність засобу захисту, $Cost_i$ – витрати на впровадження та супровід. Співвідношення дозволяє визначити доцільність використання засобу захисту з урахуванням його вартості та рівня ефективності.

Запропонована модель забезпечує комплексний вибір засобів захисту з урахуванням їх технічних, економічних і функціональних характеристик.

Ігрова модель стратегічної взаємодії між системою кіберзахисту та порушником. Для моделювання взаємодії системи кіберзахисту з порушником використовується ігрова модель, що враховує сценарії атак та адаптивну протидію [2, 5, 17].

Ігрову модель подамо у вигляді:

$$G = \langle D, A, UD, UA \rangle, \quad (11)$$

де D – множина стратегій системи кіберзахисту, A – множина стратегій порушника, UD – функція виграшу системи кіберзахисту, UA – функція виграшу порушника. Модель описує структуру стратегічної взаємодії між сторонами конфлікту в умовах кіберпротиборства.

Функція виграшу системи кіберзахисту визначається залежністю:

$$UD = \sum_{i=1}^{n} (E_i - L_i - C_i), \quad (12)$$

де E_i – ефективність реалізованого механізму захисту, L_i – очікувані втрати від реалізації атаки, C_i – витрати на впровадження та підтримку механізмів кіберзахисту, n – кількість реалізованих механізмів захисту. Залежність оцінює ефективність стратегії кіберзахисту з урахуванням витрат і потенційних збитків від атак.

Функція виграшу порушника визначається залежністю:

$$UA = \sum_{i=1}^{n} (G_i - P_i D_i), \quad (13)$$

де G_i – очікуваний виграш порушника від реалізації атаки, P_i – імовірність виявлення атаки, D_i – рівень складності реалізації атаки. Вираз характеризує ефективність стратегії порушника залежно від складності атаки та ймовірності її виявлення системою кіберзахисту.

Для визначення оптимальної стратегії системи використовується умова рівноваги Неша:

$$UD(d, a) \geq UD(d, a^*), \quad (14)$$

$$UA(d, a) \geq UA(d^*, a), \quad (15)$$

де d^* – оптимальна стратегія системи кіберзахисту, a^*– оптимальна стратегія порушника. Умови визначають стійкий стан системи, за якого жодна зі сторін не зацікавлена у зміні власної стратегії.

Адаптивність системи кіберзахисту оцінюємо коефіцієнтом адаптації:

$$K_{ad} = \frac{\Delta Sec}{\Delta T}, \tag{16}$$

де K_{ad} – коефіцієнт адаптивності системи, ΔSec – зміна рівня захищеності системи, ΔT – зміна рівня кіберзагроз. Співвідношення дозволяє оцінити швидкість адаптації системи кіберзахисту до зміни параметрів кіберсередовища.

Для визначення поточного рівня кіберзагроз використовується інтегральний показник:

$$T(t) = \frac{1}{N}\sum_{i=1}^{N} g_i(t)\,\mu_i(t), \tag{17}$$

де $T(t)$ – інтегральний рівень кіберзагроз, $g_i(t)$ – частота виникнення атак, $\mu_i(t)$ – коефіцієнт небезпечності атаки, N – кількість зареєстрованих кіберінцидентів. Рівняння дозволяє оцінити поточний рівень небезпеки функціонування розподіленої інформаційної системи.

Адаптивна зміна параметрів системи кіберзахисту визначається як:

$$\Delta Z(t) = \eta(T(t) - T_{crit}), \tag{18}$$

де ΔZ(t) – величина зміни параметрів захисту, η – коефіцієнт адаптації системи, T_{crit} – критичний рівень кіберзагроз. Вираз описує процес динамічного коригування параметрів системи кіберзахисту залежно від зміни інтенсивності кіберзагроз.

Поточний рівень захищеності системи визначається виразом:

$$Sec(t+1) = Sec(t) + \Delta Z(t) - \rho Risk(t), \tag{19}$$

де $Sec(t)$ – поточний рівень захищеності системи, ΔZ(t) – величина адаптивної зміни параметрів захисту, ρ – коефіцієнт деградації системи, $Risk(t)$ – поточний рівень ризику. Залежність визначає зміну захищеності системи залежно від рівня кіберзагроз і поточного ризику.

Запропонована ігрова модель враховує поведінку порушника, ефективність кіберзахисту та забезпечує адаптивне формування стратегій протидії.

Архітектура інтелектуальної системи підтримки прийняття рішень Для реалізації методу розроблено архітектуру системи підтримки прийняття рішень, що поєднує моніторинг кіберсередовища, аналіз загроз, оцінювання ризику, багатокритеріальну оптимізацію, ігровий аналіз та формування адаптивних рішень [14, 23, 26]. Вибір засобів захисту здійснюється з урахуванням ризику, критичності ресурсів, ефективності, витрат, продуктивності та поведінки порушника [19, 20, 24, 27–29].

Архітектуру системи наведено на рис. 1. На основі даних моніторингу й аналізу загроз формуються оцінки ризику, результати оптимізації та ігрового аналізу, за якими обираються засоби й стратегія захисту. Адаптивне оновлення та зворотний зв'язок забезпечують коригування захисту відповідно до змін кіберсередовища.

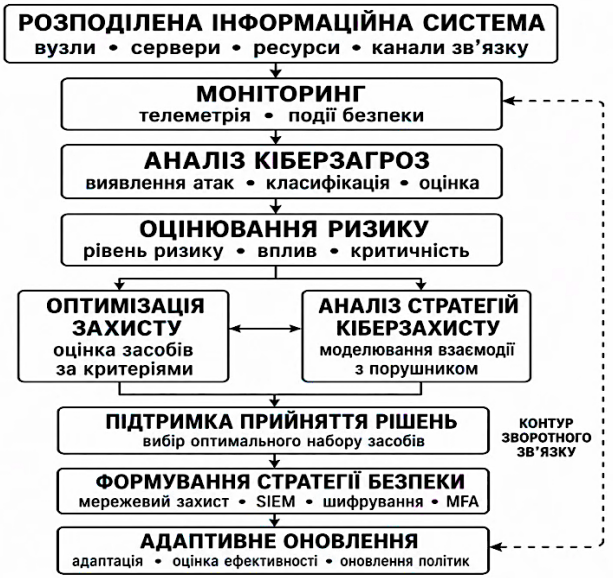

Рис. 1. Архітектура системи підтримки прийняття рішень для вибору засобів захисту інформації

Функціональний стан системи кіберзахисту визначається вектором:

$$F(t) = (Net(t), Risk(t), Sec(t), Load(t), Threat(t)), \quad (20)$$

де $Net(t)$ – стан мережевого середовища, $Risk(t)$ – поточний рівень ризику, $Sec(t)$ – рівень захищеності системи, $Load(t)$ – рівень навантаження системи, $Threat(t)$ – поточний рівень кіберзагроз. Вектор формалізує поточний стан розподіленої інформаційної системи та використовується для подальшого аналізу й прийняття рішень.

Для визначення інтегрального рівня безпеки системи використовується така залежність:

$$S_{Int}(t) = \alpha_1 Sec(t) + \alpha_2 Res(t) + \alpha_3 Stab(t) - \alpha_4 Risk(t), \quad (21)$$

де $S_{Int}(t)$ – інтегральний рівень безпеки системи, $Sec(t)$ – рівень захищеності системи, $Res(t)$ – рівень стійкості системи до атак, $Stab(t)$ – рівень стабільності функціонування системи, $Risk(t)$ – поточний рівень ризику, $\alpha_1, \alpha_2, \alpha_3, \alpha_4$– вагові коефіцієнти критеріїв. Співвідношення використовується для комплексного оцінювання рівня безпеки системи з урахуванням ризику та стійкості до кіберзагроз.

Для формування адаптивного керуючого рішення використовується вираз:

$$D(t) = \arg\max\{S_{Int}(t), E(z_i), K_{ad}(t)\}, \quad (22)$$

де $D(t)$ – керуюче рішення системи, $S_{Int}(t)$ – інтегральний рівень безпеки, $E(z_i)$ – ефективність засобу захисту, $K_{ad}(t)$ – коефіцієнт адаптивності системи. Вираз визначає оптимальне керуюче рішення на основі рівня безпеки системи, ефективності засобів захисту та показників адаптивності.

Інтелектуальність методу полягає в автоматичному формуванні та коригуванні стратегій захисту з урахуванням ризику, кіберзагроз, критичності ресурсів та результатів ігрового аналізу [18, 20, 24], що забезпечує адаптацію до змін кіберсередовища й стану системи.

Алгоритм функціонування інтелектуального методу. Метод передбачає безперервний моніторинг кіберсередовища, оцінювання ризику й критичності ресурсів та адаптивне формування стратегій кіберзахисту.

Інтенсивність потоку кіберзагроз визначається як:

$$\lambda(t) = \frac{N_{att}(t)}{\Delta t}, \quad (23)$$

де $\lambda(t)$ – інтенсивність потоку атак, $N_{att}(t)$ – кількість атак за інтервал часу, Δt – часовий інтервал спостереження. Залежність характеризує інтенсивність потоку кіберзагроз у досліджуваній системі.

Для прогнозування зміни рівня ризику використовується вираз:

$$Risk(t+1) = Risk(t) + \beta \Delta T(t) - \gamma Sec(t), \quad (24)$$

де $Risk(t+1)$ – прогнозований рівень ризику, $Risk(t)$ – поточний рівень ризику, $\Delta T(t)$ – зміна інтенсивності кіберзагроз, $Sec(t)$ – поточний рівень захищеності системи, β, γ – коефіцієнти адаптації моделі. Рівняння описує прогнозовану зміну рівня ризику залежно від динаміки кіберзагроз і поточного стану захищеності системи.

Для визначення рівня ефективності адаптивного керування використовується коефіцієнт:

$$K_{adm} = \frac{Sec_{new}}{Sec_{base}}, \quad (25)$$

де K_{adm} – коефіцієнт ефективності адаптивного керування, Sec_{new} – рівень захищеності після адаптації системи, Sec_{base} – базовий рівень захищеності системи. Коефіцієнт, визначений виразом, характеризує ефективність адаптивного оновлення параметрів системи кіберзахисту.

Алгоритм 1 інтегрує оцінювання кіберризику, багатокритеріальну оптимізацію та ігровий аналіз, а зворотний зв'язок забезпечує адаптивне коригування захисту при перевищенні допустимого ризику.

Algorithm 1. Intelligent Information Security Tool Selection Method

```
Input:
    Network environment parameters,
    cyber threat information,
    resource criticality indicators
Output:
    Optimal information protection strategy
Begin
1. Collect and preprocess network environment data;
2. Identify and assess cyber threats;
3. Calculate risk levels according to (3);
```

```
4. Generate a set of protection alternatives;
5. Perform multicriteria evaluation using (7)–(10);
6. Execute game-theoretic analysis based on (11)–(15);
7. Select the optimal information protection strategy;
8. Evaluate residual cyber risk;
9. If ResidualRisk > RiskThreshold then
       Adapt protection parameters;
       Recalculate risk level;
       Repeat evaluation procedure;
   End If
10. Generate decision recommendations;
11. Deploy the selected protection strategy;
End
```

Обчислювальна складність методу залежить від кількості ресурсів, засобів захисту та стратегій порушника й забезпечує його застосування в режимі, наближеному до реального часу.

Результати експериментального моделювання. Ефективність методу оцінено для чотирьох сценаріїв із різною інтенсивністю кіберзагроз [9]: S1 – низький рівень загроз; S2 – середній із періодичними мережевими атаками; S3 – високий з одночасними атаками на різні вузли; S4 – комбіновані мережеві, програмні та соціотехнічні атаки.

Моделювання проведено для системи з 50 вузлів, 12 сервісів і 8 типів ресурсів різної критичності [10]. Оцінювали інтегральний ризик, захищеність, час реагування, ефективність вибору засобів захисту та адаптивність системи.

Програмну реалізацію виконано на Python 3.11 із використанням NumPy, SciPy та Pandas. Для кожного сценарію проведено 100 ітерацій з усередненням результатів, наведених у табл. 1.

Таблиця 1. Порівняння результатів моделювання для різних сценаріїв

Сценарій	**Рівень ризику до впровадження**	**Рівень ризику після впровадження**	**Зниження ризику, %**	**Скорочення часу реагування, %**	K_{ad}
S1	0,31	0,22	29,0	14,5	1,08
S2	0,48	0,33	31,3	18,7	1,14
S3	0,69	0,46	33,3	21,9	1,21
S4	0,83	0,54	34,9	24,1	1,29

Коефіцієнт адаптивності K_{ad} характеризує здатність системи кіберзахисту адаптувати параметри захисту до зміни інтенсивності кіберзагроз. Зростання значення K_{ad} від 1,08 для сценарію S1 до 1,29 для сценарію S4 свідчить про підвищення ефективності адаптивного механізму керування в умовах ускладнення атак та зростання рівня кіберзагроз.

Для наочного порівняння результатів оцінювання ризику до та після застосування запропонованого методу побудовано графік зміни інтегрального рівня ризику для всіх експериментальних сценаріїв.

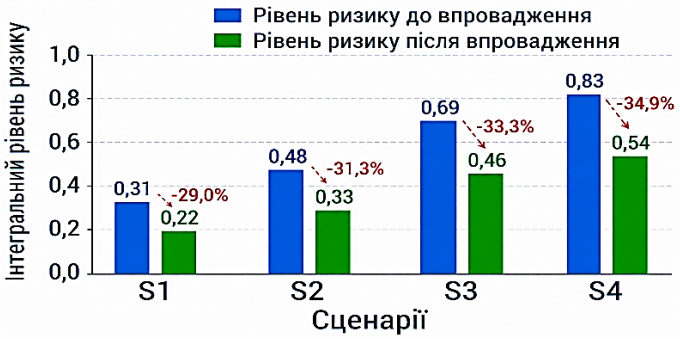

Рис. 2. Зміна інтегрального рівня ризику до та після застосування запропонованого методу для сценаріїв S1–S4

Як видно з рис. 2, зі збільшенням інтенсивності кіберзагроз ефективність запропонованого методу не знижується, що підтверджує його придатність для використання в розподілених інформаційних системах різного рівня складності. Результати підтверджують стійкість методу до

зростання інтенсивності кіберзагроз. Найбільший ефект отримано для S4: ризик знижено майже на 35 %, а час реагування − більш ніж на 24 %.

Для оцінювання практичної доцільності запропонованого підходу проведено порівняння з традиційним методом вибору засобів захисту інформації (табл. 2), який базується на статичному оцінюванні ризику та фіксованих правилах прийняття рішень.

Таблиця 2. Порівняння традиційного підходу та запропонованого методу

Показник	**Традиційний підхід**	**Запропонований метод**
Урахування рівня ризику	Часткове	Повне
Урахування поведінки порушника	Відсутнє	Наявне
Багатокритеріальна оптимізація	Відсутня	Наявна
Адаптивне оновлення параметрів захисту	Відсутнє	Наявне
Середній рівень зниження ризику	14,8 %	32,1 %
Середнє скорочення часу реагування	8,6 %	19,8 %
Підтримка стратегічного вибору засобів захисту	Відсутня	Наявна

Результати табл. 2 підтверджують перевагу запропонованого методу: середнє зниження ризику становило 32,1 % проти 14,8 %, а скорочення часу реагування − 19,8 % проти 8,6 % для традиційного підходу [11, 27]. Найбільшу ефективність отримано за високого рівня та комбінованих кіберзагроз, що підтверджує адаптивність і практичну доцільність методу.

Обговорення. Результати підтверджують ефективність поєднання оцінювання ризику, багатокритеріальної оптимізації та теорії ігор для адаптивного вибору засобів захисту [18, 24, 29, 31]. На відміну від статичних і ризик-орієнтованих підходів [11, 24, 25, 28], метод враховує стан кіберсередовища, критичність ресурсів, характеристики засобів захисту та поведінку порушника, забезпечуючи адаптацію до зміни кіберзагроз. Найбільшу ефективність отримано за високого ризику та комбінованих атак, що узгоджується з необхідністю адаптивного кіберзахисту складних мережевих середовищ [14–16].

Метод може застосовуватися в корпоративних, телекомунікаційних і хмарних розподілених системах [13, 30]. Його обмеження пов'язані з точністю оцінювання ризику й ваг критеріїв, повнотою даних та зростанням обчислювальної складності зі збільшенням кількості альтернатив [11, 28]. Загрозами валідності є спрощена модель порушника, узагальнені параметри загроз і обмежена кількість сценаріїв моделювання. Перспективним є розширення методу нейромережевими механізмами аналізу загроз та адаптивного керування захистом [18, 30–32].

Висновки та перспективи подальших досліджень. Запропонований інтелектуальний метод формує єдиний адаптивний механізм вибору засобів захисту інформації, у якому оцінювання кіберризику, багатокритеріальна оптимізація та ігрова модель стратегічної взаємодії використовуються спільно для прийняття рішень у динамічному кіберсередовищі. На відміну від статичних підходів, метод враховує критичність ресурсів, характеристики засобів захисту, зміну інтенсивності загроз і можливі стратегії порушника. Експериментальне моделювання підтвердило результативність запропонованого підходу: для сценаріїв S1–S4 зниження інтегрального ризику становило 29,0–34,9 %, а скорочення часу реагування − 14,5–24,1 %. У середньому метод забезпечив зниження ризику на 32,1 % проти 14,8 % та скорочення часу реагування на 19,8 % проти 8,6 % для традиційного підходу. Найбільший ефект досягнуто за високої інтенсивності та комбінованого характеру кіберзагроз, що підтверджує стійкість адаптивного механізму.

Наукова новизна полягає у формалізації інтегрованого механізму стратегічного вибору й адаптивного коригування засобів кіберзахисту залежно від поточного ризику та стану системи. Подальші дослідження доцільно спрямувати на прогнозування кіберзагроз методами машинного навчання, розвиток багатоагентної взаємодії та апробацію методу в реальних розподілених інформаційних системах.

Список бібліографічного опису

1. Abdallah M. et al. Game theory in distributed systems security: Foundations, challenges, and future directions. *IEEE Security & Privacy*. 2025. Vol. 23, No. 1. P. 64–74. DOI: https://doi.org/10.1109/MSEC.2024.3407593.
2. Collins B. C., Xu S., Brown P. N. Game-theoretic cybersecurity: The good, the bad and the ugly. *arXiv*. 2024. URL: https://arxiv.org/abs/2401.13815.

3. Gorbachuk V., Golotsukov G., Dunaievskyi M., Syrku A., Suleimanov S.-B. Game theory and optimization models and methods to increase security of cyberinfrastructures. *Problems of Control and Informatics*. 2023. Vol. 67, No. 2. P. 92–105. DOI: https://doi.org/10.34229/2786-6505-2022-2-6.
4. Nehodenko O. V., Shevchenko S. M., Nehodenko V. P., Zhdanova Yu. D. Model of an intelligent decision support system for ensuring cyber resilience of military information systems. *Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems*. 2025. Vol. 4145. P. 307–316.
5. Yang Y.-T., Zhu Q. Game-theoretic foundations for cyber resilience against deceptive information attacks in intelligent transportation systems. *arXiv*. 2024. DOI: https://doi.org/10.48550/arXiv.2412.04627.
6. Tanak K. S. Game theory applications in cybersecurity: An operations research approach. *Journal of Al-Qadisiyah for Computer Science and Mathematics*. 2025. Vol. 17, No. 2. P. 96–109. DOI: https://doi.org/10.29304/jqcsm.2025.17.22213.
7. Witt C. Open challenges in multi-agent security: Towards secure systems of interacting AI agents. *arXiv*. 2025. DOI: https://doi.org/10.48550/arXiv.2505.02077.
8. Yaskevych Yu. Distributed information systems as an object of cyber protection and threats to their security. 2026. No. 1. P. 120–129. DOI: https://doi.org/10.31673/2412-4338.2026.019012.
9. Lande D. V., Novikov O. M., Stopochkina I. V. Reference functions of cyber incidents displaying in the media space. *Theoretical and Applied Cybersecurity*. 2021. Vol. 3, No. 1. P. 64–74. DOI: https://doi.org/10.20535/tacs.2664-29132021.1.251315.
10. Kostiuk Y., Skladannyi P., Sokolov V., Rzaieva S., Khorolska K. Machine learning methods for detecting intrusions based on network traffic analysis. *Proceedings of the Cybersecurity Providing in Information and Telecommunication Systems II (CPITS-II 2025)*. Kyiv, Ukraine, 26 October 2025. Vol. 4145. P. 72–94. ISSN 1613-0073.
11. Bouramdane A. A. Cyberattacks in smart grids: Challenges and solving the multi-criteria decision-making for cybersecurity options, including ones that incorporate artificial intelligence, using an analytical hierarchy process. *Journal of Cybersecurity and Privacy*. 2023. Vol. 3, No. 4. P. 662–705.
12. Kostiuk Y., Skladannyi P., Sokolov V., Rzaieva S. Intelligent System for Simulation Modeling and Research of Information Objects. *Proceedings of the 1st Workshop Software Engineering and Semantic Technologies (SEST 2025)*, co-located with the 15th International Scientific and Practical Programming Conference (UkrPROG 2025). Kyiv, Ukraine, 13–14 May 2025. Vol. 4053. P. 237–251. ISSN 1613-0073. URL: https://ceur-ws.org/Vol-4053/paper15.pdf.
13. Dodonov O. H., Nykyforov O. V., Putiatin V. H., Dodonov V. O., Kutsenko S. A., Hermaniuk A. P. Territorial-distributed information computer systems in a unified information space: Basic concepts and definitions. *Data Registration, Storage and Processing*. 2024. Vol. 26, No. 1. P. 89–112.
14. Kostiuk Y., Bebeshko B., Kotenko N., Mazur N., Khorolska K., Zhyrova T. Methods for assessing the effectiveness of information security systems in distributed information systems. *International Journal of Electronics and Telecommunications*. 2026. Vol. 72. P. 1–10. ISSN 2081-8491.
15. Cunningham J. D., Aved A., Ferris D., Morrone P., Tucker C. S. A deep learning game theoretic model for defending against large scale smart grid attacks. *IEEE Transactions on Smart Grid*. 2022. Vol. 14, No. 2. P. 1188–1197.
16. Kostiuk Y. Multi-Agent System for Detecting and Counteracting Attacks on the Enterprise Information System. In: *Insider Threats and Security in Corporations*. 2025. P. 205–232. DOI: https://doi.org/10.36690/ITSC-205-232.
17. Gan C., Lin J., Huang D. W., Zhu Q., Tian L., Jain D. K. Equipment classification based differential game method for advanced persistent threats in industrial Internet of Things. *Expert Systems with Applications*. 2024. Vol. 236. Art. 121255.
18. Kostiuk Y., Skladannyi P., Sokolov V., Vorokhob M. Models and technologies of cognitive agents for decision-making with integration of Artificial Intelligence. *Proceedings of the Modern Data Science Technologies Doctoral Consortium (MoDaST 2025)*. Aachen : CEUR, 2025. Vol. 4005. P. 82–96. ISSN 1613-0073.
19. Huang L., Zhu Q. A dynamic games approach to proactive defense strategies against advanced persistent threats in cyber-physical systems. *Computers & Security*. 2020. Vol. 89. Art. 101660.
20. Rzaeva S., Skladannyi P., Kostiuk Y., Abramov V., Kravchenko V. Adaptive information security management in cloud-oriented intelligent transportation systems. *Ukrainian Scientific Journal of Information Security*. 2025. Vol. 31, No. 1. P. 23–36. DOI: https://doi.org/10.18372/2225-5036.31.20634.
21. Heryak Y., Berko A. A system of criteria for assessing data quality in distributed information systems. *Information Systems and Networks*. 2024. No. 16. P. 191–202.
22. Romaniv R. S., Bandurka O. I. Methods for ensuring the functional stability of distributed information systems for monitoring vehicle movement using blockchain technology. In: *Information Technologies and Automation 2024*. 2024. P. 221.
23. Kostiuk Y., Skladannyi P., Samoilenko Y., Khorolska K., Bebeshko B., Sokolov V. A system for assessing the interdependencies of information system agents in information security risk management using cognitive maps. *Proceedings of the Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN'24)*. 2024. Vol. 3925. P. 249–264.
24. Yaskevych Y. Game-theoretic optimization model for selecting protection means for distributed information systems. *Cybersecurity: Education, Science, Technique*. 2025. Vol. 2, No. 30. P. 715–726. DOI: https://doi.org/10.28925/2663-4023.2025.30.913.
25. He W., Tan J., Guo Y., Shang K., Zhang H. A deep reinforcement learning-based deception asset selection algorithm in differential games. *IEEE Transactions on Information Forensics and Security*. 2024. DOI: https://doi.org/10.1109/TIFS.2024.3451189.
26. Kostiuk Y., Skladannyi P., Sokolov V., Hulak H., Korshun N. Models and algorithms for analyzing information risks during the security audit of personal data information system. *CH&CMiGIN'24*. 2024. Vol. 3925. P. 155–171.

27. Zhang Y., Malacaria P. Dealing with uncertainty in cybersecurity decision support. *Computers & Security*. 2024. Vol. 148. Art. 104153. DOI: https://doi.org/10.1016/j.cose.2024.104153.
28. Šijan A., Viduka D., Ilić L., Predić B., Karabašević D. Modeling cybersecurity risk: The integration of decision theory and pivot pairwise relative criteria importance assessment with scale for cybersecurity threat evaluation. *Electronics*. 2024. Vol. 13, No. 21. Art. 4209. DOI: https://doi.org/10.3390/electronics13214209.
29. Bhol S. G. Applications of multi criteria decision making methods in cyber security. In: Choudhury A., Kaushik K., Kumar V., Singh B. K. (eds.). *Cyber-Physical Systems Security*. Studies in Big Data. Vol. 154. Springer, 2025. DOI: https://doi.org/10.1007/978-981-97-5734-3_11.
30. Fischer M., Garcia-Alfaro J., Kesdogan D., Mann Z. Secure Communication Networks and Distributed Systems for a Resilient Society (TC 11 Briefing Paper). *Computers & Security*. 2025. Vol. 162. Art. 104791. DOI: https://doi.org/10.1016/j.cose.2025.104791.
31. Labu M. R., Ahammed M. F. Next-generation cyber threat detection and mitigation strategies: A focus on artificial intelligence and machine learning. *Journal of Computer Science and Technology Studies*. 2024. Vol. 6, No. 1. P. 179–188.
32. Yadav I., Shekhawat V., Gautam K., Soni G. K., Yadav R. Artificial Intelligence for Cybersecurity: Emerging Techniques, Challenges, and Future Trends. In: *2025 3rd International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*. IEEE, 2025. P. 1176–1180.

References

1. Abdallah M. et al. Game theory in distributed systems security: Foundations, challenges, and future directions. *IEEE Security & Privacy*. 2025. Vol. 23, No. 1. P. 64–74. DOI: https://doi.org/10.1109/MSEC.2024.3407593.
2. Collins B. C., Xu S., Brown P. N. Game-theoretic cybersecurity: The good, the bad and the ugly. *arXiv*. 2024. URL: https://arxiv.org/abs/2401.13815.
3. Gorbachuk V., Golotsukov G., Dunaievskyi M., Syrku A., Suleimanov S.-B. Game theory and optimization models and methods to increase security of cyberinfrastructures. *Problems of Control and Informatics*. 2023. Vol. 67, No. 2. P. 92–105. DOI: https://doi.org/10.34229/2786-6505-2022-2-6.
4. Nehodenko O. V., Shevchenko S. M., Nehodenko V. P., Zhdanova Yu. D. Model of an intelligent decision support system for ensuring cyber resilience of military information systems. *Proceedings of the Workshop on Cybersecurity Providing in Information and Telecommunication Systems*. 2025. Vol. 4145. P. 307–316.
5. Yang Y.-T., Zhu Q. Game-theoretic foundations for cyber resilience against deceptive information attacks in intelligent transportation systems. *arXiv*. 2024. DOI: https://doi.org/10.48550/arXiv.2412.04627.
6. Tanak K. S. Game theory applications in cybersecurity: An operations research approach. *Journal of Al-Qadisiyah for Computer Science and Mathematics*. 2025. Vol. 17, No. 2. P. 96–109. DOI: https://doi.org/10.29304/jqcsm.2025.17.22213.
7. Witt C. Open challenges in multi-agent security: Towards secure systems of interacting AI agents. *arXiv*. 2025. DOI: https://doi.org/10.48550/arXiv.2505.02077.
8. Yaskevych Yu. Distributed information systems as an object of cyber protection and threats to their security. 2026. No. 1. P. 120–129. DOI: https://doi.org/10.31673/2412-4338.2026.019012.
9. Lande D. V., Novikov O. M., Stopochkina I. V. Reference functions of cyber incidents displaying in the media space. *Theoretical and Applied Cybersecurity*. 2021. Vol. 3, No. 1. P. 64–74. DOI: https://doi.org/10.20535/tacs.2664-29132021.1.251315.
10. Kostiuk Y., Skladannyi P., Sokolov V., Rzaieva S., Khorolska K. Machine learning methods for detecting intrusions based on network traffic analysis. *Proceedings of the Cybersecurity Providing in Information and Telecommunication Systems II (CPITS-II 2025)*. Kyiv, Ukraine, 26 October 2025. Vol. 4145. P. 72–94. ISSN 1613-0073.
11. Bouramdane A. A. Cyberattacks in smart grids: Challenges and solving the multi-criteria decision-making for cybersecurity options, including ones that incorporate artificial intelligence, using an analytical hierarchy process. *Journal of Cybersecurity and Privacy*. 2023. Vol. 3, No. 4. P. 662–705.
12. Kostiuk Y., Skladannyi P., Sokolov V., Rzaieva S. Intelligent System for Simulation Modeling and Research of Information Objects. *Proceedings of the 1st Workshop Software Engineering and Semantic Technologies (SEST 2025)*, co-located with the 15th International Scientific and Practical Programming Conference (UkrPROG 2025). Kyiv, Ukraine, 13–14 May 2025. Vol. 4053. P. 237–251. ISSN 1613-0073. URL: https://ceur-ws.org/Vol-4053/paper15.pdf.
13. Dodonov O. H., Nykyforov O. V., Putiatin V. H., Dodonov V. O., Kutsenko S. A., Hermaniuk A. P. Territorial-distributed information computer systems in a unified information space: Basic concepts and definitions. *Data Registration, Storage and Processing*. 2024. Vol. 26, No. 1. P. 89–112.
14. Kostiuk Y., Bebeshko B., Kotenko N., Mazur N., Khorolska K., Zhyrova T. Methods for assessing the effectiveness of information security systems in distributed information systems. *International Journal of Electronics and Telecommunications*. 2026. Vol. 72. P. 1–10. ISSN 2081-8491.
15. Cunningham J. D., Aved A., Ferris D., Morrone P., Tucker C. S. A deep learning game theoretic model for defending against large scale smart grid attacks. *IEEE Transactions on Smart Grid*. 2022. Vol. 14, No. 2. P. 1188–1197.
16. Kostiuk Y. Multi-Agent System for Detecting and Counteracting Attacks on the Enterprise Information System. In: *Insider Threats and Security in Corporations*. 2025. P. 205–232. DOI: https://doi.org/10.36690/ITSC-205-232.
17. Gan C., Lin J., Huang D. W., Zhu Q., Tian L., Jain D. K. Equipment classification based differential game method for advanced persistent threats in industrial Internet of Things. *Expert Systems with Applications*. 2024. Vol. 236. Art. 121255.
18. Kostiuk Y., Skladannyi P., Sokolov V., Vorokhob M. Models and technologies of cognitive agents for decision-making with integration of Artificial Intelligence. *Proceedings of the Modern Data Science Technologies Doctoral Consortium (MoDaST 2025)*. Aachen : CEUR, 2025. Vol. 4005. P. 82–96. ISSN 1613-0073.

19. Huang L., Zhu Q. A dynamic games approach to proactive defense strategies against advanced persistent threats in cyber-physical systems. *Computers & Security*. 2020. Vol. 89. Art. 101660.
20. Rzaeva S., Skladannyi P., Kostiuk Y., Abramov V., Kravchenko V. Adaptive information security management in cloud-oriented intelligent transportation systems. *Ukrainian Scientific Journal of Information Security*. 2025. Vol. 31, No. 1. P. 23–36. DOI: https://doi.org/10.18372/2225-5036.31.20634.
21. Heryak Y., Berko A. A system of criteria for assessing data quality in distributed information systems. *Information Systems and Networks*. 2024. No. 16. P. 191–202.
22. Romaniv R. S., Bandurka O. I. Methods for ensuring the functional stability of distributed information systems for monitoring vehicle movement using blockchain technology. In: *Information Technologies and Automation 2024*. 2024. P. 221.
23. Kostiuk Y., Skladannyi P., Samoilenko Y., Khorolska K., Bebeshko B., Sokolov V. A system for assessing the interdependencies of information system agents in information security risk management using cognitive maps. *Proceedings of the Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN'24)*. 2024. Vol. 3925. P. 249–264.
24. Yaskevych Y. Game-theoretic optimization model for selecting protection means for distributed information systems. *Cybersecurity: Education, Science, Technique*. 2025. Vol. 2, No. 30. P. 715–726. DOI: https://doi.org/10.28925/2663-4023.2025.30.913.
25. He W., Tan J., Guo Y., Shang K., Zhang H. A deep reinforcement learning-based deception asset selection algorithm in differential games. *IEEE Transactions on Information Forensics and Security*. 2024. DOI: https://doi.org/10.1109/TIFS.2024.3451189.
26. Kostiuk Y., Skladannyi P., Sokolov V., Hulak H., Korshun N. Models and algorithms for analyzing information risks during the security audit of personal data information system. *CH&CMiGIN'24*. 2024. Vol. 3925. P. 155–171.
27. Zhang Y., Malacaria P. Dealing with uncertainty in cybersecurity decision support. *Computers & Security*. 2024. Vol. 148. Art. 104153. DOI: https://doi.org/10.1016/j.cose.2024.104153.
28. Šijan A., Viduka D., Ilić L., Predić B., Karabašević D. Modeling cybersecurity risk: The integration of decision theory and pivot pairwise relative criteria importance assessment with scale for cybersecurity threat evaluation. *Electronics*. 2024. Vol. 13, No. 21. Art. 4209. DOI: https://doi.org/10.3390/electronics13214209.
29. Bhol S. G. Applications of multi criteria decision making methods in cyber security. In: Choudhury A., Kaushik K., Kumar V., Singh B. K. (eds.). *Cyber-Physical Systems Security*. Studies in Big Data. Vol. 154. Springer, 2025. DOI: https://doi.org/10.1007/978-981-97-5734-3_11.
30. Fischer M., Garcia-Alfaro J., Kesdogan D., Mann Z. Secure Communication Networks and Distributed Systems for a Resilient Society (TC 11 Briefing Paper). *Computers & Security*. 2025. Vol. 162. Art. 104791. DOI: https://doi.org/10.1016/j.cose.2025.104791.
31. Labu M. R., Ahammed M. F. Next-generation cyber threat detection and mitigation strategies: A focus on artificial intelligence and machine learning. *Journal of Computer Science and Technology Studies*. 2024. Vol. 6, No. 1. P. 179–188.
32. Yadav I., Shekhawat V., Gautam K., Soni G. K., Yadav R. Artificial Intelligence for Cybersecurity: Emerging Techniques, Challenges, and Future Trends. In: *2025 3rd International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*. IEEE, 2025. P. 1176–1180.

Історія статті:
Отримано: 21.05.2026 Доопрацьовано: 11.08.2026 Прийнято до друку: 23.09.2026 Опубліковано: 29.09.2026