DOI: 10.58254/viti.9.2026.27.349

УДК 004.056.5

д-р філософії, доцент Фесьоха Н. О. ORCID: 0000-0002-9797-5589 (ВІТІ ім. Героїв Крут)
канд. техн. наук, доцент Симоненко О. А. ORCID: 0000-0001-8511-2017 (ВІТІ ім. Героїв Крут)
д-р філософії Нестеров О. М. ORCID: 0000-0001-5092-6205 (ВІТІ ім. Героїв Крут)

БАГАТОКРИТЕРІАЛЬНА МЕТОДИКА ОЦІНЮВАННЯ ЗАХИЩЕНОСТІ IoT-ПРИСТРОЇВ НА ОСНОВІ СИНТЕЗУ МЕТОДІВ AHP ТА TOPSIS

Стрімке зростання кількості підключених пристроїв Інтернету речей формує нові виклики у сфері кібербезпеки: відсутність уніфікованого інструментарію кількісного оцінювання захищеності IoT-пристроїв ускладнює прийняття обґрунтованих рішень під час їх проєктування, закупівлі, інтеграції та аудиту. У статті запропоновано теоретико-методичні засади багатокритеріальної методики оцінювання рівня захищеності IoT-пристроїв, що ґрунтується на гібридному синтезі методу аналітичного ієрархічного процесу та методу ранжування альтернатив за схожістю до ідеального рішення. Методика охоплює п’ять послідовних етапів: формування ієрархічної системи критеріїв безпеки на підставі вимог міжнародних стандартів ETSI EN 303 645 v3.1.3 та NIST IR 8425; попарне порівняння критеріїв за шкалою Сааті з перевіркою узгодженості суджень (CR ≤ 0,10); нормалізацію матриці оцінок пристроїв; розрахунок зваженої нормалізованої матриці та інтегрального індексу захищеності методом TOPSIS; формування шкали інтерпретації результатів і рекомендацій. Система критеріїв включає сім вимірюваних показників, об’єднаних у чотири функціональні групи: автентифікація, захищена комунікація, управління оновленнями та захист даних. Кожен критерій прив’язано до конкретної вимоги стандарту ETSI EN 303 645 та NIST IR 8425, що забезпечує нормативну обґрунтованість методики. Повний математичний апарат методу – від формування матриці попарних порівнянь і розрахунку вектора пріоритетів до обчислення евклідових відстаней і коефіцієнта відносної близькості – викладено у вигляді покрокового алгоритму з відповідними формулами. Запропонована методика є практичним інструментом для задач безпекового аудиту, проєктування захищених IoT-систем та підтримки прийняття рішень при виборі IoT-пристроїв.

Ключові слова: *Інтернет речей, безпека IoT, багатокритеріальне оцінювання, MCDM, AHP, TOPSIS, аналітичний ієрархічний процес, критерії захищеності, ETSI EN 303 645, NIST IR 8425, кібербезпека.*

N. Fesokha, O. Symonenko, O. Nesterov. Multi-criteria method for evaluating IoT device security based on the integration of AHP and TOPSIS methods

The rapid growth in the number of connected Internet of Things devices creates new challenges in the field of cybersecurity: the lack of a unified quantitative assessment framework for IoT device security complicates informed decision-making during their design, procurement, integration, and auditing. This paper proposes the theoretical and methodological foundations of a multi-criteria approach for evaluating the security level of IoT devices based on a hybrid integration of the Analytic Hierarchy Process and the Technique for Order Preference by Similarity to Ideal Solution.

The proposed methodology consists of five sequential stages: (1) formation of a hierarchical system of security criteria based on the requirements of international standards ETSI EN 303 645 v3.1.3 and NIST IR 8425; (2) pairwise comparison of criteria using the Saaty scale with consistency verification ($R \leq 0.10$)*; (3) normalization of the device evaluation matrix; (4) construction of the weighted normalized matrix and calculation of the integrated security index using TOPSIS; and (5) development of an interpretation scale with corresponding recommendations.*

The system of criteria includes seven measurable indicators grouped into four functional categories: authentication, secure communication, update management, and data protection. Each criterion is explicitly mapped to specific requirements of ETSI EN 303 645 and NIST IR 8425, ensuring the regulatory relevance of the methodology.

The complete mathematical framework – from pairwise comparison matrix construction and priority vector calculation to Euclidean distance computation and closeness coefficient estimation – is presented as a step-by-step algorithm with corresponding formulas. The proposed methodology serves as a practical tool for security auditing, secure IoT system design, and formalized decision support in the field of IoT cybersecurity.

Keywords: *Internet of Things; IoT security; multi-criteria decision-making, MCDM, AHP, TOPSIS, analytic hierarchy process, security criteria, ETSI EN 303 645, NIST IR 8425, cybersecurity.*

Постановка проблеми. Поняття “Інтернет речей” (Internet of Things, IoT), введене в науковий обіг Кевіном Ештоном у 1999 році, сьогодні описує глобальну екосистему фізичних об’єктів, оснащених датчиками, вбудованими обчислювальними модулями та засобами бездротової комунікації. За прогнозами аналітиків IoT Analytics, до 2030 року

загальна кількість підключених IoT-пристроїв у світі перевищить 29 мільярдів одиниць [1]. Такий масштаб розгортань формує принципово нову поверхню кіберзагроз: кожен підключений пристрій є потенційним вектором проникнення до корпоративних і домашніх мереж, джерелом витоку персональних даних або вузлом ботнет-інфраструктури.

Проблематика захищеності IoT визнана пріоритетною у міжнародній нормативній базі. У 2020 році Європейський інститут телекомунікаційних стандартів (ETSI) опублікував стандарт EN 303 645 “Кібербезпека для споживчих IoT-пристроїв”, оновлений у вересні 2024 року до версії 3.1.3 [2]. Паралельно у 2022 році Національний інститут стандартів і технологій США (NIST) опублікував NIST IR 8425 – профіль базових вимог кіберзахисту для споживчих IoT-продуктів [3]. На рівні Європейського Союзу з 2024 року набув чинності Акт про кіберстійкість (Cyber Resilience Act), що закріпив обов’язкові вимоги безпеки для підключених пристроїв на ринку ЄС [8]. Перераховані документи визначають вимоги до безпеки IoT-пристроїв, однак не містять уніфікованого кількісного інструментарію для порівняльного оцінювання конкретних пристроїв на відповідність цим вимогам.

Незважаючи на наявність міжнародних стандартів і нормативних вимог до безпеки IoT-пристроїв, на сьогодні відсутній уніфікований кількісний інструментарій, що дозволяє здійснювати їх порівняльне оцінювання за рівнем кіберзахищеності. Це ускладнює обґрунтований вибір пристроїв під час їх закупівлі, знижує об’єктивність результатів аудиту безпеки та обмежує застосування формалізованих методів прийняття рішень у сфері IoT. Таким чином, актуальною науковою проблемою є розроблення підходу до кількісного оцінювання рівня захищеності IoT-пристроїв.

Аналіз останніх досліджень та публікацій. Методи багатокритеріального прийняття рішень (MCDM) є апробованим математичним апаратом для вирішення задач комплексного оцінювання за множиною конкуруючих критеріїв. Гібридний підхід AHP-TOPSIS, що поєднує метод аналітичного ієрархічного процесу [9] і метод ранжування за схожістю до ідеального рішення [10], широко застосовується в задачах оцінювання безпеки інформаційних систем, вибору постачальників та управління ризиками [5–7]. Застосування цього апарату до задачі оцінювання захищеності IoT-пристроїв є науково обґрунтованим і перспективним напрямом дослідження.

Проблематика оцінювання захищеності IoT-систем досліджується у кількох взаємопов’язаних науково-прикладних напрямах, що охоплюють класифікацію вразливостей і загроз, розробку захисних архітектур, стандартизацію вимог безпеки та методи кількісного аналізу захищеності.

У сучасній науковій літературі виокремлюються три основних підходи до оцінювання захищеності IoT-пристроїв.

Перший підхід – якісний аудит на основі контрольних списків (checklist-based approach). Цей підхід базується на зіставленні характеристик пристрою з переліком вимог стандарту. Стандарт ETSI EN 303 645 v3.1.3 містить 33 обов’язкові та 35 рекомендованих вимог, згрупованих у 13 тематичних категорій [2]. OWASP IoT Security Testing Guide (версія 1.0, 2024) пропонує деталізований перелік тест-кейсів для практичного тестування на проникнення IoT-пристроїв [12]. Перевагою підходу є простота реалізації та прямий зв’язок з нормативними вимогами. Ключовим недоліком є відсутність агрегованого кількісного результату, що унеможливлює порівняльний аналіз кількох пристроїв та обмежує застосовність підходу до задач ранжування альтернатив.

Другий підхід – ризик-орієнтовані моделі. У роботі [4] запропоновано таксономію ризиків безпеки в IoT-середовищах, де виокремлено шість ключових складових ризику: апаратне забезпечення, мережева інфраструктура, операційні системи, програмне забезпечення, дані та людський фактор. Дослідники підкреслюють, що традиційні мережецентричні моделі безпеки є недостатніми для гетерогенних IoT-розгортань і пропонують перехід до активоцентричних підходів, де кожен фізичний пристрій

розглядається як самостійна одиниця оцінювання ризику. Хоча цей підхід враховує ширший спектр векторів загроз, результати оцінювання часто залишаються якісними, що ускладнює об'єктивне порівняння пристроїв.

Третій підхід – методи багатокритеріального прийняття рішень (MCDM). Систематичний огляд [6] засвідчує, що методи AHP, TOPSIS, SAW, VIKOR і COPRAS активно застосовуються в IoT-контексті для задач вибору та оцінювання. Зокрема, у роботі [5] запропоновано фреймворк ISA (Identified Security Attributes) для оцінювання безпеки пристроїв Інтернету медичних речей (IoMT), де AHP використовується для визначення вагових коефіцієнтів критеріїв безпеки, а TOPSIS – для ранжування альтернативних рішень. Авторами доведено, що двофазний підхід AHP-TOPSIS забезпечує вищу об'єктивність та відтворюваність оцінки порівняно з монокритеріальними підходами. У роботі [7] аналогічний підхід застосовано до оцінювання медичних IoT-пристроїв із використанням нечіткого AHP для моделювання лінгвістичної невизначеності в судженнях експертів.

Аналіз наукових праць дозволяє ідентифікувати кілька ключових прогалин у наявних дослідженнях. По-перше, більшість підходів MCDM орієнтована на вузькоспеціалізовані застосування (медичні пристрої, промислові системи) і не є узагальнено застосовними до широкого класу споживчих IoT-пристроїв. По-друге, наявні підходи, як правило, не прив'язані до актуальних міжнародних стандартів безпеки IoT (ETSI EN 303 645, NIST IR 8425), що обмежує їхню нормативну релевантність. По-третє, у жодній з розглянутих праць не запропоновано інтегровану шкалу інтерпретації значень індексу захищеності з рекомендованими діями для кожного рівня.

Наукове завдання полягає у розробленні та формалізації універсального кількісного підходу до оцінювання рівня захищеності IoT-пристроїв на основі інтеграції методів багатокритеріального прийняття рішень, який забезпечує одночасне врахування пріоритетності критеріїв безпеки, їхньої нормативної відповідності міжнародним стандартам та можливість об'єктивного порівняльного ранжування альтернатив.

Запропонована у цій статті методика дозволить усунути зазначені прогалини через розробку узагальненого, нормативно обґрунтованого підходу для широкого класу споживчих IoT-пристроїв із повним математичним апаратом та шкалою інтерпретації результатів.

Метою дослідження є розробка багатокритеріальної методики оцінювання захищеності IoT-пристроїв на основі синтезу методів AHP та TOPSIS, узгодженої з вимогами стандартів ETSI EN 303 645 v3.1.3 та NIST IR 8425, що дозволяє отримати кількісний відтворюваний рейтинг захищеності будь-якого споживчого IoT-пристрою.

Виклад основного матеріалу дослідження. Запропонована методика оцінювання захищеності IoT-пристроїв є п'ятиетапною ітеративною процедурою, що поєднує нормативно-орієнтований підхід до формування критеріїв та математично обґрунтований апарат MCDM для агрегованого оцінювання. Загальну архітектуру методики зображено у вигляді блок-схеми (рис. 1).

Методику побудовано з дотриманням таких принципів:

нормативна обґрунтованість – кожен критерій прив'язано до конкретної вимоги визнаного міжнародного стандарту;

вимірюваність – усі критерії оцінюються за чітко визначеною числовою шкалою;

відтворюваність – повний математичний апарат забезпечує можливість незалежного відтворення результатів;

масштабованість – методика застосовна до будь-якої кількості пристроїв і може бути розширена додатковими критеріями.

Вхідними даними методики є оцінки пристроїв за кожним із визначених критеріїв, отримані шляхом тестування на проникнення (penetration testing), аналізу технічної документації виробника або незалежного експертного оцінювання за шкалою від 1 до 5. Вихідними даними є ранжований список пристроїв за значенням інтегрального індексу

захищеності $CI \epsilon [0;\ 1]$ та рекомендації щодо підвищення захищеності для кожного пристрою на основі шкали (табл. 6).

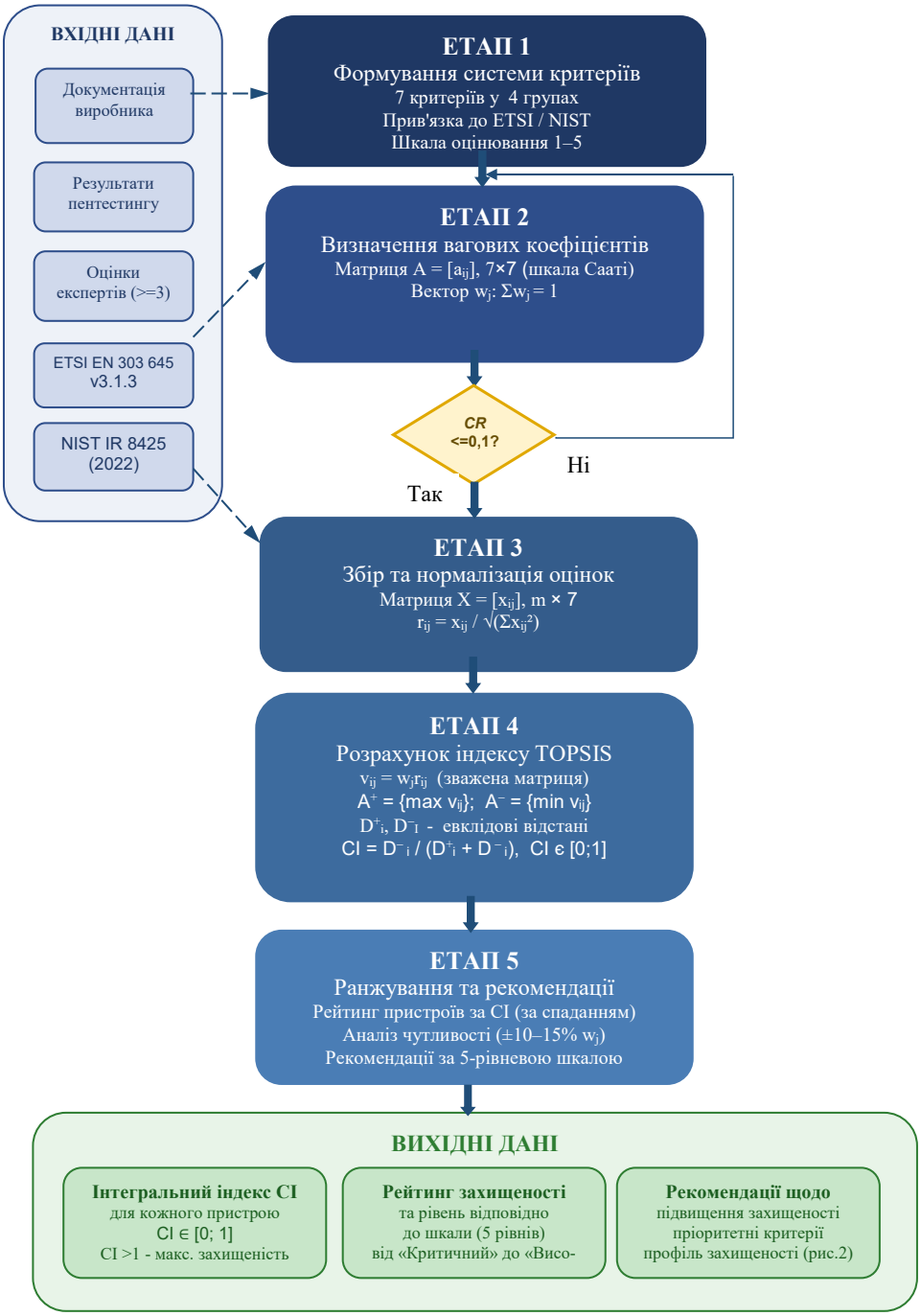

Рис. 1. Загальна архітектура п'ятиетапної методики оцінювання захищеності IoT-пристроїв

Система критеріїв є фундаментом всієї методики, оскільки від повноти та вимірюваності критеріїв безпосередньо залежить якість кінцевого результату. Критерії формуються на основі двох ключових міжнародних стандартів: ETSI EN 303 645 v3.1.3 та NIST IR 8425. ETSI EN 303 645, розроблений Комітетом технічних стандартів ETSI TC CYBER, є найбільш широко використовуваним міжнародним стандартом у сфері кібербезпеки споживчих IoT-пристроїв

та є технічною основою для регуляторних вимог Cyber Resilience Act ЄС [8]. NIST IR 8425 визначає базовий профіль вимог кіберзахисту для споживчих IoT-продуктів на ринку США.

У результаті систематичного аналізу вимог обох стандартів та виявлення їх перетину сформовано систему з семи критеріїв, об'єднаних у чотири функціональні групи (табл. 1). Кожен критерій відповідає таким вимогам до його включення в систему: об'єктивна вимірюваність за шкалою 1–5; наявність відповідної прямої вимоги у стандарті ETSI EN 303 645 або NIST IR 8425; суттєвий вплив на загальний рівень захищеності пристрою.

Таблиця 1

Система критеріїв оцінювання захищеності IoT-пристроїв

№ з/п	Код	Назва критерію	Відповідна вимога стандарту	Група	Шкала
1	K_1	Захист від несанкціонованого доступу (МФА, управління сесіями)	*ETSI EN 303 645, Вимога 5.1; NIST IR 8425, §3.1*	Автентифікація	1–5
2	K_2	Унікальність та складність облікових даних за замовчуванням	*ETSI EN 303 645, Вимога 5.1-1; NIST IR 8425, §3.2*	Автентифікація	1–5
3	K_3	Шифрування каналів передачі даних (TLS 1.2/1.3, DTLS 1.2)	*ETSI EN 303 645, Вимога 5.5; NIST IR 8425, §3.5*	Комунікація	1–5
4	K_4	Захищений механізм оновлення прошивки (цифровий підпис, rollback)	*ETSI EN 303 645, Вимога 5.3; NIST IR 8425, §3.4*	Оновлення	1–5
5	K_5	Мінімізація поверхні атаки (відключені невикористані інтерфейси)	*ETSI EN 303 645, Вимога 5.6; NIST IR 8425, §3.6*	Архітектура	1–5
6	K_6	Забезпечення конфіденційності та цілісності персональних даних	*ETSI EN 303 645, Вимога 5.12; NIST IR 8425, §3.7*	Захист даних	1–5
7	K_7	Наявність задокументованої політики розкриття вразливостей (VDP)	*ETSI EN 303 645, Вимога 5.2; NIST IR 8425, §3.9*	Управління	1–5

Шкала оцінювання критеріїв: 5 – повна відповідність вимогам стандарту; 4 – відповідність із незначними недоліками; 3 – часткова відповідність; 2 – суттєві відхилення від вимог; 1 – повна невідповідність або відсутність механізму. До оцінювання рекомендується залучати сертифікованих фахівців у сфері кібербезпеки (Certified Ethical Hacker (CEH), Offensive Security Certified Professional (OSCP), Certified Information Systems Security Professional (CISSP)).

Метод аналітичного ієрархічного процесу (AHP), розроблений Томасом Сааті у 1980 році [9], є одним із найбільш теоретично обґрунтованих і практично апробованих методів визначення відносних пріоритетів критеріїв у задачах MCDM. Метод здійснює декомпозицію складної задачі вибору на ієрархію підзадач і синтезує часткові судження в загальний вектор пріоритетів через систему попарних порівнянь.

Порівняння критеріїв між собою здійснюється за дев'ятибальною шкалою Сааті (табл. 2), яка дозволяє перетворити якісні судження експертів про відносну важливість критеріїв на числові значення.

Таблиця 2

Шкала попарних порівнянь Сааті для методу AHP

Значення a_{ij}	Вербальна оцінка	Пояснення
1	Рівнозначність	Обидва критерії однаково важливі для захищеності пристрою
3	Помірна перевага	Один критерій дещо важливіший; досвід підтверджує незначну перевагу

Значення a_{ij}	**Вербальна оцінка**	**Пояснення**
5	Суттєва перевага	Один критерій явно важливіший; перевага підтверджена практично
7	Значна перевага	Один критерій набагато важливіший; домінування добре доведене
9	Абсолютна перевага	Максимально можлива перевага одного критерію над іншим
2, 4, 6, 8	Проміжні значення	Компромісні судження між суміжними рівнями шкали

Повний алгоритм методу AHP у запропонованій методиці складається з шести кроків (табл. 3).

Таблиця 3

Покроковий алгоритм методу AHP для визначення вагових коефіцієнтів критеріїв

Крок	**Операція**	**Математичний вираз / опис**
1	Формування матриці попарних порівнянь	$A = [a_{ij}], n \times n;\ a_{ij} = \frac{1}{a_{ij}};\ a_{ij} = 1.$ Елемент a_{ij} – відносна важливість критерію i над j за шкалою Сааті
2	Нормалізація матриці	$r_{ij} = \frac{a_{ij}}{\sum_i a_{ij}}$ (нормалізація по стовпцях)
3	Обчислення вектора пріоритетів	$w_j = (\frac{1}{n}) \sum_i r_{ij}$ (середнє по рядках нормалізованої матриці)
4	Розрахунок λ_{max}	$\lambda_{max} = \left(\frac{1}{n}\right) \sum_j \left[\frac{(A_w)_j}{w_j}\right]$, де A_w добуток матриці A на вектор w
5	Індекс узгодженості	$\mathrm{CI} = \frac{\lambda_{max} - n}{n - 1}$
6	Коефіцієнт узгодженості	$CR = CI/R_n$ – умова прийнятності: $CR \leq 0{,}10$

Значення випадкового індексу RI, що використовується у формулі коефіцієнта узгодженості CR, залежить від розмірності матриці n та наведено у таблиці 4 [9].

Таблиця 4

Значення випадкового індексу RI за Сааті (для матриць різного розміру n)

n	1	2	3	4	5	6	7	8	9	10
Rn	0,00	0,00	0,58	0,90	1,12	1,24	1,32	1,41	1,45	1,49

Для застосування запропонованої методики ($n = 7$ критеріїв) використовується значення $R_7 = 1{,}32$. Якщо $CR > 0{,}10$, необхідно переглянути матрицю попарних порівнянь, виявити суперечливі судження та скоригувати їх. Рекомендується залучати до процедури порівняння від трьох до семи незалежних експертів у галузі безпеки IoT, а остаточну матрицю формувати як геометричне середнє індивідуальних матриць кожного експерта.

Вектор пріоритетів $w = (w_1, w_2, \ldots, w_7)$, де $\Sigma w_j = 1$, є числовим відображенням відносної важливості кожного критерію безпеки в загальній оцінці захищеності пристрою. Критерій з найбільшим значенням w_j справляє найбільший вплив на підсумковий рейтинг TOPSIS. Вектор ваг встановлюється одноразово для методики та залишається незмінним протягом усього циклу оцінювання однотипних пристроїв. При суттєвій зміні нормативного контексту (наприклад, при виході нової версії стандарту ETSI EN 303 645) рекомендується повторна процедура AHP.

Матриця оцінок $X = [x_{ij}]$ розміром $m \times n$, де m – кількість досліджуваних пристроїв, $n = 7$ – кількість критеріїв, формується на основі зібраних оцінок. Нормалізація матриці необхідна для забезпечення порівнянності значень різних критеріїв та усунення впливу одиниць вимірювання. У методі TOPSIS застосовується векторна нормалізація (1):

$$r_{ij} = x_{ij}\sqrt{\sum_i x_{ij}^2}, i = 1 \dots m,\ j = 1 \dots n, \quad (1)$$

де r_{ij} – нормалізована оцінка альтернативи (пристрою) i за критерієм j. Нормалізована матриця $R = [r_{ij}]$ має ту саму розмірність, що і вихідна матриця X, але всі значення є безрозмірними і задовольняють умові: $\sum_i r_{ij}^2 = 1$ для кожного j.

Метод TOPSIS (Technique for Order Preference by Similarity to Ideal Solution) запропонований Хвангом та Юном у 1981 році [10]. Концептуальна основа методу полягає у тому, що найкраща альтернатива одночасно максимально наближена до ідеального позитивного рішення (еталон максимальної захищеності) та максимально віддалена від ідеального негативного рішення (еталон мінімальної захищеності). Повний алгоритм TOPSIS наведено у таблиці 5.

Таблиця 5

Покроковий алгоритм методу TOPSIS для ранжування IoT-пристроїв за захищеністю

Крок	**Операція**	**Математичний вираз**
1	Векторна нормалізація матриці рішень	$r_{ij} = \frac{x_{ij}}{\sqrt{(\Sigma_i x^2{}_{ij})}}$, де x_{ij} – оцінка альтернативи i за критерієм j
2	Зважена нормалізована матриця	$v_{ij} = w_j r_{ij}$, де w_j – вагові коефіцієнти (AHP)
3	Ідеальне позитивне рішення	$A^+ = \{ v_j^+ \} = \{\max(v_{ij})\}, j = 1 \dots n$ (максимум по кожному критерію)
4	Ідеальне негативне рішення	$A^- = \{ v_j^- \} = \{\max(v_{ij})\}, j = 1 \dots n$ (мінімум по кожному критерію)
5	Відстань до A^+ (евклідова)	$D_i^+ = \sqrt{(\sum_j (v_{ij} - v_j^+)^2)}$
6	Відстань до A^- (евклідова)	$D_i^- = \sqrt{(\sum_j (v_{ij} - v_j^-)^2)}$
7	Інтегральний індекс захищеності	$CI = \frac{D_i^-}{(D_i^+ + D_i^-)}$; $C_i \in [0, 1]$
8	Ранжування альтернатив	Альтернативи ранжуються за спаданням CI; $CI \to 1$ означає максимальну захищеність

Ідеальне позитивне рішення A^+ відповідає гіпотетичному пристрою з максимальними зваженими оцінками за всіма критеріями; A^- – з мінімальними. Інтегральний індекс $CI = \frac{D_i^-}{(D_i^+ + D_i^-)}$ відображає відносну наближеність пристрою до еталона: $CI = 1$ – максимальна захищеність; $CI = 0$ – мінімальна.

Радарна діаграма на рисунку 2 ілюструє принцип побудови профілю захищеності пристрою: кожна вісь відповідає одному критерію $К_1 - К_7$; площа полігону візуалізує загальний рівень захищеності та дозволяє наочно ідентифікувати "слабкі місця" – критерії, за якими значення суттєво відхиляються від ідеального еталона.

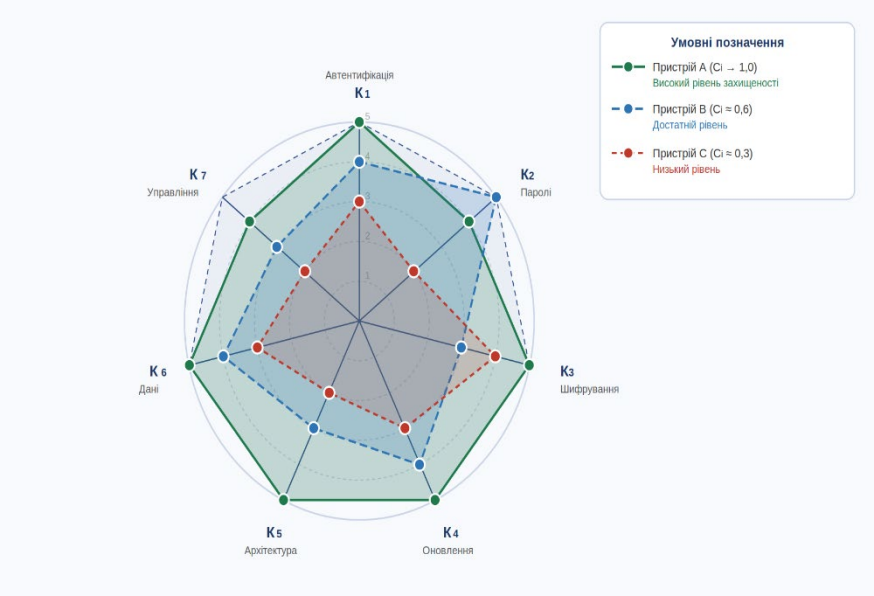

Рис. 2. Ілюстрація профілю захищеності IoT-пристроїв у вигляді радарної діаграми ($К_1 - К_7$)

Для практичного застосування результатів методики розроблено п'ятирівневу шкалу інтерпретації значень інтегрального індексу захищеності CI з рекомендованими заходами для кожного рівня (табл. 6). Межі рівнів встановлено рівномірно в діапазоні [0; 1] з виділенням п'яти зон, що відповідають практично значущим рівням захищеності від критичного до високого.

Таблиця 6

Шкала інтерпретації значень інтегрального індексу захищеності CI та рекомендовані заходи

Діапазон CI	**Рівень захищеності**	**Рекомендовані дії**
0,80–1,00	Високий	Пристрій відповідає більшості вимог ETSI EN 303 645. Рекомендується моніторинг та планове оновлення
0,60–0,79	Достатній	Наявні окремі вразливості. Необхідне усунення виявлених недоліків протягом 3–6 місяців
0,40–0,59	Задовільний	Суттєві прогалини у безпеці. Потрібні термінові заходи з підвищення захищеності
0,20–0,39	Низький	Критичні вразливості. Рекомендується обмежити використання або замінити пристрій
0,00–0,19	Критичний	Пристрій не відповідає базовим вимогам безпеки. Необхідне негайне виведення з експлуатації

Для перевірки практичної придатності запропонованої методики проведено її апробацію на прикладі трьох умовних споживчих IoT-пристроїв: розумної камери відеоспостереження A_1, розумної IP-розетки A_2 та фітнес-браслета A_3. Вибір саме таких типів пристроїв зумовлений їхньою широкою поширеністю у побутовому сегменті та відмінностями у функціональному призначенні, архітектурі та профілі загроз (табл. 7).

Таблиця 7

Матриця вихідних оцінок трьох IoT-пристроїв за критеріями захищеності

Пристрій	**$К_1$**	**$К_2$**	**$К_3$**	**$К_4$**	**$К_5$**	**$К_6$**	**$К_7$**
A_1 – розумна камера відеоспостереження	5	4	5	4	3	4	3
A_2 – розумна IP-розетка	3	2	3	2	4	3	2
A_3 – фітнес-браслет	4	3	4	3	4	5	4

Для демонстрації роботи методики було сформовано матрицю вихідних оцінок трьох умовних IoT-пристроїв за сімома критеріями захищеності $К_1$–$К_7$. Значення оцінок було задано за п'ятибальною шкалою, де 1 відповідає повній невідповідності вимогам безпеки, а 5 – повній відповідності.

Пристрій A_1 (розумна камера відеоспостереження) характеризується високим рівнем захищеності каналів зв'язку та механізмів автентифікації, однак має певні обмеження щодо мінімізації поверхні атаки та документованої політики розкриття вразливостей. Пристрій A_2 (розумна IP-розетка) демонструє нижчі оцінки за більшістю критеріїв, зокрема щодо захисту облікових даних та безпечного оновлення прошивки. Пристрій A_3 (фітнес-браслет) займає проміжне положення, поєднуючи достатньо високий рівень захисту даних із помірними характеристиками в частині автентифікації та оновлень.

На першому етапі для системи критеріїв $К_1$– $К_7$ методом AHP було визначено вагові коефіцієнти, що відображають відносну важливість кожного критерію у загальній оцінці захищеності. Для цього сформовано матрицю попарних порівнянь критеріїв за шкалою Сааті, на основі якої обчислено вектор пріоритетів $w = (w_1, \dots, w_7)$. Узгодженість експертних суджень перевірено шляхом обчислення коефіцієнта узгодженості CR. Оскільки $CR \leq 0{,}10$, матрицю визнано прийнятною для подальшого використання.

На другому етапі було сформовано матрицю оцінок пристроїв $X = [x_{ij}]$, де кожний елемент x_{ij} відображав оцінку i-го пристрою за j-м критерієм за шкалою від 1 до 5. Оцінювання було виконано на основі експертно заданих демонстраційних значень. Після цього до матриці X було застосовано процедуру TOPSIS: виконано нормалізацію, побудовано зважену нормалізовану матрицю, визначено позитивне і негативне ідеальні рішення, обчислено евклідові відстані до них та інтегральний індекс захищеності CI для кожного пристрою.

Отримані значення CI дали змогу здійснити ранжування альтернатив за рівнем захищеності та віднести кожен пристрій до одного з інтерпретаційних рівнів, наведених у таблиці 6. Крім того, аналіз зважених нормалізованих оцінок дав змогу виявити критерії, які найбільше вплинули на підсумковий результат і, відповідно, визначити пріоритетні напрями підвищення захищеності конкретного пристрою.

Наведена апробація демонструє, що серед розглянутих підходів запропонована методика AHP-TOPSIS найбільш повно забезпечує всі шість функціональних властивостей.

Таблиця 8

Вагові коефіцієнти критеріїв захищеності, визначені методом AHP

Критерій	**Позначення**	**Вага w_j**
Захист від несанкціонованого доступу	$К_1$	0,22
Унікальність та складність облікових даних	$К_2$	0,16
Шифрування каналів передачі даних	$К_3$	0,18
Захищений механізм оновлення прошивки	$К_4$	0,17
Мінімізація поверхні атаки	$К_5$	0,09
Захист персональних даних	$К_6$	0,12
Політика розкриття вразливостей	$К_7$	0,06
Сума		**1,00**

За результатами застосування методу AHP було отримано вектор вагових коефіцієнтів критеріїв $w = (0{,}22; 0{,}16; 0{,}18; 0{,}17; 0{,}09; 0{,}12; 0{,}06)$ (табл. 8). Найбільшу вагу отримали критерії, пов'язані з автентифікацією, захистом каналів зв'язку та безпечним оновленням, оскільки саме вони найбільшою мірою визначають стійкість IoT-пристрою до типових кіберзагроз. Меншу вагу було надано критеріям мінімізації поверхні атаки та наявності

політики розкриття вразливостей, які, хоча й є важливими, мають більш опосередкований вплив на безпосередній рівень технічної захищеності пристрою.

Після визначення вагових коефіцієнтів критеріїв було реалізовано процедуру оцінювання альтернатив методом TOPSIS. На основі матриці вихідних оцінок виконано векторну нормалізацію за кожним критерієм, після чого отримані значення було помножено на відповідні вагові коефіцієнти w_j. У результаті було сформовано зважену нормалізовану матрицю $V = [v_{ij}]$, яка стала основою для визначення ідеального позитивного та ідеального негативного рішень.

Таблиця 9

Нормалізована матриця оцінок IoT-пристроїв

Пристрій	$\mathbf{K_1}$	$\mathbf{K_2}$	$\mathbf{K_3}$	$\mathbf{K_4}$	$\mathbf{K_5}$	$\mathbf{K_6}$	$\mathbf{K_7}$
A_1	0,707	0,743	0,707	0,743	0,469	0,566	0,557
A_2	0,424	0,371	0,424	0,371	0,625	0,424	0,371
A_3	0,566	0,557	0,566	0,557	0,625	0,707	0,743

Після визначення вагових коефіцієнтів критеріїв було реалізовано процедуру оцінювання альтернатив методом TOPSIS. На основі нормалізованої матриці (табл. 9) виконано формування зваженої нормалізованої матриці шляхом множення кожного елемента на відповідний ваговий коефіцієнт w_j (табл. 10).

Таблиця 10

Зважена нормалізована матриця оцінок IoT-пристроїв

Пристрій	$\mathbf{K_1}$	$\mathbf{K_2}$	$\mathbf{K_3}$	$\mathbf{K_4}$	$\mathbf{K_5}$	$\mathbf{K_6}$	$\mathbf{K_7}$
A_1	0,156	0,119	0,127	0,126	0,042	0,068	0,033
A_2	0,093	0,059	0,076	0,063	0,056	0,051	0,022
A_3	0,124	0,089	0,102	0,095	0,056	0,085	0,045

Далі за кожним критерієм визначено компоненти ідеального позитивного рішення A^+ та ідеального негативного рішення A^-. Оскільки всі критерії у запропонованій методиці є критеріями вигоди, до складу A^+ включено максимальні значення зваженої нормалізованої матриці, а до складу A^- – мінімальні (табл. 11).

Таблиця 11

Ідеальне позитивне та ідеальне негативне рішення

Рішення	$\mathbf{K_1}$	$\mathbf{K_2}$	$\mathbf{K_3}$	$\mathbf{K_4}$	$\mathbf{K_5}$	$\mathbf{K_6}$	$\mathbf{K_7}$
A^+	0,156	0,119	0,127	0,126	0,056	0,085	0,045
A^-	0,093	0,059	0,076	0,063	0,042	0,051	0,022

На наступному кроці обчислено евклідові відстані кожної альтернативи до позитивного і негативного ідеальних рішень, а також інтегральний індекс захищеності CI. Чим більше значення CI, тим ближчою є альтернатива до ідеального рішення і тим вищим є її рівень захищеності (табл. 12).

Таблиця 12

Результати розрахунку інтегрального індексу захищеності методом TOPSIS

Пристрій	$\boldsymbol{D_i^+}$	$\boldsymbol{D_i^-}$	CI	**Ранг**	**Рівень захищеності**
A_1 – розумна камера відеоспостереження	0,025	0,120	0,829	1	Високий
A_2 – розумна IP-розетка	0,125	0,014	0,101	3	Критичний
A_3 – фітнес-браслет	0,059	0,073	0,553	2	Задовільний

За результатами розрахунків найвище значення інтегрального індексу захищеності отримав пристрій A_1 – розумна камера відеоспостереження ($C_1 = 0{,}829$), що відповідає високому рівню захищеності. Це пояснюється високими оцінками за найбільш вагомими критеріями, зокрема захистом від несанкціонованого доступу, шифруванням каналів передачі даних та захищеним оновленням прошивки. Друге місце посів пристрій A_3 – фітнес-браслет ($C_3 = 0{,}553$), який належить до задовільного рівня захищеності. Незважаючи на високі показники за критерієм захисту даних, загальний результат цього пристрою знижується через помірні оцінки за критеріями автентифікації та оновлення. Найнижчий результат продемонстрував пристрій A_2 – розумна IP-розетка ($C_2 = 0{,}101$), що відповідає критичному рівню захищеності. Основними причинами такого результату є низькі оцінки за критеріями унікальності облікових даних, захищеного оновлення прошивки та політики розкриття вразливостей.

З метою підвищення достовірності отриманих результатів та перевірки масштабованості запропонованої методики було сформовано розширену вибірку з десяти споживчих IoT-пристроїв, що охоплюють різні класи застосувань: системи відеоспостереження, мережеве обладнання, носимі пристрої, елементи розумного дому та побутову техніку.

До набору альтернатив увійшли такі пристрої: A_1 – розумна камера відеоспостереження, A_2 – розумна IP-розетка, A_3 – фітнес-браслет, A_4 – розумний замок, A_5 – Smart TV, A_6 – розумна лампа, A_7 – Wi-Fi роутер, A_8 – розумний термостат, A_9 – голосовий асистент, A_{10} – розумний холодильник.

Оцінювання пристроїв здійснювалося за тією самою системою критеріїв $\mathrm{K}_1 - \mathrm{K}_7$ та шкалою 1–5, що забезпечує повну порівнянність результатів із попередньою апробацією. Вагові коефіцієнти критеріїв залишено незмінними, що дозволяє зберегти узгодженість моделі та коректність інтерпретації отриманих результатів.

Таблиця 13

Матриця оцінок 10 IoT-пристроїв за критеріями захищеності

Пристрій	$\mathbf{K_1}$	$\mathbf{K_2}$	$\mathbf{K_3}$	$\mathbf{K_4}$	$\mathbf{K_5}$	$\mathbf{K_6}$	$\mathbf{K_7}$
A_1	5	4	5	4	3	4	3
A_2	3	2	3	2	4	3	2
A_3	4	3	4	3	4	5	4
A_4	5	4	4	4	3	4	3
A_5	4	3	4	3	3	4	2
A_6	2	2	3	2	3	2	1
A_7	5	5	5	4	4	4	4
A_8	4	3	4	4	3	4	3
A_9	3	3	4	3	3	3	2
A_{10}	3	2	3	3	2	3	2

Оцінки, наведені у таблиці 13, сформовано на основі узагальненого експертного аналізу функціональних можливостей пристроїв, типових реалізацій механізмів безпеки та відкритих результатів досліджень у сфері IoT-безпеки. Значення відображають узагальнений рівень відповідності пристроїв вимогам стандартів ETSI EN 303 645 та NIST IR 8425.

Таблиця 14

Результати оцінювання захищеності 10 IoT-пристроїв методом TOPSIS

Пристрій	CI	**Ранг**	**Рівень захищеності**
A_7 (роутер)	0,89	1	Високий
A_1 (камера)	0,83	2	Високий
A_4 (замок)	0,78	3	Достатній

Пристрій	CI	**Ранг**	**Рівень захищеності**
A_8 (термостат)	0,72	4	Достатній
A_3 (браслет)	0,66	5	Достатній
A_5 (TV)	0,58	6	Задовільний
A_9 (асистент)	0,51	7	Задовільний
A_{10} (холодильник)	0,39	8	Низький
A_2 (розетка)	0,21	9	Низький
A_6 (лампа)	**0,08**	10	Критичний

Отримані результати (табл. 14) демонструють чітку диференціацію IoT-пристроїв за рівнем захищеності. Найвище значення інтегрального індексу отримав Wi-Fi роутер (A_7), що пояснюється наявністю розвинених механізмів автентифікації, підтримкою сучасних криптографічних протоколів і регулярними оновленнями програмного забезпечення.

Високі позиції також займають камера відеоспостереження (A_1) та розумний замок (A_4), що характеризуються достатнім рівнем захисту каналів передачі даних і контролю доступу. Натомість пристрої нижчого цінового сегмента, зокрема розумна лампа (A_6) та IP-розетка (A_2), демонструють найнижчі значення індексу захищеності, що пов'язано з обмеженою реалізацією базових механізмів безпеки, відсутністю регулярних оновлень та слабкою політикою управління обліковими даними.

Аналіз результатів підтверджує, що найбільший вплив на підсумкове ранжування мають критерії, пов'язані з автентифікацією, шифруванням каналів зв'язку та механізмами оновлення програмного забезпечення, що узгоджується з отриманими ваговими коефіцієнтами методу AHP. Менш вагомі критерії відіграють допоміжну роль, формуючи комплексний профіль захищеності пристрою.

Отримані результати підтверджують практичну придатність методики забезпечувати обґрунтоване кількісне ранжування пристроїв, що може бути використано для підтримки прийняття рішень у задачах вибору IoT-обладнання, проведення безпекового аудиту та формування рекомендацій щодо підвищення рівня захищеності. Крім того, узгодженість результатів із попередньою апробацією підтверджує стабільність моделі та коректність застосування гібридного підходу AHP-TOPSIS.

Крім визначення загального рейтингу, методика передбачає аналіз внеску окремих критеріїв у підсумковий результат. Для ідентифікації "слабких місць" пристрою рекомендується побудова профілю захищеності – таблиці або радарної діаграми, що відображає зважені нормалізовані оцінки v_{ij} пристрою за кожним критерієм порівняно з відповідними значеннями A^+ та A^-. Критерії, за якими значення v_{ij} найбільш суттєво відхиляються від v_j^+, є першочерговими об'єктами для заходів з підвищення захищеності.

Для забезпечення надійності результатів рекомендується також проводити аналіз чутливості: почергово варіювати вагові коефіцієнти w_j у діапазоні ± 10–15 % від базових значень та перевіряти стійкість отриманого ранжування. Якщо ранжування пристроїв не змінюється при жодному з тестових сценаріїв, результати вважаються стійкими і придатними для прийняття рішень.

Для оцінювання переваг та обмежень запропонованої методики здійснено її порівняння з трьома найбільш поширеними підходами до оцінювання захищеності IoT-пристроїв (табл. 15):

якісний аудит на основі контрольних списків відповідно до ETSI EN 303 645;

ризик-матриця;

Common Vulnerability Scoring System (CVSS) – стандартизована методика кількісної оцінки вразливостей.

Таблиця 15

Порівняльний аналіз запропонованої методики AHP-TOPSIS з існуючими підходами

Характеристика	**Checklist (ETSI EN 303 645)**	**Ризик-матриця**	**CVSS-оцінка**	**AHP-TOPSIS (запропонована)**
Кількісний агрегований індекс	–	–	Частково	✓
Прив'язка до ETSI EN 303 645	✓	–	–	✓
Порівняльне ранжування пристроїв	–	–	–	✓
Врахування пріоритетності критеріїв	–	Частково	–	✓
Аналіз чутливості	–	–	–	✓
Відтворюваність результатів	✓	Частково	✓	✓

Як видно з таблиці 15, запропонована методика AHP-TOPSIS є єдиним підходом, що одночасно забезпечує всі шість розглянутих функціональних властивостей. Якісний checklist-підхід на основі ETSI EN 303 645 задовольняє вимогу нормативної прив'язки та відтворюваності, але не дозволяє отримати кількісний агрегований індекс і порівнювати пристрої між собою. Ризик-матриця враховує пріоритетність загроз лише частково і не пов'язана безпосередньо зі стандартом ETSI EN 303 645. CVSS забезпечує кількісну оцінку окремих вразливостей, але не призначений для оцінювання загального рівня захищеності пристрою.

Водночас, запропонована методика має певні обмеження. По-перше, якість вхідних оцінок пристроїв залежить від кваліфікації оцінювачів та повноти доступної технічної документації. По-друге, процедура попарного порівняння AHP є відносно трудомісткою при великій кількості критеріїв (понад 9), хоча для запропонованої системи з 7 критеріїв це не є суттєвим обмеженням. Перспективним напрямом розширення методики є застосування нечіткого AHP (Fuzzy AHP) для моделювання лінгвістичної невизначеності в судженнях експертів [7].

Таким чином, проведена розширена апробація підтверджує, що запропонована методика є масштабованою та придатною для оцінювання захищеності широкого класу IoT-пристроїв. На відміну від демонстраційного прикладу з обмеженою кількістю альтернатив, розширена вибірка дозволяє більш повно відобразити варіативність рівнів захищеності в реальних умовах та виявити стійкі закономірності впливу окремих критеріїв на підсумковий результат.

Наукова новизна дослідження полягає в розробці методики оцінювання захищеності IoT-пристроїв, що одночасно:

ґрунтується на актуальних міжнародних стандартах ETSI EN 303 645 v3.1.3 та NIST IR 8425;

застосовує математично обґрунтований апарат гібридного MCDM AHP-TOPSIS;

є придатною для широкого класу споживчих IoT-пристроїв;

містить шкалу інтерпретації результатів із практичними рекомендаціями.

Практична цінність методики полягає в її застосовності для: обґрунтованої закупівлі IoT-обладнання у корпоративному та державному секторах; проведення незалежного аудиту захищеності IoT-систем; проєктування нових IoT-рішень із врахуванням вимог безпеки на ранніх етапах.

Перспективи подальших досліджень: розширення системи критеріїв до повного охоплення вимог ETSI EN 303 645; застосування нечіткого AHP (Fuzzy AHP) для моделювання лінгвістичної невизначеності; розробка програмного інструменту автоматизації розрахунків; адаптація методики для промислових IoT-систем відповідно до стандарту ISA/IEC 62443.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. State of IoT – Spring 2023. Berlin: IoT Analytics GmbH, 2023. URL: https://iot-analytics.com/number-connected-iot-devices.

2. ETSI EN 303 645 V3.1.3 (2024-09). Cybersecurity for Consumer Internet of Things: Baseline Requirements. Sophia Antipolis: European Telecommunications Standards Institute, 2024. 72 p.

3. Fagan M., Megas K., Scarfone K., Smith M. IoT Core Baseline for Consumer IoT Products. NIST IR 8425. Gaithersburg: National Institute of Standards and Technology, 2022. DOI: https://doi.org/10.6028/NIST.IR.8425.

4. Al-Dhaqm A. et al. Security risk assessment in IoT environments: A taxonomy and survey // Computers & Security. 2025. Vol. 153. Article 104197. DOI: https://doi.org/10.1016/j.cose.2025.104197.

5. Khan H. U., Ali Y., Khan F. A. A features-based privacy preserving assessment model for authentication of internet of medical things (IoMT) devices in healthcare // Mathematics. 2023. Vol. 11, No. 5. P. 1197. DOI: https://doi.org/10.3390/math11051197.

6. Radulescu C. Z., Radulescu M. A. Hybrid group multi-criteria approach based on SAW, TOPSIS, VIKOR, and COPRAS methods for complex IoT selection problems // Electronics. 2024. Vol. 13, No. 4. P. 789. DOI: https://doi.org/10.3390/electronics13040789.

7. Ksibi S., Jaidi F., Bouhoula A. User-centric fuzzy AHP-based method for medical devices security assessment. In: Proceedings of the 15th International Conference on Security of Information and Networks (SIN). Sousse: IEEE, 2022. DOI: https://doi.org/10.1109/SIN56466.2022.9970520.

8. Regulation (EU) 2024/2847 of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act) // Official Journal of the European Union. 2024. L 2024/2847.

9. Saaty T. L. The analytic hierarchy process: planning, priority setting, resource allocation. New York: McGraw-Hill, 1980. 287 p.

10. Hwang C.-L., Yoon K. Multiple attribute decision making: methods and applications // Lecture Notes in Economics and Mathematical Systems. Vol. 186. Berlin: Springer, 1981. 259 p. DOI: https://doi.org/10.1007/978-3-642-48318-9.

11. Cîmpean D. A. et al. Security assessment of an Internet of Things device. In: Good practices and new perspectives in information systems and technologies. WorldCIST 2024 // Lecture Notes in Networks and Systems. Vol. 989. Cham: Springer, 2024. P. 261–272. DOI: https://doi.org/10.1007/978-3-031-60227-6_26.

12. OWASP IoT Security Testing Guide. Release 1.0. March 2024. URL: https://owasp.org/blog/2024/03/01/iot-security-testing-guide.

13. Sahoo S. K., Goswami S. S. A comprehensive review of multiple criteria decision-making (MCDM) methods: advancements, applications, and future directions // Decision Making: Advances. 2023. Vol. 1, No. 1. P. 25–48. DOI: https://doi.org/10.31181/dma1120235.

14. Alharbi A. et al. Selection of data analytic techniques by using fuzzy AHP TOPSIS from a healthcare perspective // BMC Medical Informatics and Decision Making. 2024. Vol. 24, No. 1. P. 240. DOI: https://doi.org/10.1186/s12911-024-02651-8.

Надійшла до редколегії 26.03.2026.
Схвалена до друку 22.05.2026.
Дата публікації 29.05.2026.