УДК 004.056.5:519.816
DOI: 10.31673/2409-7292.2026.010765

Собчук А.В., Лаптєва Т.О., Капустян Д.О., Степанченко Б. С., Лаптєв С.О.

МЕТОД ОПТИМІЗАЦІЇ СИСТЕМИ ЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЗА ЗВАЖЕНОЇ СУМИ КРИТЕРІЇВ

У статті розглядається актуальна наукова задача багатокритеріальної оптимізації системи захисту інформації на об'єктах критичної інфраструктури, де одночасно діють суперечливі вимоги: необхідність мінімізації ризиків, витрат і затримок при забезпеченні високої доступності та швидкості реагування на кіберзагрози. Запропоновано застосування методу зваженої суми критеріїв як ефективного інструменту для зведення векторної цільової функції до скалярної форми, що дозволяє інтегрувати суб'єктивні пріоритети власника інфраструктури через налаштування вагових коефіцієнтів. Особливу увагу приділено умовам коректного застосування методу, зокрема припущенню про опуклість Парето-фронту, яке гарантує отримання повної множини Парето-оптимальних розв'язків. Обґрунтовано необхідність попередньої обробки критеріїв – уніфікації напрямку оптимізації, нормалізації значень, виміряних у різних одиницях, та формалізації обмежень, пов'язаних із бюджетом, латентністю та рівнем доступності. На прикладі трьох ключових критеріїв – ризик, витрати та час реагування – продемонстровано побудову цільової функції, яка мінімізується в рамках реалістичних обмежень, характерних для великих інфраструктурних об'єктів. Аналіз існуючих підходів (ε-обмежень, AHP, TOPSIS, еволюційних алгоритмів) підтверджує переваги запропонованого методу у контексті швидкого прототипування та практичної реалізації завдяки його обчислювальній простоті, інтерпретованості та сумісності з класичними методами оптимізації. Результати дослідження підкреслюють значення методу зваженої суми як науково обґрунтованого та практично придатного підходу до проєктування ефективних, економічно доцільних і функціонально стійких систем кіберзахисту для критично важливих секторів економіки.

Ключові слова: система захисту інформації, об'єкти критичної інфраструктури, багатокритеріальна оптимізація, метод зваженої суми, Парето-оптимальність, кібербезпека, ризики.

Вступ

У цифровому світі об'єкти критичної інфраструктури (ОКІ), а саме енергетичні мережі, транспортні системи, фінансові установи, медичні заклади та інші, стають стратегічними цілями для кібератак, що постійно зростають за складністю, частотою та руйнівним потенціалом. Забезпечення їх кібербезпеки вимагає не лише застосування передових захисних механізмів, а й узгодженого балансу між конфліктуючими цілями: мінімізацією інформаційних ризиків, економічною доцільністю, низькою латентністю обробки даних, високою доступністю систем та швидкістю реагування на інциденти. Ця багатокритеріальна природа задачі ускладнює вибір оптимальних рішень при проєктуванні системи захисту інформації (СЗІ), оскільки поліпшення одного показника часто призводить до погіршення іншого. У цьому контексті особливо актуальною стає проблема формалізації процесу прийняття зважених рішень, який би одночасно враховував як об'єктивні обмеження (бюджет, технічні параметри), так і суб'єктивні пріоритети власника інфраструктури.

Метод зваженої суми критеріїв (Weighted Sum Method, WSM) є ефективним підхідодом до вирішення цієї проблеми: він дозволяє об'єднати різнорідні цільові функції в єдину скалярну функцію, сумісну з класичними методами оптимізації (LP/NLP, евристики). Хоча WSM має відоме обмеження, здатність генерувати повну множину Парето-оптимальних розв'язків лише за умови опуклості Парето-фронту, саме ця властивість робить його ідеальним інструментом для швидкого прототипування та первинного проєктування СЗІ у реальних інфраструктурних умовах, де простота, інтерпретованість і обчислювальна ефективність є вирішальними.

Актуальність запропонованого підходу підтверджується аналізом сучасних досліджень: хоча існують роботи, що застосовують WSM до налаштування IDS або розподілу ресурсів у 5G-мережах, жодна з них не надає достатнього теоретичного обґрунтування умов його коректного застосування зокрема, щодо нормалізації критеріїв різної природи та умови опуклості. Тому подальша розробка та обґрунтування методу зваженої суми в контексті СЗІ ОКІ є науково та практично значущим завданням, спрямованим на підвищення надійності, ефективності та адаптивності систем кіберзахисту в умовах усе більш агресивного нападу.

Аналіз літературних джерел та формулювання проблеми

Системам захисту інформації об'єктів критичної інфраструктури присвячено велика кількість наукових робіт. Так у роботі [1] застосовують еволюційний алгоритм NSGA-II для одночасної оптимізації безпеки та якості обслуговування в IoT-мережах ОКІ. Хоча цей підхід дозволяє отримати наближену множину Парето, він не передбачає формалізованого механізму інтеграції суб'єктивних пріоритетів замовника через вагові коефіцієнти, що є ключовою перевагою WSM у практичному проєктуванні. У роботі [2] пропонують модель розподілу кіберзахисних ресурсів у розумних енергомережах на основі ε-обмежень. Цей метод теоретично повніший, оскільки здатен охопити неопуклі Парето-фронти, але є обчислювально складним і важким для інтеграції з класичними техніками оптимізації (LP/NLP), що обмежує його придатність для швидкого прототипування архітектури СЗІ. У роботі [3] автори розробляють гібридну модель AHP-TOPSIS для оцінки кіберризиків. Проте це метод ранжування, а не оптимізації: він використовує скалярну цільову функцію, що не є зручним інструментом мінімізації чи максимізації стандартними оптимізаційними процедурами.

У роботах [5, 4] безпосередньо застосовують WSM – для налаштування систем виявлення вторгнень та розподілу ресурсів у 5G-мережах. Однак обидві роботи не аналізують умови коректності методу: зокрема, вони ігнорують критичне припущення про опуклість Парето-фронту та не надають чіткої процедури нормалізації різнорідних критеріїв (наприклад, ризик у бітах ентропії, витрати в гривнях, затримка в мілісекундах). У роботі [6] здійснюються візуальний аналіз компромісів «безпека–витрати» за допомогою Парето-фронтів, але не пропонують формалізованого механізму перетворення багатокритеріальної задачі на однокритеріальну для подальшого розв'язання. Робота [7] фокусуються на динамічній адаптації у промислових системах за допомогою еволюційних алгоритмів, що робить їх метод надто складним для широкого застосування на етапі первинного проєктування.

Таким чином, усі дослідження підтверджують необхідність збалансованого підходу до оптимізації СЗІ, але лише запропонований у нижче підхід забезпечує: чітке теоретичне обґрунтування застосування WSM за умови опуклості Парето-фронту; системну процедуру попередньої обробки критеріїв (уніфікація напрямків оптимізації, нормалізація); формалізацію реальних обмежень (бюджет, латентність, доступність); та практичну сумісність з класичними методами оптимізації. Це робить роботу науково актуальною та значущою у прикладному контексті проєктування ефективних систем кіберзахисту для об'єктів критичної інфраструктури. У даній роботі розв'язуються **протиріччя** між суперечливими вимогами, що виникають при проєктуванні системи захисту інформації на об'єктах критичної інфраструктури. З одного боку, прагнення до мінімізації ризиків, витрат і затримок обробки даних, а з іншого боку необхідність забезпечення високої доступності та оперативності реагування на кіберзагрози.

Мета роботи та цілі дослідження

Метою дослідження є розробка та обґрунтування методу багатокритеріальної оптимізації системи захисту інформації шляхом застосування методу зваженої суми критеріїв, який дозволяє трансформацію багатокритеріальної задачі, коли потрібно максимізувати або мінімізувати декілька, часто суперечливих, цільових функцій на однокритеріальну скалярну задачу з урахуванням пріоритетів власника інфраструктури. Особлива увага приділяється умовам застосовності методу, зокрема припущенню про опуклість Парето-фронту, що гарантує отримання Парето-оптимальних розв'язків.

Огляд методів знаходження рішень багатокритеріальної оптимізації (Pareto-оптимальність)

Багатокритеріальна оптимізація систем захисту інформації (СЗІ) передбачає, що одночасно маємо справу з кількома конфліктуючими цілями, а саме:

- мінімізація ризику;
- мінімізація витрат;

© Собчук А.В., Лаптєва Т.О., Капустян Д.О., Степанченко Б.С., Лаптєв С.О. Метод оптимізації системи захисту об'єктів критичної інфраструктури за зваженої суми критеріїв. Сучасний захист інформації, 1(65), 54–61. https://doi.org/10.31673/2409-7292.2026.010765

– максимізація доступності;
– мінімізація затримок обробки даних.

Кінцевою метою багатокритеріальної оптимізації є ідентифікація множини Парето-оптимальних розв'язків X^*. Розв'язок $\bar{x}^* \in X^*$ вважається Парето-оптимальним, якщо не існує іншого допустимого розв'язку x', який покращує значення принаймні одного критерію.

Для досягнення цієї мети існують різні методи знаходження множени Парето-оптимальних рішень, самі відомі методи:

– метод зваженої суми;
– метод ε-обмежень;
– метод аналізу ієрархій;
– метод TOPSIS.

Зробимо аналіз цих методів, з метою обрання найкращого для систем захисту інформації:

Метод зваженої суми критеріїв (Weighted Sum Method, WSM). Об'єднує всі цільові функції в одну скалярну за допомогою додатних вагових коефіцієнтів:

$$F(x)=\sum_{i=1}^{k} w_i f_i(x), \quad w_i > 0, \sum w_i = 1. \tag{1}$$

Мінімізується (або максимізується) ця зважена сума. Метод добре працює лише для опуклих Парето-фронтів; не може знайти недоміновані рішення на неопуклих ділянках.

*Метод ε-обмежень (ε-C*onstraint Method*)* Один критерій обирається як основна цільова функція, а решта перетворюються на обмеження: $\min f_j(x)$ за умов $f_i(x) \le \varepsilon_i.\ i \ne j.$

Варіюючи значення ε_i, можна отримати різні точки Парето-фронтів, включаючи неопуклі. Цей метод складніший за попередній, здатний генерувати всю множину Парето-оптимальних розв'язків.

Метод аналізу ієрархій (AHP – Analytic Hierarchy Process). Цей метод побудований на попарному порівнянні критеріїв та альтернатив. Ваги критеріїв визначаються з власного вектора матриці попарних порівнянь. Метод є суб'єктивним (залежить від експертних оцінок), не гарантує отримання Парето-оптимальних розв'язків, але допомагає у ранжуванні альтернатив.

Метод TOPSIS (Technique for Order Preference by Similarity to Ideal Solution). Визначає найкращу альтернативу як ту, що найближча до ідеального рішення (де всі критерії оптимальні) і найдальша від антиідеального (де всі критерії найгірші). Відстані обчислюються зазвичай за Евклідовою метрикою після нормалізації. TOPSIS є методом ранжування, а не прямою технікою пошуку множини Парето.

Виходячи з проведеного аналізу можливо зробити висновок. Що для безпосереднього знаходження множини Парето-оптимальних рішень найбільш придатними є метод ε-обмежень (особливо при неопуклості) та метод зваженої суми (у випадку опуклості). AHP та TOPSIS – це, скоріше, методи ухвалення рішень після формування або апроксимації Парето-множини.

Метод зваженої суми критеріїв (Weighted Sum Method, WSM) є одним із найпоширеніших підходів у багатокритеріальній оптимізації системи захисту інформації (СЗІ) на об'єктах критичної інфраструктури (ОКІ).

Він дозволяє звести векторну цільову функцію до скалярної, об'єднуючи кілька, часто суперечливих, критеріїв в єдиний показник ефективності. Він характеризується простотою реалізації та інтерпретації, його зручно добре використовувати разом з класичними методами оптимізації (LP, NLP, евристики). Метод дозволяє враховувати суб'єктивні пріоритети власника ОКІ через систему ваг w_i.

Відтак, саме метод зваженої суми та будемо розглядати як один з найбільш придатних методів оптимізації системи захисту інформації на об'єктах критичної інфраструктури.

© Собчук А.В., Лаптєва Т.О., Капустян Д.О., Степанченко Б.С., Лаптєв С.О. Метод оптимізації системи захисту об'єктів критичної інфраструктури за зваженої суми критеріїв. Сучасний захист інформації, 1(65), 54–61. https://doi.org/10.31673/2409-7292.2026.010765

Виклад головного матеріалу

Для розгляду методу зваженої суми критеріїв (Weighted Sum Method, WSM) оптимізації системи захисту інформації на об'єктах критичної інфраструктури. Введемо ряд припущень та обмежень.

Нехай система оцінюється за k критеріями:

$$F(x)=(f_1(x), f_2(x),...f_i(x)), \quad x \in X, \tag{2}$$

де x – вектор змінних (наприклад, вибір механізмів захисту, конфігурація IDS/IPS); X – допустима множина розв'язків; $f_i\ (x)$ – значення i-го критерію (може як мінімізовуватись так і максимізовуватись).

Для застосування WSM усі критерії мають бути приведені до однакового напрямку оптимізації, зазвичай мінімізації (якщо критерій максимізується, (наприклад, за критеріями надійності), то замінюємо його на $-f_i(x)$ або на $1/f_i(x)$.

Тоді нова цільова функція будується таким чином:

$$F_{WSM}(x)=\sum_{i=1}^{k} w_i \tilde{f}_i(x), \tag{3}$$

де $\tilde{f}_i(x)$ – нормалізоване (i за потреби, інвертоване) значення i-ого критерію; $w_i \geq 0$ – ваговий коефіцієнт, що відображає важливість i-ого критерію для об'єктів критичної інфраструктури:

$$\sum_{i=1}^{k} w_i = 1.$$

Слід мати на увазі, що вкрай необхідною є нормалізація, оскільки критерії можуть мати різні одиниці виміру (наприклад, гривні, секунди, біти ентропії).

Оптимальне рішення задачі багатокритеріальної оптимізації для об'єкту критичної інфраструктури шукатимемо серед Парето-оптимальних розв'язків, а саме:

$$\overset{*}{x}=\arg\min_{x \in X} \sum_{i=1}^{k} w_i \tilde{f}_i(x). \tag{4}$$

Важливо підкреслити, що допустиму множину рішень (feasible set) у багатокритерійній задачі оптимізації визначають обмеження, зокрема – у контексті проєктування або оцінки інфраструктурних, мережевих чи інформаційно-комунікаційних систем (наприклад, у кібербезпеці чи хмарних обчисленнях).

– Budget $x \leq B_{\max}$ – загальна вартість рішення x (наприклад, вартість розгортання, обладнання, ліцензій, обслуговування) не повинна перевищувати заданий максимальний бюджет $B_{\max}$. Для нашого випадку обмеження на витрати на криптографічні механізми, IDS/IPS, сертифікати тощо;

– Latency $x \leq L_{\max}$ – час затримки (латентність) при виконанні операцій у системі, що реалізується через розв'язок x, має бути не більшим за допустиме значення $L_{\max}$ (наприклад, у мілісекундах). Для СЗІ вплив захисних механізмів на швидкодію мережі (наприклад, затримка через шифрування або інспекцію трафіку);

– Anailability $(x) \geq A_{\min}$ – рівень доступності системи (ймовірність того, що система працює у заданий момент часу) має бути не нижчим за мінімально прийнятний поріг $A_{\min}$ (гарантія того, що система залишається доступною навіть за наявності атак (наприклад, DDoS) або відмов наприклад, 99.9% або 0.999 у діапазоні $[0, 1]$);

Будемо оптимізувати за такими критеріями: перший критерій ризик $R(x)$ потрібно мінімізувати, другий критерій витрати $C(x)$ слід мінімізувати, третій критерій час реагування $T(x)$ теж мінімізувати.

© Собчук А.В., Лаптєва Т.О., Капустян Д.О., Степанченко Б.С., Лаптєв С.О. Метод оптимізації системи захисту об'єктів критичної інфраструктури за зваженої суми критеріїв. Сучасний захист інформації, 1(65), 54–61. https://doi.org/10.31673/2409-7292.2026.010765

Вагові коефіцієнти нехай мають значення: $w_R = 0.5$, $w_C = 0.3$, $w_T = 0.2$.

Після нормалізації, згідно (3) отримуємо:

$$F_{WSM}(x) = 0.5\tilde{R}(x) + 0.3\tilde{C}(x) + 0.2\tilde{T}(x). \quad (5)$$

Задачею оптимізації системи кіберзахисту об'єкта критично інфраструктури є побудова таки рубежів захисту $\overset{*}{x}$, що мінімізує $F_{WSM}(x)$ за умови, що загальний бюджет орієнтовно становить 5-10 млн грн і час реагування не перевищує 10-15 с.

Для отримання розв'язку даної задачі реалізовано алгоритм, представлений нижче за допомогою програмного коду (рис. 1 – рис. 3).

```
# ----------------------------
# 1. Визначення критеріальних функцій
# ----------------------------
def R(x):
    """Ризик: зменшується зі зростанням x"""
    return 100.0 / (1.0 + x)

def C(x):
    """Витрати (млн грн): зростають зі зростанням x"""
    return 0.8 * x ** 1.5

def T(x):
    """Час реагування (сек): зменшується зі зростанням x"""
    return 20.0 / (1.0 + 0.3 * x)
```

Рис.1. Фрагмент програмного коду визначення обмежень

```
# 2. Нормалізація (мінімаксна на дискретній множині)
# ----------------------------
def normalize(values):
    """Мінімаксна нормалізація до [0, 1]"""
    vmin, vmax = np.min(values), np.max(values)
    if vmax == vmin:
        return np.zeros_like(values)
    return (values - vmin) / (vmax - vmin)

# ----------------------------
# 3. Основна функція оптимізації
# ----------------------------
def optimize_scenarios():
    wR, wC, wT = 0.5, 0.3, 0.2
    x_vals = np.arange(1, 51)  # рівні захисту від 1 до 50

    # Обчислюємо всі критерії
    R_vals = np.array([R(x) for x in x_vals])
    C_vals = np.array([C(x) for x in x_vals])
    T_vals = np.array([T(x) for x in x_vals])
```

Рис.2. Код нормалізації та функції оптимізації

© Собчук А.В., Лаптєва Т.О., Капустян Д.О., Степанченко Б.С., Лаптєв С.О. Метод оптимізації системи захисту об'єктів критичної інфраструктури за зваженої суми критеріїв. Сучасний захист інформації, 1(65), 54–61. https://doi.org/10.31673/2409-7292.2026.010765

```
# Знаходимо мінімум зваженої суми серед допустимих
best_idx_local = np.argmin(feasible_F)
x_opt = feasible_x[best_idx_local]
r_opt = R(x_opt)
c_opt = C(x_opt)
t_opt = T(x_opt)
f_opt = feasible_F[best_idx_local]

results.append((idx, x_opt, r_opt, c_opt, t_opt, f_opt, budget, t_max))
```

Рис.3. Розв’язок задачі багатокритеріальної оптимізації

Результати моделювання методом зваженої суми критеріїв для різних сценаріїв бюджетних витрат на об’єкт критичної інфраструктури та часу реакції представлено на рис.4 – рис. 6)

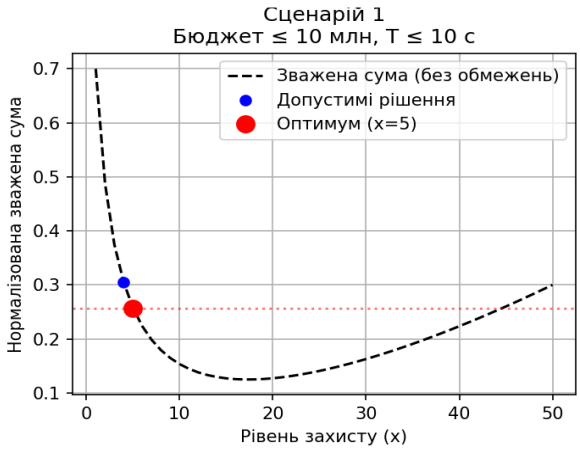

Рис.4. Графічні результат для першого сценарію

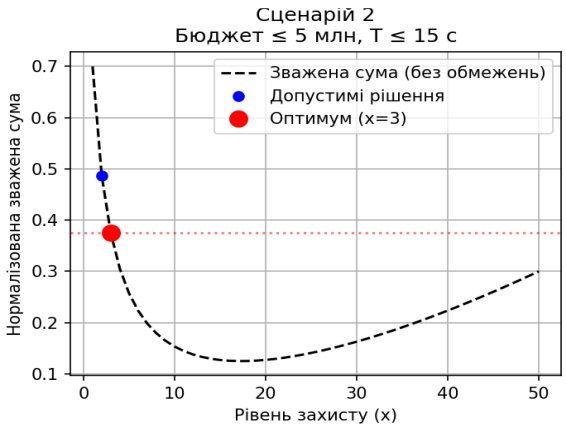

Рис.5. Графічні результат для другого сценарію

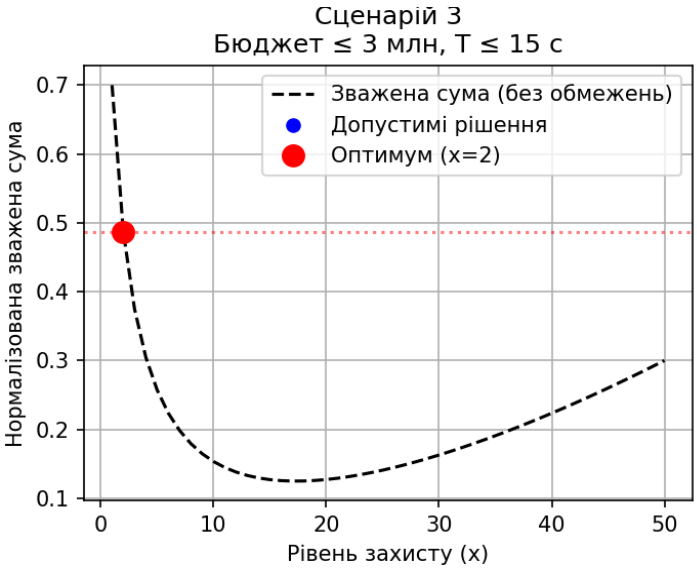

Рис.6. Графічні результат для третього сценарію

© Собчук А.В., Лаптєва Т.О., Капустян Д.О., Степанченко Б.С., Лаптєв С.О. Метод оптимізації системи захисту об’єктів критичної інфраструктури за зваженої суми критеріїв. Сучасний захист інформації, 1(65), 54–61. https://doi.org/10.31673/2409-7292.2026.010765

Таблиця 1

Аналітичні результати моделювання процесу оптимізації за запропонованими сценаріями

Сценарій	x^*	Ризик $R(x^*)$	Витрати $C(x^*)$	Час $T(x^*)$	$F(x^*)$
1	5	16.67	8.94	8.00	0.2572
2	3	25.00	4.16	10.53	0.3746
3	2	33.33	2.26	12.50	0.4873

Аналіз отриманих графічних результатів рис.4 – рис. 6 та даних таблиці 1, наочно доводить застосовність запропонованого методу. Як бачимо з наведених графіків метод зваженої суми критеріїв надає можливість за рахунок оптимізації суттєво зберегти кошти, при цьому не погіршує систему захисту об'єкта. Для промодельованих трьох сценаріїв за рахунок оптимізації отримали економічний ефект від 0,5 до 1,5 млн. грн.

Таким чином розроблений метод надає можливість оперативно обирати оптимальне рішення, у нашому випадку за критеріями кошторисної вартості, рівнем захисту та часом реагування для захисту об'єктів критичної інфраструктури, спираючись на дані близькі до реальних.

Висновки

У статті обґрунтовано актуальність застосування методу зваженої суми критеріїв для багатокритеріальної оптимізації системи захисту інформації на об'єктах критичної інфраструктури, де одночасно враховуються такі мало сумісні цілі, як мінімізація ризиків, витрат і затримок обробки даних, та водночас максимізується задача доступності та оперативності реагування на кіберзагрози. Проведений аналіз альтернативних підходів до багатокритеріальної оптимізації – зокрема, методів ε-обмежень, аналізу ієрархій (AHP) та TOPSIS – дозволив обґрунтувати доцільність використання саме методу зваженої суми у випадку опуклості Парето-фронту, що характерно для багатьох практичних сценаріїв у сфері кібербезпеки. Метод зваженої суми критеріїв вирізняється обчислювальною ефективністю, сумісністю з класичними техніками оптимізації (лінійного, нелінійного програмування, евристичних алгоритмів) та здатністю враховувати суб'єктивні пріоритети власника інфраструктури через налаштування вагових коефіцієнтів.

Для коректного застосування методу зваженої суми запропоновано необхідні етапи попередньої обробки: уніфікація напрямків оптимізації, нормалізація значень критеріїв, що вимірюються в різних одиницях, та формалізація обмежень, пов'язаних із бюджетом, латентністю та рівнем доступності. На прикладі трьох ключових критеріїв – ризик, витрати та час реагування – продемонстровано, як формується скалярна цільова функція, яка мінімізується в периметрах заданих обмежень, характерних для реальних об'єктів критичної інфраструктури.

Отримані результати свідчать про те, що метод зваженої суми критеріїв є не лише теоретично обґрунтованим, а й практично придатним інструментом для прийняття зважених рішень у проєктуванні систем захисту інформації. Його застосування дозволяє отримувати Парето-оптимальні конфігурації захисних механізмів, які гармонійно поєднують безпеку, економічну доцільність та функціональну ефективність. Відтак, даний підхід доцільно використовувати на етапі первинного проєктування або швидкого прототипування

© Собчук А.В., Лаптєва Т.О., Капустян Д.О., Степанченко Б.С., Лаптєв С.О. Метод оптимізації системи захисту об'єктів критичної інфраструктури за зваженої суми критеріїв. Сучасний захист інформації, 1(65), 54–61. https://doi.org/10.31673/2409-7292.2026.010765

архітектури системи захисту інформації, де потрібна швидка оцінка компромісів між цілями, які конфліктуються, а не повний перебір усіх можливих варіантів альтернатив.

Перелік посилань

1. Almiani, M., et al. (2021). "Multi-objective optimization for security and QoS in IoT-based critical infrastructure." Computers & Security, 103, 102167. DOI: 10.1016/j.cose.2021.102167.

2. Khan, R., et al. (2020). "A Pareto-based approach for cybersecurity resource allocation in smart grids." IEEE Transactions on Smart Grid, 11(5), 4234–4245. DOI: 10.1109/TSG.2020.2985432.

3. Sharma, S., & Trivedi, M. C. (2022). "AHP-TOPSIS hybrid model for cybersecurity risk assessment in critical infrastructure." Journal of Information Security and Applications, 68, 103235. DOI: 10.1016/j.jisa.2022.103235.

4. Wang, Y., et al. (2023). "Multi-objective optimization of intrusion detection systems using weighted sum and machine learning." Expert Systems with Applications, 213, Part A, 118923. DOI: 10.1016/j.eswa.2022.118923.

5. García, J. M., et al. (2021). "Security-cost trade-off analysis in critical information infrastructures using Pareto fronts." Reliability Engineering & System Safety, 216, 107923. DOI: 10.1016/j.ress.2021.107923.

6. Li, X., et al. (2024). "Dynamic multi-objective optimization for adaptive cybersecurity in industrial control systems." IEEE Transactions on Industrial Informatics, 20(2), 1654–1665. DOI: 10.1109/TII.2023.3308765.

7. Chen, H., et al. (2020). "Weighted-sum based security-aware resource allocation in 5G-enabled critical infrastructures." IEEE Access, 8, 134567-134579.

8. Лаптєв О.А., Собчук В.В., Савченко В.А. Метод підвищення завадостійкості системи виявлення, розпізнавання і локалізації цифрових сигналів в інформаційних системах. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. ВІКНУ, 2019. Вип. 66. С. 124-132.

9. Yevseiev, S., Khokhlachova, Yu., Ostapov, S., Laptiev, O., Korol, O., Milevskyi, S. et. al. 2023. "Models of socio-cyber-physical systems security," Monographs, PC TECHNOLOGY CENTER, 168p. http://doi.org/10.15587/978-617-7319-72-5.

10. O. Laptiev, V. Sobchuk, A. Ryzhov, A. Sobchuk, S. Kopytko and G. Shuklin. Harmonic Operators in Mathematical Models of Sources of Detection of Unauthorized Access to Information, 6 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA 2024), Istanbul, Turkiye, 2024, P. 1-6. https://doi.org/10.1109/HORA61326.2024.10550552. Scopus.

11. Олександр Лаптєв, Валентин Собчук, Олег Барабаш, Андрій Мусієнко. Метод визначення параметрів радіозакладних пристроїв з використанням диференціальних перетворень. V Міжнародна науково-практична конференція. “Проблеми кібербезпеки інформаційно-телекомунікаційних систем” (PCSITS)”27-28 жовтня 2022 р. м. Київ, Україна. Збірник матеріалів доповідей та тез. С 63-65.

12. Лаптєв О.А., Марченко В.В. Застосування завад для захисту інформації від витоку радіоканалом. Сучасний захист інформації. 2025. №1. С.89-97. https://doi.org/10.31673/2409-7292.2025.013057

Надійшла до редакції (Received): 29.01.2026
Прийнята до друку (Accepted): 17.03.2026
Опубліковано онлайн (Available online): 30.03.2026

УДК 347.78:004.056(4-6ЄС)
DOI: 10.31673/2409-7292.2026.010831

Лаптев О.А., Браіловський М.М., Хорошко Г.О.

АВТОРСЬКЕ ПРАВО У ЦИФРОВОМУ ПРОСТОРІ ЄС В КОНТЕКСТІ КІБЕРБЕЗПЕКИ

У статті досліджено взаємозв’язок авторського права та кібербезпеки в умовах цифрової трансформації суспільства. Авторське право розглядається не лише як правовий механізм охорони інтелектуальної власності, а й як інтегральний компонент системи кібербезпеки, що забезпечує цілісність, конфіденційність та легітимність використання цифрових об’єктів. Особливу увагу приділено проблемам захисту програмного забезпечення, баз даних та мультимедійного контенту від цифрового піратства, несанкціонованого копіювання та модифікації. Розглянуто сучасні технічні засоби реалізації авторських прав – системи цифрового управління правами (DRM-

© Собчук А.В., Лаптєва Т.О., Капустян Д.О., Степанченко Б.С., Лаптєв С.О. Метод оптимізації системи захисту об’єктів критичної інфраструктури за зваженої суми критеріїв. Сучасний захист інформації, 1(65), 54–61. https://doi.org/10.31673/2409-7292.2026.010765