КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.34.1389
УДК 004.056:681.5

Жебка Вікторія Вікторівна
доктор технічних наук, професор, завідувачка кафедри Технологій цифрового розвитку
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0000-0003-4051-1190
v.zhebka@duikt.edu.ua

Аронов Андрій Олексійович
кандидат технічних наук, доцент кафедри технологій цифрового розвитку,
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0009-0000-7868-8341
a.aronov@duikt.edu.ua

Ніщеменко Дмитро Олександрович
доктор філософії, викладач кафедри Технологій цифрового розвитку,
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0009-0006-1781-4109
d.nishchemenko@duikt.edu.ua

Ананченко Олексій Євгенович
к.т.н, доцент кафедри технологій цифрового розвитку
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID:0009-0005-3446-5994
o.ananchenko@duikt.edu.ua

УДОСКОНАЛЕННЯ МЕТОДУ БАГАТОЦІЛЬОВОЇ ОПТИМІЗАЦІЇ КЕРУВАННЯ IoT-СИСТЕМОЮ РОЗУМНОГО БУДИНКУ З УРАХУВАННЯМ КІБЕРРИЗИКУ

Анотація. Розвиток технологій Інтернету речей та систем розумного будинку супроводжується збільшенням кількості автоматизованих рішень, що приймаються на основі інформації від сенсорів. Достовірність цих даних безпосередньо впливає на якість керування, оскільки помилкові або навмисно змінені значення можуть призвести до формування нераціональних керуючих дій. У статті запропоновано удосконалення методу багатоцільової оптимізації керування IoT-системою розумного будинку шляхом додаткового врахування кіберризику. За основу прийнято модель проактивного керування, в якій вибір дії здійснюється на основі оцінювання комфорту користувача та енергоефективності. Для підвищення стійкості системи до спотворення сенсорних даних до функції корисності введено додаткову складову, яка залежить від рівня недовіри до отриманого значення та можливого впливу керуючої дії на стан системи. Рівень недовіри визначається на основі відхилення поточного сенсорного значення від довіреної оцінки контрольованого параметра. Для перевірки запропонованого підходу використано імітаційне моделювання процесу керування температурою приміщення. Проведено порівняння базового та удосконаленого методів у штатному режимі та за умов навмисного заниження показників температурного сенсора. Результати моделювання показали, що врахування кіберризику дозволяє суттєво зменшити кількість помилкових керуючих дій та зберегти температурний комфорт на рівні, близькому до штатної роботи системи. У модельному сценарії частка часу в зоні температурного комфорту зросла з 89,50 % для базового алгоритму зі спотворенням даних до 99,66 % для удосконаленого, а середня кількість ризикових команд зменшилася з 184,37 до 4,63. Запропоноване удосконалення не потребує істотної зміни архітектури програмної системи та може бути реалізоване шляхом модифікації функції оцінювання альтернативних керуючих дій.

Ключові слова: розумний будинок; Інтернет речей; кіберризик; багатоцільова оптимізація; керування; сенсорні дані; проактивне керування; імітаційне моделювання

ВСТУП

Постановка проблеми. Системи розумного будинку використовують дані сенсорів для автоматизованого керування опаленням, освітленням, енергоспоживанням та іншими підсистемами. Зі збільшенням рівня автоматизації зростає залежність результатів керування від достовірності вхідної інформації. Помилки сенсорів, порушення передавання даних або їх навмисна зміна можуть призвести до прийняття некоректних рішень. Особливо важливою ця проблема є для проактивного керування, коли система прогнозує наслідки декількох можливих дій і автоматично обирає найбільш доцільну. У такому випадку спотворене вхідне значення може призвести до формально правильного з точки зору алгоритму, але неправильного з точки зору фактичного стану об'єкта рішення.

Аналіз останніх досліджень і публікацій. У сучасних дослідженнях систем розумного будинку значна увага приділяється оптимізації енергоспоживання, підвищенню комфорту користувача, обробці сенсорних даних та виявленню їх аномальних значень [1] – [6]. Окремі роботи розглядають методи виявлення аномалій та підвищення надійності сенсорних даних [7] – [8], а також оптимізацію параметрів мікроклімату та енергоспоживання [9] – [10]. Для проактивного керування застосовуються контекстно-залежні моделі та багатоцільова оптимізація [11] – [12]. Водночас безпосереднє врахування ризику використання недостовірних сенсорних даних у функції вибору керуючої дії потребує подальшого розвитку.

Мета статті. Метою статті є удосконалення методу багатоцільової оптимізації керування IoT-системою розумного будинку шляхом введення додаткового критерію кіберризику, що дозволяє враховувати можливе спотворення сенсорних даних під час вибору керуючої дії.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

За основу удосконалення прийнято проактивний підхід до керування розумним будинком, відповідно до якого система на кожному часовому кроці формує множину допустимих керуючих дій, прогнозує результат їх виконання та обирає дію, що забезпечує максимальне значення функції корисності [11, 12]. У вихідній моделі основними критеріями є температурний комфорт користувача та енергоефективність. Така модель дозволяє відмовитися від жорстко заданих правил та здійснювати вибір рішення відповідно до поточного стану середовища і встановлених пріоритетів.

Стан середовища в момент часу t подамо вектором:

$$S_t = \left(T_{in,t}, T_{out,t}, H_t, C_t\right) \tag{1}$$

де $T_{in,t}$ – внутрішня температура приміщення; $T_{out,t}$ – зовнішня температура; H_t – поточний час; C_t – параметр, що характеризує тариф на електроенергію. Для кожного стану системи формується множина допустимих керуючих дій. Для підсистеми опалення в роботі використано три режими: вимкнення, 50% та 100% потужності.

Прогнозований стан після виконання певної дії визначається функцією:

$$S'_{t+1} = P(S_t, a) \tag{2}$$

де P – модель зміни стану середовища, а a – одна з допустимих керуючих дій. Для кожної дії визначається прогноз температури та відповідні показники комфорту й енергоефективності.

У базовому методі функція корисності формується на основі двох критеріїв:

$$U_0 = w_c S_c + w_e S_e \tag{3}$$

де S_c – оцінка температурного комфорту; S_e – оцінка енергоефективності; w_c та w_e – вагові коефіцієнти, причому $w_c + w_e = 1$. Ваги можуть змінюватися залежно від контексту: у вечірній час більшу вагу отримує комфорт, а під час високого тарифу збільшується значення енергоефективності. Такий принцип відповідає базовій моделі проактивного керування [12].

Недоліком такої постановки при використанні в IoT-середовищі є припущення про достовірність отриманих даних. Наприклад, якщо фактична температура приміщення становить 21 °C, але контролер унаслідок помилки або навмисного спотворення отримує значення 16 °C, базовий алгоритм може обрати

максимальну потужність обігріву. У результаті спотворення інформації безпосередньо переходить у фізичну дію системи. Механізм поширення спотворення сенсорних даних у керуючу дію та місце застосування довіреної оцінки для його стримування наведено на рис. 1.

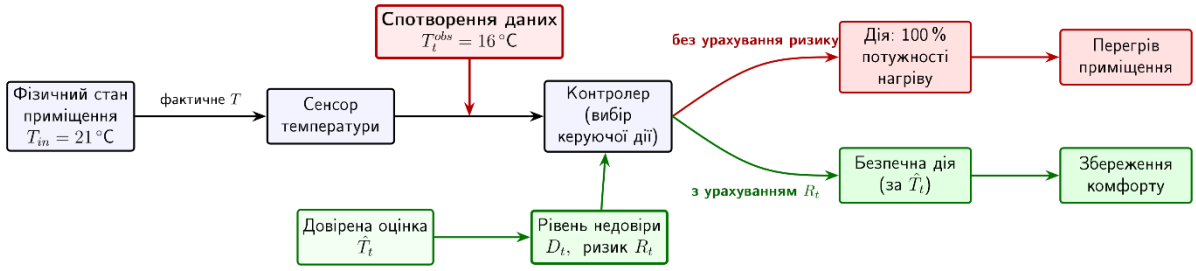

Рис. 1. Модель поширення спотворення сенсорних даних у керуючу дію та точка застосування довіреної оцінки

Для врахування цієї ситуації запропоновано використовувати довірену оцінку контрольованого параметра $\hat{T}_t$. Вона може формуватися на основі попереднього стану, прогнозної моделі, резервного сенсора або результатів попередньої обробки даних. У межах цієї роботи не ставиться задача створення окремого складного методу виявлення кібератак; необхідно лише кількісно оцінити відхилення поточного сенсорного значення від очікуваного.

Рівень недовіри до отриманого значення пропонується визначати таким чином:

$$D_t = \min\left(1, \frac{\left|T_t^{obs} - \hat{T}_t\right|}{\Delta T_{crit}}\right) \tag{4}$$

де T_t^{obs} – значення, отримане від сенсора; $\hat{T}_t$ – довірена оцінка; ΔT_{crit} – граничне відхилення, після досягнення якого рівень недовіри приймається максимальним. При близьких значеннях сенсорного вимірювання та довіреної оцінки D_t наближається до нуля. Зі збільшенням розбіжності значення D_t зростає до одиниці. Характер зміни рівня недовіри залежно від величини відхилення сенсорного значення від довіреної оцінки показано на рис. 2.

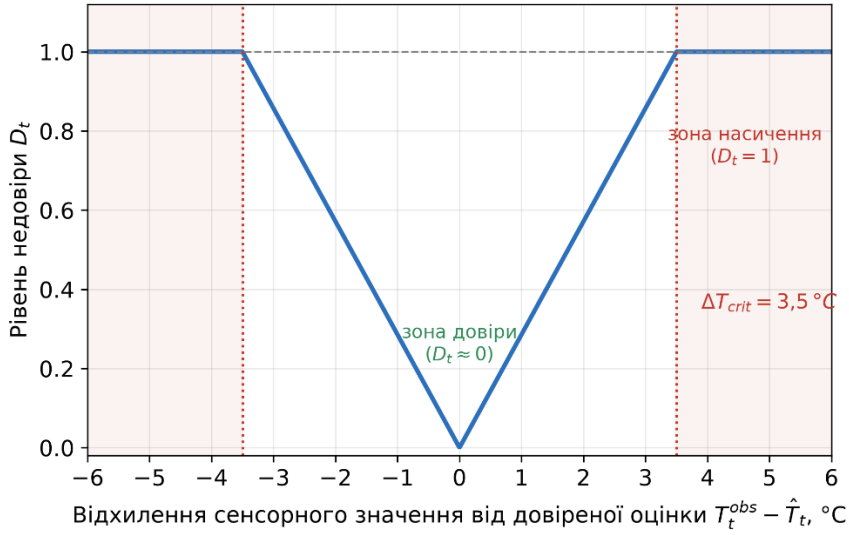

Рис. 2. Залежність рівня недовіри D_t від відхилення сенсорного значення від довіреної оцінки (ΔT_{crit} = 3,5 °C)

У модельному експерименті довірена оцінка температури формувалася прогнозною моделлю на основі попереднього стану системи, а безпечна дія визначалася базовим оптимізатором із використанням цієї оцінки.

Додатково враховується можливий вплив керуючої дії. На основі довіреної оцінки стану визначається безпечна дія a_t^{safe}, а ризик потенційної дії пропонується оцінювати як:

$$R_t = D_t \cdot \frac{|p(a_t) - p(a_t^{safe})|}{p_{max}} \quad (5)$$

де $p(a_t)$ – потужність потенційної дії; $p(a_t^{safe})$ – потужність дії, сформованої за довіреною оцінкою стану; p_{max} – максимальна потужність виконавчого пристрою. Якщо потенційна і безпечна дії збігаються, ризик дорівнює нулю. Чим більшою є недовіра до сенсорних даних і відмінність між діями, тим більшим стає значення R_t. Спільний вплив рівня недовіри та нормованої відмінності потенційної і безпечної дій на величину штрафу ілюструє рис. 3.

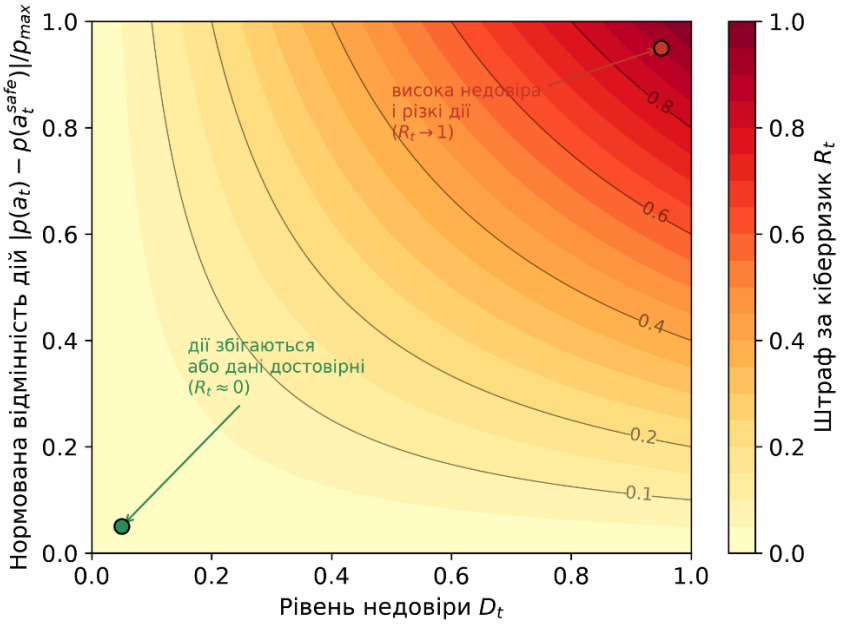

Рис. 3. Залежність штрафу за кіберризик R_t від рівня недовіри та нормованої відмінності потенційної і безпечної керуючих дій

З урахуванням введеного критерію базова функція корисності набуває вигляду:

$$U = w_c S_c + w_e S_e - w_r R_t \quad (6)$$

де w_r – коефіцієнт чутливості системи до кіберризику. На відміну від w_c та w_e, цей коефіцієнт не характеризує переваги користувача, а визначає силу штрафу за ризикову дію. При $D_t = 0$ ризикова складова також дорівнює нулю, тому удосконалена модель фактично переходить до базового варіанта. Отже, загальний принцип багатоцільової оптимізації не змінюється: система перебирає можливі дії та обирає дію з найбільшим значенням функції корисності, але за наявності ознак недостовірності інформації потенційно небажані дії отримують додатковий штраф.

Програмна реалізація такого удосконалення не потребує зміни загальної структури агента. Достатньо додати обчислення рівня недовіри, оцінку відмінності керуючих дій та третю складову функції корисності.

Фрагмент реалізації мовою Python наведено нижче.

```
def calc_util(comf, en, obs_t, trust_t, act, safe_act):
    distrust = min(1.0, abs(obs_t - trust_t) / dt_crit)
    impact = abs(power[act] - power[safe_act]) / max_power
    risk = distrust * impact
    return w_comf * comf + w_en * en - w_risk * risk
```

Узагальнену структурну схему удосконаленого методу багатоцільової оптимізації керування з урахуванням кіберризику наведено на рис. 4.

Рис. 4. Структурна схема удосконаленого методу багатоцільової оптимізації керування з урахуванням кіберризику

Деталізовану послідовність обчислень, що виконуються на кожному часовому кроці під час вибору керуючої дії, наведено на рис. 5. Для кожної допустимої дії обчислюються рівень недовіри (4), штраф за кіберризик (5) та значення функції корисності (6), після чого обирається дія з максимальним значенням U.

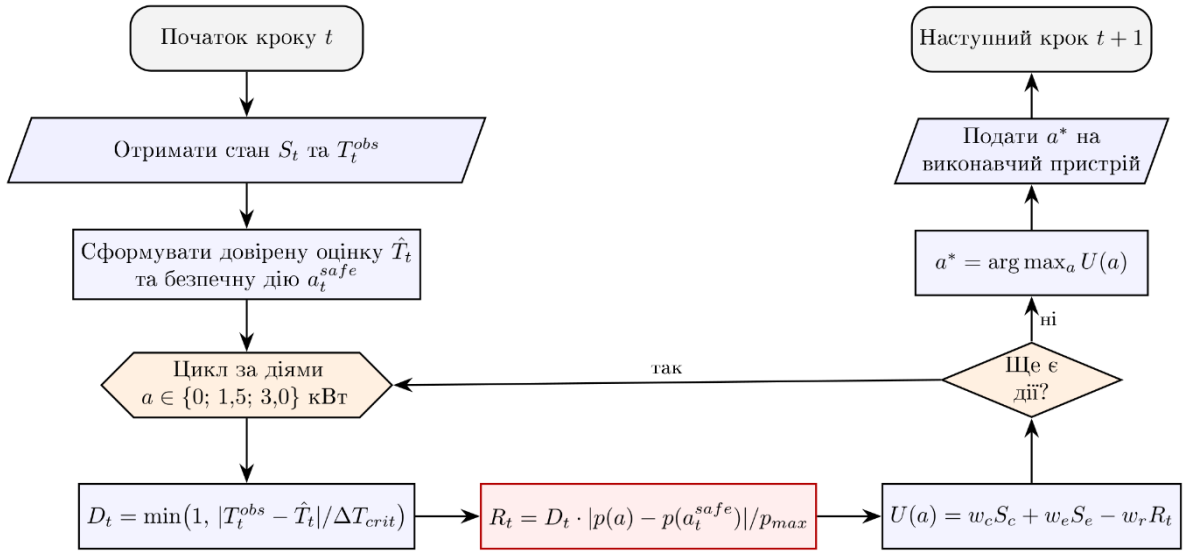

Рис. 5. Блок-схема алгоритму вибору керуючої дії на одному часовому кроці з урахуванням кіберризику

Для оцінювання запропонованого удосконалення використано імітаційний сценарій керування температурою однієї умовної житлової кімнати. Тривалість одного експерименту становила 60 діб, стан системи оновлювався з кроком 15 хвилин, тому кожний прогін містив 5760 часових кроків. Перші 30 діб відповідали помірнішим зовнішнім умовам, наступні 30 діб – холоднішому періоду. Така структура зберігає загальний принцип експериментального стенду, використаного для перевірки проактивного керування у попередньому дослідженні [12]. Параметри термодинамічної моделі обрано відповідно до базового імітаційного стенду.

Основні параметри імітаційного сценарію зафіксовано однаковими для всіх порівнюваних варіантів та наведено у Таблиці 1.

Таблиця 1

Основні параметри імітаційного моделювання

Параметр	Значення
Тривалість одного прогону	60 діб
Крок моделювання	15 хв
Кількість часових кроків	5760
Кількість повторень	30
Зона температурного комфорту	20-22 °C
Режими роботи обігрівача	0; 1,5; 3,0 кВт
Високий тариф	17:00-22:00
Частка інтервалів зі спотворенням	близько 8 %
Заниження температури	2-5 °C
ΔT_{crit}	3,5 °C
w_r	20

Коефіцієнт w_r є штрафним коефіцієнтом чутливості системи до кіберризику та не нормується разом із ваговими коефіцієнтами w_c і w_e.

Спотворення даних моделювалося шляхом періодичного заниження показника внутрішньої температури на 2-5 °C. Тривалість окремих інтервалів становила від однієї до чотирьох годин, а сумарна частка таких інтервалів у середньому становила близько 8 %. Подібний принцип контрольованого внесення спотворень у сенсорні дані є поширеним при експериментальній перевірці алгоритмів виявлення аномалій та очищення даних [2], [7], [8].

Розглянуто три сценарії: базовий алгоритм без спотворення сенсорних даних; базовий алгоритм за наявності спотворення; удосконалений алгоритм за ідентичного спотворення. Основними показниками порівняння обрано частку часу в зоні температурного комфорту, умовні енергетичні витрати, частку часу перегріву й переохолодження та кількість ризикових команд. Ризиковою вважалася команда максимального нагріву, сформована під час спотворення даних за фактичної температури не нижче 20 °C. Кожен сценарій повторено 30 разів із різними початковими значеннями генератора випадкових чисел.

Результати наведено у Таблиці 2.

Таблиця 2

Результати порівняння методів керування

Показник	Без спотворення	Базовий зі спотворенням	Удосконалений зі спотворенням
Комфорт, % часу	100,00 ± 0,00	89,50 ± 0,29	99,66 ± 0,23
Ризикові команди, к-ть	0	184,37 ± 11,54	4,63 ± 2,03
Перегрів, % часу	0	10,50 ± 0,29	0,31 ± 0,24
Переохолодження, % часу	0	0	0,03 ± 0,03
Умовні витрати, у.о.	1990,21 ± 4,36	2030,61 ± 15,62	1987,95 ± 3,18

Графічне порівняння середньої кількості ризикових керуючих команд для досліджуваних сценаріїв наведено на рис. 6.

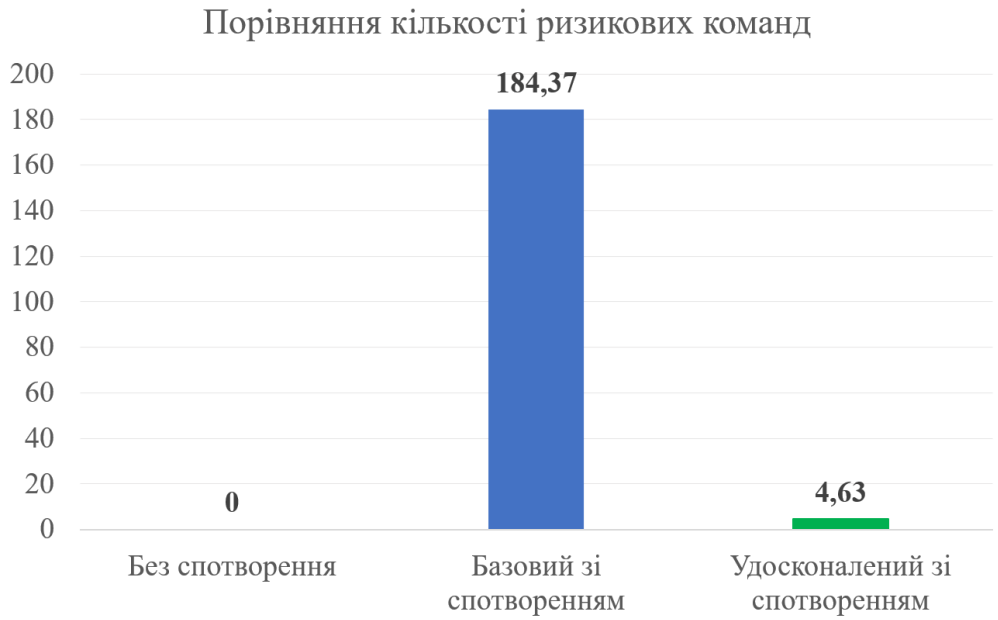

Рис. 6. Порівняння середньої кількості ризикових керуючих команд для досліджуваних сценаріїв

Узагальнене порівняння температурних показників та умовних енергетичних витрат для трьох досліджуваних сценаріїв наведено на рис. 7.

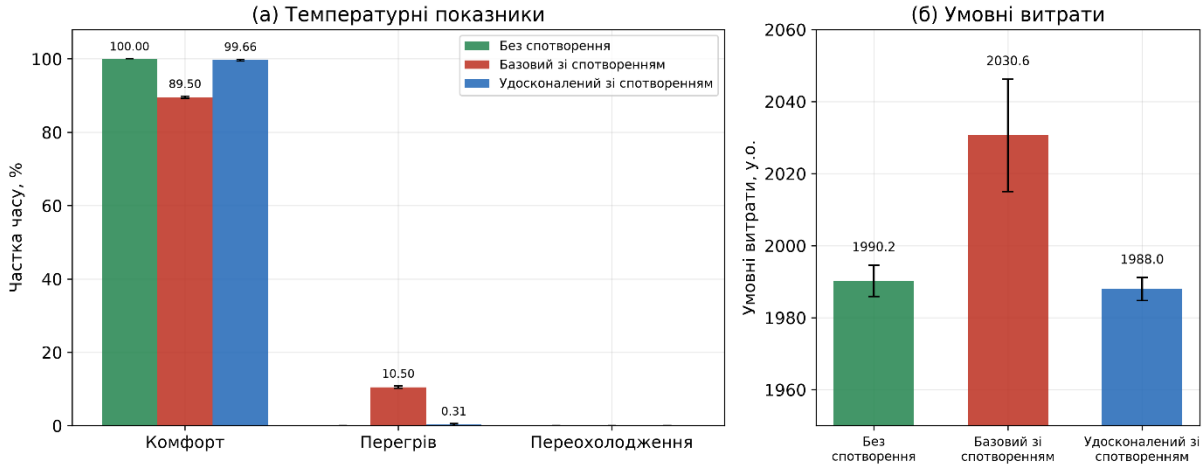

Рис. 7. Порівняння показників якості керування для трьох сценаріїв: (а) температурні показники (частка часу в зоні комфорту, перегріву та переохолодження); (б) умовні енергетичні витрати

За штатного функціонування базовий метод забезпечив перебування температури в заданому діапазоні в середньому протягом 100,00% часу. Після внесення спотворень цей показник зменшився до 89,50%. Основною причиною стало те, що занижене значення температури змушувало базовий алгоритм частіше обирати максимальну потужність обігріву, що призводило до подальшого перегріву приміщення.

Найбільш показовою є кількість ризикових керуючих дій. Для базового алгоритму за умов спотворення їх середня кількість становила 184,37 за один 60-добовий прогін. Після додавання критерію кіберризику середня кількість таких команд зменшилася до 4,63. Таким чином, у розглянутому модельному сценарії запропоноване удосконалення забезпечило зменшення кількості ризикових команд на 97,49%. Відносне зменшення визначається як:

$$\eta = \frac{184{,}37 - 4.63}{184{,}37} \cdot 100\% = 97{,}49\% \qquad (7)$$

Частка часу в зоні комфорту для удосконаленого алгоритму становила 99,66%, тобто практично відповідала штатному режиму. Частка часу перегріву при застосуванні базового алгоритму зі спотвореними даними становила 10,50%, тоді як для удосконаленого методу вона зменшилася до 0,31%. Переохолодження для удосконаленого методу становило лише 0,03% часу.

Умовні витрати для базового алгоритму за умов спотворення збільшилися з 1990,21 до 2030,61 у.о., тобто приблизно на 2,03 %. При застосуванні удосконаленого методу вони становили 1987,95 у.о. і практично відповідали штатному рівню. Отриманий результат пояснюється тим, що алгоритм не блокує автоматичне керування, а зменшує привабливість керуючих дій, які суттєво відрізняються від рішення, сформованого за довіреною оцінкою стану.

Результати підтверджують доцільність введення додаткового критерію до процесу вибору керуючої дії. При невеликій розбіжності між сенсорним і прогнозованим значеннями система працює майже так само, як базова. При збільшенні рівня недовіри зростає штраф за потенційно ризикові дії, що дозволяє зменшити вплив недостовірної інформації на фізичний стан об’єкта. Практичною перевагою є простота інтеграції: базові компоненти прогнозування, контекстного визначення ваг і перебору дій можуть залишатися без змін.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті запропоновано удосконалення методу багатоцільової оптимізації керування IoT-системою розумного будинку шляхом додаткового врахування кіберризику під час вибору керуючої дії. На відміну від базового підходу, що використовує критерії комфорту та енергоефективності, до функції корисності введено складову, яка враховує рівень недовіри до поточних сенсорних даних та відмінність потенційної дії від безпечного рішення.

Результати імітаційного моделювання показали, що навмисне спотворення температурних даних може суттєво погіршити роботу базового алгоритму. У розглянутому сценарії частка часу в зоні комфорту зменшилася зі 100,00% до 89,50%, а середня кількість ризикових керуючих дій становила 184,37 за 60 діб. Використання удосконаленого методу дозволило забезпечити 99,66% часу в зоні комфорту та скоротити середню кількість ризикових дій до 4,63, що відповідає зменшенню на 97,49%. При цьому умовні витрати практично відповідали штатному режиму.

Запропонований підхід має просту програмну реалізацію та може бути інтегрований до існуючої проактивної архітектури без суттєвої зміни її основних компонентів. Перспективами подальших досліджень є використання складніших способів формування довіреної оцінки стану, одночасне врахування інформації від декількох сенсорів, адаптивне визначення коефіцієнта кіберризику, а також перевірка методу на реальному апаратно-програмному стенді розумного будинку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010
2. Karkouch, A., Mousannif, H., Al Moatassime, H., & Noel, T. (2016). Data quality in Internet of Things: A state-of-the-art survey. Journal of Network and Computer Applications, 73, 57–81. https://doi.org/10.1016/j.jnca.2016.08.002
3. Zhang, A., Song, S., Wang, J., & Yu, P. S. (2017). Time series data cleaning: From anomaly detection to anomaly repairing. Proceedings of the VLDB Endowment, 10(10), 1046–1057. https://doi.org/10.14778/3115404.3115410
4. Chahuara, P., Portet, F., & Vacher, M. (2017). Context-aware decision making under uncertainty for voice-based control of smart home. Expert Systems with Applications, 75, 63–79. https://doi.org/10.1016/j.eswa.2017.01.014
5. Cotti, L., Guizzardi, D., Barricelli, B. R., & Fogli, D. (2024). Enabling end-user development in smart homes: A machine learning-powered digital twin for energy efficient management. Future Internet, 16(6), 208. https://doi.org/10.3390/fi16060208
6. Dobrovolskis, A., Kazanavičius, E., & Kižauskienė, L. (2023). Building XAI-based agents for IoT systems. Applied Sciences, 13(6), 4040. https://doi.org/10.3390/app13064040
7. Ahmad, R., & Alkhammash, E. H. (2024). Online adaptive Kalman filtering for real-time anomaly detection in wireless sensor networks. Sensors, 24(15), 5046. https://doi.org/10.3390/s24155046

8. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), 1–58. https://doi.org/10.1145/1541880.1541882
9. Khan, A. N. (2023). An OCF-IoTivity enabled smart-home optimal indoor environment control system for energy and comfort optimization. Internet of Things, 22, 100712. https://doi.org/10.1016/j.iot.2023.100712
10. Khan, Q. W., Ahmad, R., Rizwan, A., Khan, A., Lee, K., & Kim, D. (2024). Optimizing energy efficiency and comfort in smart homes through predictive optimization: A case study with indoor environmental parameter consideration. Energy Reports, 11, 5619–5637. https://doi.org/10.1016/j.egyr.2024.05.038
11. Ніщеменко, Д. О., & Аронов, А. О. (2025). Дослідження методик оптимізації параметрів системи керування розумним будинком з використанням IoT. Телекомунікаційні та інформаційні технології, 1, 141–150. https://doi.org/10.31673/2412-4338.2025.013027
12. Ніщеменко, Д. О., & Олейніков, І. А. (2025). Проактивна архітектура керування розумним будинком на основі контекстуальних намірів користувача та багатоцільової оптимізації. Телекомунікаційні та інформаційні технології, 3, 141–149. https://doi.org/10.31673/2412-4338.2025.038716

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

Viktoriia Zhebka
Doctor of Technical Sciences, Professor, Head of the Department of Digital Development Technologies
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0000-0003-4051-1190
v.zhebka@duikt.edu.ua

Andrii Aronov
PhD in Engineering, Associate Professor, Department of Digital Development Technologies,
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0009-0000-7868-8341
a.aronov@duikt.edu.ua

Dmytro Nishchemenko
Doctor of Philosophy, Lecturer, Department of Digital Development Technologies,
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID: 0009-0006-1781-4109
d.nishchemenko@duikt.edu.ua

Oleksii Ananchenko
PhD in Engineering, Associate Professor, Department of Digital Development Technologies,
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID:0009-0005-3446-5994
o.ananchenko@duikt.edu.ua

IMPROVEMENT OF THE MULTI-OBJECTIVE OPTIMIZATION METHOD FOR SMART HOME IoT SYSTEM CONTROL TAKING CYBER RISK INTO ACCOUNT

Abstract. The development of Internet of Things technologies and smart home systems is accompanied by an increasing number of automated decisions based on sensor information. The reliability of these data directly affects control quality because erroneous or intentionally modified measurements may result in inappropriate control actions. This paper proposes a simple improvement of a multi-objective optimization method for smart home IoT control by additionally taking cyber risk into account. The approach is based on a proactive control model in which a control action is selected according to user comfort and energy-efficiency criteria. To increase the resilience of the control process to distorted sensor data, an additional term is introduced into the utility function. This term depends on the level of distrust in the received measurement and on the difference between a candidate control action and a safe action obtained from a trusted state estimate. The distrust level is calculated from the deviation between the current sensor value and an expected value produced by a predictive model or another trusted source. The results section presents the mathematical model of the improved method, a short Python implementation fragment, and the parameters of the simulation experiment. The approach was tested using a 60-day indoor-temperature control simulation with a 15-minute time step. The baseline and improved methods were compared under normal operation and under intentional reduction of temperature sensor readings. Thirty simulation runs were performed. The results show that including cyber risk in the utility function reduces the average number of risky maximum-heating commands from 184.37 to 4.63, which corresponds to a reduction of 97.49%. The improved method maintained thermal comfort for 99.66% of the simulation time, compared with 89.50% for the baseline method under distorted sensor data. The conclusions outline further research directions, including multi-sensor state estimation, adaptive risk weighting, and validation on a physical smart-home testbed.

Keywords: smart home; Internet of Things; cyber risk; multi-objective optimization; sensor data; proactive control; simulation modeling.

REFERENCES

1. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010
2. Karkouch, A., Mousannif, H., Al Moatassime, H., & Noel, T. (2016). Data quality in Internet of Things: A state-of-the-art survey. Journal of Network and Computer Applications, 73, 57–81. https://doi.org/10.1016/j.jnca.2016.08.002
3. Zhang, A., Song, S., Wang, J., & Yu, P. S. (2017). Time series data cleaning: From anomaly detection to anomaly repairing. Proceedings of the VLDB Endowment, 10(10), 1046–1057. https://doi.org/10.14778/3115404.3115410
4. Chahuara, P., Portet, F., & Vacher, M. (2017). Context-aware decision making under uncertainty for voice-based control of smart home. Expert Systems with Applications, 75, 63–79. https://doi.org/10.1016/j.eswa.2017.01.014
5. Cotti, L., Guizzardi, D., Barricelli, B. R., & Fogli, D. (2024). Enabling end-user development in smart homes: A machine learning-powered digital twin for energy efficient management. Future Internet, 16(6), 208. https://doi.org/10.3390/fi16060208
6. Dobrovolskis, A., Kazanavičius, E., & Kižauskienė, L. (2023). Building XAI-based agents for IoT systems. Applied Sciences, 13(6), 4040. https://doi.org/10.3390/app13064040
7. Ahmad, R., & Alkhammash, E. H. (2024). Online adaptive Kalman filtering for real-time anomaly detection in wireless sensor networks. Sensors, 24(15), 5046. https://doi.org/10.3390/s24155046
8. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), 1–58. https://doi.org/10.1145/1541880.1541882
9. Khan, A. N. (2023). An OCF-IoTivity enabled smart-home optimal indoor environment control system for energy and comfort optimization. Internet of Things, 22, 100712. https://doi.org/10.1016/j.iot.2023.100712
10. Khan, Q. W., Ahmad, R., Rizwan, A., Khan, A., Lee, K., & Kim, D. (2024). Optimizing energy efficiency and comfort in smart homes through predictive optimization: A case study with indoor environmental parameter consideration. Energy Reports, 11, 5619–5637. https://doi.org/10.1016/j.egyr.2024.05.038
11. Nishchemenko, D. O., & Aronov, A. O. (2025). Research on methods for optimizing parameters of a smart home control system using IoT. Telecommunication and Information Technologies, 1, 141–150. https://doi.org/10.31673/2412-4338.2025.013027
12. Nishchemenko, D. O., & Oleinikov, I. A. (2025). Proactive smart home control architecture based on contextual user intentions and multi-objective optimization. Telecommunication and Information Technologies, 3, 141–149. https://doi.org/10.31673/2412-4338.2025.038716

Отримано редакцією журналу / Received: 04.03.26
Прорецензовано / Revised: .25.03.26
Схвалено до друку / Accepted: 24.09.26