

DOI: <https://doi.org/10.36910/6775-2524-0560-2025-60-06>

УДК 004.93

Христинець Наталія Анатоліївна¹, к. т. н., доцент

<https://orcid.org/0000-0002-4836-7632>

Биков Сергій Олегович, магістрант

Марчук Олександр Юрійович, магістрант

Луцький національний технічний університет, м. Луцьк, Україна

ПРОТОТИПИ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ БЕЗПЕКИ І УПРАВЛІННЯ ІНФРАСТРУКТУРОЮ НА БАЗІ ІОТ-ПЛАТФОРМ

Христинець Н. А., Биков С. О., Марчук О. Ю. Прототипи інтелектуальних систем безпеки і управління інфраструктурою на базі ІоТ-платформ. У сучасних інженерних проектах дедалі важливішим стає створення інтелектуальних систем безпеки та управління інфраструктурою, зумовлене зростаючими вимогами до ефективності, надійності та адаптивності інженерних рішень у техногенному середовищі. Інтенсивна урбанізація, збільшення транспортних потоків та ускладнення архітектури будівель потребують впровадження високотехнологічних засобів моніторингу та контролю. У цьому контексті інтеграція концепції Інтернету речей (ІоТ), програмних платформ та алгоритмічних методів обробки даних є ключовою для побудови комплексних інженерних рішень нового покоління. Дослідження спрямоване на створення програмно-апаратного комплексу, що поєднує сенсорні пристрої, комунікаційні протоколи та алгоритми обробки інформації. Важлива увага приділяється розробці методів збору, аналізу та інтерпретації даних у реальному часі, що дозволяє приймати ефективні інженерні рішення. Аналіз українських досліджень показав, що існуючі системи здебільшого орієнтовані на окремі аспекти – енергоефективність сенсорних мереж, алгоритми маршрутизації або локальний захист ІоТ-пристроїв – та часто не мають комплексної апробації. Це обґрунтовує потребу у створенні інтегрованих рішень, які забезпечують обробку поточкових даних у реальному часі, багаторівневий захист інформації, масштабованість та надійність системи. Експериментальна частина включає прототип системи для моніторингу приміщень та управління паркінгом із використанням сенсорів і камер, де дані агрегуються та обробляються алгоритмами штучного інтелекту. Оцінка ефективності системи здійснюється за точністю спрацювань, затримкою обробки, продуктивністю поточкових даних, середнім енергоспоживанням та надійністю. Побудова узгоджених масивів даних із часовими мітками та унікальними ідентифікаторами забезпечує когерентність інформації та дозволяє оптимізувати баланс між швидкістю реакції та енергозбереженням. Перспективи дослідження включають розширення сенсорної мережі, інтеграцію різних типів даних, впровадження адаптивних алгоритмів розподілу навантаження та розвиток моделей штучного інтелекту для прогнозування аномалій і автоматичного налаштування системи, що підвищить надійність і ефективність ІоТ-рішень у критично важливих і довготривалих сценаріях.

Ключові слова: ІоТ, сенсорні мережі, інтелектуальна безпека, моніторинг, штучний інтелект, енергоефективність, паркінг, масштабування.

Khrystynets N., Bykov S., Marchuk O. Prototypes of Intelligent Security and Infrastructure Management Systems Based on IoT Platforms. In modern engineering projects, the development of intelligent security and infrastructure management systems is becoming increasingly important due to growing demands for efficiency, reliability, and adaptability of engineering solutions in technologically complex environments. Rapid urbanization, increased traffic flows, and the growing complexity of building architectures require the implementation of advanced monitoring and control technologies. In this context, the integration of the Internet of Things (IoT) concept, software platforms, and algorithmic data processing methods is key to creating next-generation comprehensive engineering solutions. The research focuses on developing a hardware–software complex that combines sensor devices, communication protocols, and data processing algorithms. Particular attention is given to the development of methods for real-time data collection, analysis, and interpretation, enabling effective engineering decision-making. An analysis of Ukrainian studies has shown that existing systems are mainly focused on specific aspects—such as energy efficiency of sensor networks, routing algorithms, or local IoT device protection—and often lack comprehensive validation. This highlights the need for integrated solutions that provide real-time data stream processing, multi-level information protection, scalability, and system reliability. The experimental part includes a prototype system for room monitoring and parking management using sensors and cameras, where data are aggregated and processed by artificial intelligence algorithms. System performance is evaluated based on detection accuracy, processing latency, data stream throughput, average energy consumption, and reliability. The construction of synchronized datasets with timestamps and unique identifiers ensures data coherence and allows optimization of the balance between reaction speed and energy efficiency. Future research prospects include expanding the sensor network, integrating various data types, implementing adaptive load-balancing algorithms, and developing AI models for anomaly prediction and automatic system configuration, which will enhance the reliability and efficiency of IoT solutions in critical and long-term operational scenarios.

Keywords: IoT, sensor networks, intelligent security, monitoring, artificial intelligence, energy efficiency, parking, scalability.

Постановка завдання. У сучасних інженерних проектах гостро стоять питання розробки інтелектуальних систем безпеки та управління інфраструктурою, що зумовлені зростаючими вимогами до ефективності, надійності й адаптивності інженерних рішень у сьогодишньому техногенному середовищі. Інтенсивна урбанізація, зростання обсягів транспортних потоків, ускладнення архітектури будівель і споруд, а також посилення ризиків техногенного та соціального

характеру потребують застосування високотехнологічних засобів моніторингу й контролю. У цьому контексті інтеграція концепції Інтернету речей, програмних платформ та алгоритмічних методів обробки даних є ключовим фактором для формування комплексних інженерних рішень.

Завдання дослідження полягає у створенні програмно-апаратного комплексу, який об'єднує сенсорні пристрої, комунікаційні протоколи та програмні модулі обробки інформації. Особлива увага приділяється розробці алгоритмів збору, аналізу та інтерпретації даних, що забезпечують прийняття інженерних рішень у режимі реального часу. Передбачається також проведення досліджень ефективності різних підходів до побудови системних архітектур, визначення оптимальних програмних платформ для інтеграції компонентів та обґрунтування інженерних методів, здатних гарантувати масштабованість і стійкість таких систем у складних експлуатаційних умовах.

Аналіз досліджень та публікацій. У межах цієї роботи розглядаються українські дослідження з розробки інтелектуальних систем безпеки та управління інфраструктурою. Згідно ст. 1 Закону України «Про національну безпеку України» національні інтереси – це життєво важливі матеріальні, інтелектуальні і духовні цінності Українського народу, визначальні потреби суспільства і держави, реалізація яких гарантує державний суверенітет України та її прогресивний розвиток. Але, разом з тим, залишається відкритим питання про конкретні механізми та принципи визначення змісту національних інтересів.

Це зумовлено тим, що особливості впровадження таких систем безпосередньо залежать від національної інженерної, технічної та нормативно-правової бази, а також від доступності локальних технологій та IoT-платформ. Аналіз українських джерел дозволяє оцінити реальний стан розвитку програмних і апаратних рішень, сенсорних мереж та алгоритмів обробки даних у контексті національної інфраструктури.

Так, в роботі [1] здійснено огляд сучасних архітектур «смарт-паркінгу» та розглянуто роль IoT-сензорів, комунікаційних протоколів і алгоритмів планування та динамічного ціноутворення. В статті підкреслено потребу в єдиних програмних платформах для інтеграції датчиків і сервісів міської інфраструктури, зокрема, пряме відображення проблематики програмної інтеграції IoT у паркувальні системи. Дослідження [2-3] стосуються автоматизованих систем пошуку паркомісць. У них розглянуто практичні вказівки щодо вибору сенсорів і енергетичних стратегій, алгоритми маршрутизації і методи обробки поточкових даних від сенсорів і камер. З програмної точки зору, тут використані алгоритми верифікації пошуку і резервування місць. Проте, на нашу думку, у них слабка деталізація програмних стеків і алгоритмів віддаленої обробки даних. Роботи [4-6] мають інше спрямування і стосуються систем захисту домашніх IoT-мереж, які, в основному, базуються на мікроконтролерах. У всіх цих дослідженнях запропоновані практичні інструкції з розгортання, моніторингу та управління цих систем. В цих роботах містяться конкретні порівняння платформ, показники швидкості розробки, інтеграційні можливості кожного з мікроконтролерів: ESP, Arduino, STM, Raspberry Pi.

Загалом, порівняння як згаданих, так і інших вітчизняних досліджень в даній області наведено в таблиці 1.

Таблиця 1 – Аналітика вітчизняних публікацій інтелектуальних систем безпеки

№	Автори (рік)	Платформи і апаратна платформа	Протоколи зв'язку	Алгоритми і методи	Короткий результат	Обмеження, або недоліки
1	Копиця, Кветний (2025) [1]	Смарт-паркінг, IoT-сенсори	LoRa, Wi-Fi	Обробка даних для управління паркуванням	Рекомендовані інтеграційні архітектури	Теоретичні висновки, без польових тестів
2	Кононова (2023) [2]	Безпроводова сенсорна мережа (WSN)	ZigBee, Wi-Fi	Енергозберігаючі алгоритми збору даних	Оптимізація енергоспоживання сенсорів	Мало уваги до програмної частини
3	Нападій (2023) [3]	Камери, датчики паркування	Wi-Fi, Ethernet	Алгоритми маршрутизації	Автоматизація пошуку паркомісць	Локальне тестування,

				та пошуку місць		обмежений масштаб
4	Шелуха (2024) [4]	ESP32, локальні IoT- пристрої	Wi-Fi, BLE	Шифрування AES, SSL/TLS	Захист домашніх IoT- мереж	Тестування у обмежених сценаріях
5	MindScope (2024) [5]	Різні IoT- платформи	Wi-Fi, мобільні мережі	Методи оцінки ризиків	Аналітичні рекомендації щодо безпеки	Переважно аналітична робота, без експерименті в
6	SmartParking. ua (2024– 2025) [6]	Роботизова ні паркінги, сенсори	LoRa, Wi-Fi	Алгоритми управління потокami	Практичні кейси впроваджень	Відсутність академічної верифікації
7	Sii (2025) [7]	Edge- пристрої, IoT- платформи	LoRa, BLE, Wi- Fi	Edge-обробка даних	Індустріальні рішення для IoT	Маркетингов ий характер, мало академічного аналізу
8	Academy Vision (2024) [8]	Узагальнені інтелектуал ьні системи	-	Концептуальні методи безпеки	Методологічна база інтелектуальної безпеки	Абстрактніст ь, мало практичних реалізацій
9	Воропаєва та ін. (2024) [9]	Сервери обробки даних, аналітика	Ethernet, Wi-Fi	Методи машинного навчання	Підвищення ефективності інформаційної безпеки	Фокус на інформаційні й, а не технічний безпеці

Розглянуті оглядові та дискусійні журнали і публікації [7-9] з проблем інформаційної/інтелектуальної безпеки охоплюють міждисциплінарні підходи до інтелектуальної безпеки і її ролі у державних та інфраструктурних системах. У цих дослідженнях наявна широка методологічна перспектива для системного бачення проблеми та соціально-технічні аспекти інженерних рішень. Проте, у них мало практичних реалізацій для IoT-інфраструктур.

Як видно, більшість досліджень зосереджуються на окремих аспектах систем – наприклад, енергоефективності сенсорних мереж, алгоритмах маршрутизації або захисті IoT-пристроїв – і часто мають локальний або концептуальний характер без комплексної апробації. З цього випливає потреба у розробці інтегрованих рішень, що поєднують різні платформи та протоколи, забезпечують ефективну обробку поточкових даних у реальному часі, багаторівневий захист інформації та можливість масштабування системи. Крім того, важливим є створення методології оцінки продуктивності, надійності та енергоспоживання для комплексного порівняння апаратних та програмних компонентів, що дозволить сформувати практично застосовні інженерні рекомендації для впровадження інтелектуальних систем безпеки й управління інфраструктурою.

Набори даних, сценарії тестування та метрики. Експериментальна частина роботи передбачає розробку та тестування прототипу інтелектуальної системи на основі IoT-платформ із інтегрованими сенсорами, програмними модулями обробки даних та алгоритмами прийняття рішень у реальному часі. Тестування проводиться у межах двох основних сценаріїв: моніторингу приміщення та управління паркінгом. У першому випадку моделюється доступ до об'єктів і фіксується рух за допомогою сенсорів і камер із перевіркою коректності сигналізації та реагування системи. У другому – реєструється заповнюваність паркомісць, здійснюється обробка поточкових даних з сенсорів і камер, а також оцінюється робота алгоритмів маршрутизації та резервування місць. Окремо оцінюється стійкість та безпека мережі, перевіряється відмовостійкість сенсорних вузлів і захищеність даних при передачі через різні протоколи зв'язку, такі як Wi-Fi, BLE або LoRa.

Дані організовані з урахуванням класичних залежностей між сенсорними сигналами та подіями у фізичному середовищі. Наприклад, для сенсора руху можна ввести залежність активації S_r від присутності об'єкта O у зоні дії:

$$S_r = f(O, T, L), \quad (1)$$

де T – час спрацьовування, L – рівень освітленості, а функція f визначає кореляцію сенсорного сигналу з реальною подією. Для заповнюваності паркомісць P_a використовується формула:

$$P_a = \frac{N_{occ}}{N_{total}}, \quad (2)$$

де N_{occ} – кількість зайнятих місць, N_{total} – загальна кількість паркомісць. Подібні формули дозволяють формалізувати аналіз ефективності алгоритмів та побудувати точні метрики оцінки системи.

Схема залучення сенсорів передбачає взаємодію різномірних пристроїв із центральним контролером. Сенсорні вузли збирають первинні дані про рух, стан паркомісць, температуру та освітленість. Дані передаються на платформу обробки (ESP32, Arduino, Raspberry Pi або STM32), де вони агрегуються, аналізуються та інтерпретуються алгоритмами прийняття рішень. Відеопотоки обробляються паралельно за допомогою модулів детекції об'єктів і визначення заповнюваності, а результати об'єднуються з сенсорними даними для формування комплексної оцінки стану системи та реагування на події. Дана схема дозволяє забезпечити модульність системи, інтеграцію різних сенсорів та гнучкість у масштабуванні.

Ефективність системи оцінюється за кількістю правильних спрацьовувань сенсорів і алгоритмів A_c , затримкою обробки T_d , продуктивністю обробки поточних даних R_p , середнім енергоспоживанням сенсорних вузлів E_s та надійністю системи S_r . Наприклад, точність спрацьовування визначається формулою:

$$A_c = \frac{N_{correct}}{N_{total}} \cdot 100\%, \quad (3)$$

де $N_{correct}$ – кількість правильних спрацьовувань, N_{total} – загальна кількість подій.

Затримка обробки вимірюється як середній час між моментом виникнення події та формуванням реакції обчислюється як:

$$T_d = \frac{1}{N_{total}} \sum_{i=1}^{N_{total}} (t_{response,i} - t_{event,i}) \quad (4)$$

У залежності (4), що описує затримку від моменту події до реакції системи, повна затримка системи, або сумарний час від моменту виникнення події в реальному середовищі до моменту, коли інтелектуальна IoT-система сформує відповідну реакцію обчислюється як сума:

$$T_{latency} = T_{capture} + T_{transmission} + T_{processing} + T_{decision},$$

У багатоплатформеному IoT-середовищі можна зробити її більш придатною для порівнянь у, деталізуючи етапи і включивши ймовірність втрат або повторних передач. Вдосконалений вираз буде мати вигляд:

$$T_{latency} = T_{capture} + \frac{T_{transmission}}{1 - P_{loss}} + T_{processing}(N_{data}, C_{alg}) + T_{decision}, \quad (5)$$

де $T_{capture}$ – час фіксації події сенсором; $T_{transmission}$ – базовий час передачі пакета даних через канал зв'язку; P_{loss} – ймовірність втрати пакета, яка зумовлює повторні передачі та, відповідно, збільшення затримки; $T_{processing}(N_{data}, C_{alg})$ – час обробки даних, що залежить від обсягу N_{data} і складності алгоритму C_{alg} ; $T_{decision}$ – час прийняття рішення системою (вибір дії або формування сигналу).

Дана формула враховує не лише статичні часові компоненти, але й стохастичні фактори роботи мережі та алгоритмічну складність, що робить її релевантною для практичного аналізу інженерних IoT-рішень.

Експерименти досліджень передбачають порівняння різних платформ і протоколів зв'язку, а також оцінку програмних стеків з точки зору швидкості розробки, інтеграційних можливостей та ефективності алгоритмів обробки даних. Результати досліджень [10-11] дозволяють обґрунтувати оптимальні інженерні рішення для побудови інтегрованих інтелектуальних систем безпеки й управління інфраструктурою, здатних працювати в реальних умовах міських та промислових об'єктів [12], а блок-схему залучення сенсорів і потоків даних у інтелектуальних системах безпеки можна сформувати наступним чином (рис. 1):

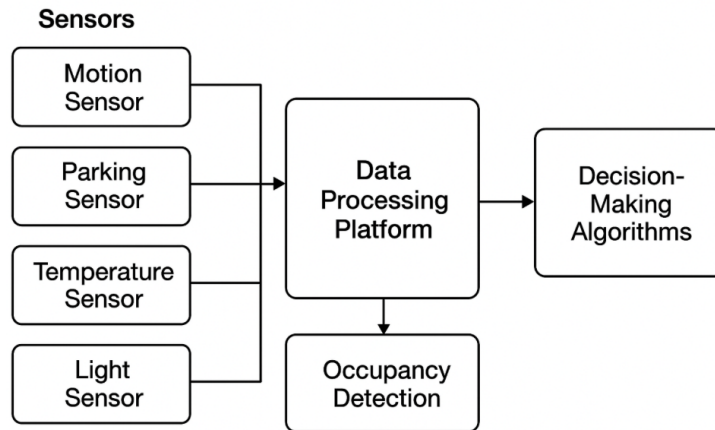


Рис.1. Архітектура залучення сенсорів та потоків даних в інтелектуальній IoT-системі безпеки (сформовано авторами публікації)

Подана блок-схема репрезентує функціональну архітектуру інтелектуальної IoT-системи безпеки та управління інфраструктурою. Вона відображає наскрізний цикл перетворення інформації – від моменту фіксації подій у фізичному середовищі до формування керуючих рішень у реальному часі. На першому етапі сенсорні вузли (датчики руху, температури, освітленості та заповнюваності паркомісць) здійснюють реєстрацію відповідних параметрів та генерують первинні сигнали. Далі інформаційні потоки передаються до обчислювальної платформи (ESP32, Arduino, Raspberry Pi або STM32), де відбувається агрегування даних, їхня попередня обробка та інтерпретація. Важливим елементом є модуль визначення заповнюваності, який виконує аналіз відеопотоків і синхронізується із сенсорними сигналами для підвищення точності оцінки стану системи. Завершальним етапом є рівень алгоритмів прийняття рішень, що на основі оброблених даних формують реакції системи – зокрема активацію сигналізації, видачу попереджувальних повідомлень, резервування паркомісць або керування ресурсами інфраструктури. Структура схеми забезпечує модульність і масштабованість системи, інтеграцію різноманітних сенсорів, а також комплексне врахування потоків даних у процесах моніторингу та управління.

Виклад основного матеріалу дослідження.

Дослідження розгортається навколо інтеграції сенсорних вузлів, комунікаційних протоколів та алгоритмів обробки даних у єдине інтелектуальне середовище, здатне функціонувати в реальному часі.

Базовим рівнем системи виступає шар збору даних, де кожен IoT-пристрій має власний унікальний ідентифікатор ID_i , що дозволяє забезпечити однозначне відображення інформаційних потоків у розподіленому середовищі. Таким чином, кожен сенсор руху, температури або паркування генерує сигнал у вигляді $S_i = f(O, T, L, ID_i)$, де параметри O , T та L описують стан середовища, а ID_i визначає конкретний пристрій у системі. Впровадження унікальних ідентифікаторів створює можливість синхронізації потоків даних при їхній агрегації та подальшій аналітичній обробці.

На другому рівні відбувається інтеграція сенсорних та відеопотоків у єдиний масив вхідних даних. Потоки формалізуються у вигляді багатовимірного набору $D = \{S_1, S_2, \dots, S_n, V_1, V_2, \dots, V_m\}$, де S_i – сенсорні дані, а V_j – відеокадри або їхні вектори ознак після попередньої обробки. Для забезпечення стійкості до втрат пакетів у комунікаційному каналі кожен блок даних позначається часовою міткою τ_k та індексом джерела, що дозволяє реалізувати функцію синхронізації:

$$D_{sync} = g(D, \tau_k, ID_i), \quad (6)$$

де g – алгоритм узгодження за часом і джерелом, що формує когерентний набір для подальшого аналізу.

Ключовим компонентом є алгоритмічна обробка, яка включає застосування методів штучного інтелекту. Модель глибокого навчання M_θ зі структурою згорткової нейронної мережі або трансформера отримує на вхід вектори ознак із D_{sync} . Функція прийняття рішень формалізується у вигляді:

$$y = M_\theta(D_{sync}), \quad (7)$$

де u – прогнозована дія системи, наприклад, активація сигналізації, маркування паркомісця як зайнятого чи формування повідомлення користувачу. Якість роботи моделі оцінюється за метрикою точності:

$$A_c = \frac{N_{correct}}{N_{total}} \cdot 100\%, \quad (8)$$

де $N_{correct}$ – кількість правильно класифікованих подій, а N_{total} – загальна кількість зафіксованих ситуацій.

Важливим аспектом є часові характеристики системи. Так як затримка реакції визначається середнім значенням формулою (4), а повна затримка з урахуванням ймовірності втрат пакетів і складності алгоритмів описується виразом (6) і енергетична ефективність сенсорних вузлів відіграє критичну роль у масштабованості системи, то середнє споживання визначається як

$$E_s = \frac{1}{T_{obs}} \int_0^{T_{obs}} P(t) dt, \quad (9)$$

де $P(t)$ – миттєва потужність, а T_{obs} – час спостереження. Для підвищення ефективності використовуються алгоритми розподілу навантаження між вузлами та оптимізації частоти передачі даних.

У поєднанні ці залежності формують двовимірний критерій оптимальності: система повинна одночасно мінімізувати затримку $T_{latency}$ і середнє споживання енергії E_s . Баланс між цими характеристиками визначає придатність IoT-рішення для практичного застосування. У випадках критичних систем безпеки пріоритет віддається зменшенню $T_{latency}$, тоді як для довготривалого моніторингу важливішим стає зменшення E_s . Це створює основу для побудови цільової функції оптимізації, яка може мати вигляд:

$$F_{opt} = \alpha \cdot T_{latency} + \beta \cdot E_s, \quad (10)$$

де коефіцієнти α та β визначають відносну вагу часової ефективності та енергозбереження у конкретному сценарії експлуатації системи.

Мета використання наведеної залежності полягає у визначенні компромісу між часовою ефективністю та енергоспоживанням системи IoT. Завдяки вимірюванню та узгодженню затримки реакції $T_{latency}$ і середнього споживання енергії E_s можна оцінити придатність рішення для конкретного сценарію: у критичних системах безпеки пріоритет надається зменшенню затримки, а для довготривалого моніторингу – зниженню енергоспоживання. Формалізація цього балансу дозволяє системно підходити до оптимізації параметрів, оцінювати ефективність алгоритмів синхронізації та обробки даних, а також планувати розподіл навантаження між сенсорними вузлами для підвищення загальної продуктивності та надійності системи.

Висновки і перспективи досліджень. Проведене дослідження демонструє, що інтеграція сенсорних та відеопотоків у єдиний масив даних із використанням унікальних ідентифікаторів забезпечує надійну синхронізацію та когерентність інформації. Використання методів штучного інтелекту, зокрема моделей глибокого навчання, дозволяє ефективно прогнозувати дії системи та приймати рішення на основі вхідних даних. Аналіз часових характеристик та енергоспоживання показав можливість оптимального балансування між швидкістю реакції та ресурсозбереженням, що визначає практичну придатність IoT-рішень у різних сценаріях експлуатації.

У перспективі доцільно розширити масштаб системи, включивши більшу кількість сенсорів та різноманітні типи даних, а також досліджувати адаптивні алгоритми розподілу навантаження та оптимізації частоти передачі даних. Крім того, розвиток моделей штучного інтелекту із врахуванням прогнозування аномалій та автоматичного налаштування параметрів системи може підвищити надійність та ефективність IoT-рішень у критично важливих і довготривалих сценаріях.

Список використаних джерел:

1. Копиця Є. Екологічне нормування у сфері зміни клімату в контексті імплементації європейського зеленого курсу в Україні. *MODALITĂȚI CONCEPTUALE DE DEZVOLTARE A ȘTIINȚEI MODERNE*. 2020. URL: <https://doi.org/10.36074/20.11.2020.v4.15> (дата звернення: 24.07.2025)
2. Kononova I. V., Samus D. V. ANALYSIS OF THE OPTION OF IMPLEMENTING AN ENERGY-EFFICIENT SMART PARKING BASED ON A WIRELESS SENSOR NETWORK. *Scientific notes of Taurida National V.I. Vernadsky University. Series: Technical Sciences*. 2023. Vol. 1, no. 3. P. 6–13. URL: <https://doi.org/10.32782/2663-5941/2023.3.1/02> (date of access: 11.07.2025).
3. Нападій О., Цюпа Н., Батрак Є. Система автоматизації пошуку місць для паркування. *Адаптивні системи автоматичного управління*. 2023. Т. 2, № 43. С. 140–153. URL: <https://doi.org/10.20535/1560-8956.43.2023.292264> (дата звернення: 11.07.2025).

4. Шелуха О. О., Квашук Д. М., Супруненко К. О. Дворівнева система захисту домашньої IoT-мережі. *Технічна інженерія*. 2025. № 2(94). С. 174–179. URL: [https://doi.org/10.26642/ten-2024-2\(94\)-174-179](https://doi.org/10.26642/ten-2024-2(94)-174-179) (дата звернення: 11.07.2025).
5. Інтеграція IoT у охоронні системи: Переваги та ризики. *mindscope.biz.ua*. URL: https://mindscope.biz.ua/integracziya-iot-u-ohoronni-systemy-perevagy-ta-ryzyky/?utm_source=chatgpt.com (дата звернення: 09.09.2025).
6. Роботизовані паркінги: історія, принцип роботи та переваги. *Smartparking.ua*. URL: https://www.smartparking.ua/robotizovani-parkingi-istorija-princip-roboti-ta-perevagi/?utm_source=chatgpt.com (дата звернення: 05.09.2025).
7. Protected and integrated IoT devices. *Sii.ua*. URL: https://sii.ua/en/what-we-offer/iot/?utm_source=chatgpt.com (date of access: 04.09.2025).
8. Кошовий Б. Ретроспективний аналіз досліджень інтелектуальної безпеки у міждисциплінарній площині. *Академічні Візії*. 2022. № 13. С. 1–9.
9. Воропаса Т. С., Авер'янова Н. М. Штучний інтелект в системі інформаційної безпеки України в умовах російсько-української війни. *SCIENTIA*. 2023. С. 62–67. URL: <http://previous.scientia.report>.
10. Антошук С. Г., Комлева Н. О. Оптимізаційне моделювання інтелектуальних систем діагностування. *Вісник Херсонського національного технічного університету*. 2024. № 2(89). С. 99–108. URL: <https://doi.org/10.35546/kntu2078-4481.2024.2.14> (дата звернення: 11.07.2025).
11. Моделі формування рекомендацій у інтелектуальних системах електронної комерції / О. Ю. Чердніченко та ін. *Системи обробки інформації*. 2020. № 1(160). С. 32–39. URL: <https://doi.org/10.30748/soi.2020.160.04> (дата звернення: 11.07.2025).
12. Ващишак І. Р., Ващишак С. П. Агروفотovoltaїчна сонячна станція з вимірювальними каналами IoT. *Scientific Bulletin of UNFU*. 2020. Т. 30, № 2. С. 129–134. URL: <https://doi.org/10.36930/40300223> (дата звернення: 11.07.2025).

References:

1. Kopytsia, Ye. Environmental Regulation in the Field of Climate Change in the Context of Implementing the European Green Deal in Ukraine. *MODALITĂȚI CONCEPTUALE DE DEZVOLTARE A ȘTIINȚEI MODERNE*, 2020. URL: <https://doi.org/10.36074/20.11.2020.v4.15> (date of access: 24.07.2025)
2. Kononova, I. V., Samus, D. V. Analysis of the Option of Implementing an Energy-Efficient Smart Parking Based on a Wireless Sensor Network. *Scientific Notes of Taurida National V.I. Vernadsky University. Series: Technical Sciences*, 2023, Vol. 1, no. 3, pp. 6–13. URL: <https://doi.org/10.32782/2663-5941/2023.3.1/02> (date of access: 11.07.2025)
3. Napadiy, O., Tsopa, N., Batrak, Ye. Automated Parking Space Search System. *Adaptive Automatic Control Systems*, 2023, Vol. 2, no. 43, pp. 140–153. URL: <https://doi.org/10.20535/1560-8956.43.2023.292264> (date of access: 11.07.2025)
4. Shelukha, O. O., Kvashuk, D. M., Suprunenko, K. O. Two-Level Home IoT Network Protection System. *Technical Engineering*, 2025, no. 2(94), pp. 174–179. URL: [https://doi.org/10.26642/ten-2024-2\(94\)-174-179](https://doi.org/10.26642/ten-2024-2(94)-174-179) (date of access: 11.07.2025)
5. Integration of IoT into Security Systems: Advantages and Risks. *mindscope.biz.ua*. URL: https://mindscope.biz.ua/integracziya-iot-u-ohoronni-systemy-perevagy-ta-ryzyky/?utm_source=chatgpt.com (date of access: 09.09.2025)
6. Robotic Parking: History, Operating Principles, and Advantages. *Smartparking.ua*. URL: https://www.smartparking.ua/robotizovani-parkingi-istorija-princip-roboti-ta-perevagi/?utm_source=chatgpt.com (date of access: 05.09.2025)
7. Protected and Integrated IoT Devices. *Sii.ua*. URL: https://sii.ua/en/what-we-offer/iot/?utm_source=chatgpt.com (date of access: 04.09.2025)
8. Koshovyi, B. Retrospective Analysis of Intelligent Security Research in an Interdisciplinary Context. *Academic Visions*, 2022, no. 13, pp. 1–9
9. Voropayeva, T. S., Averyanova, N. M. Artificial Intelligence in Ukraine's Information Security System under the Conditions of the Russian-Ukrainian War. *SCIENTIA*, 2023, pp. 62–67. URL: <http://previous.scientia.report>
10. Antoshchuk, S. H., Komleva, N. O. Optimization Modeling of Intelligent Diagnostic Systems. *Bulletin of Kherson National Technical University*, 2024, no. 2(89), pp. 99–108. URL: <https://doi.org/10.35546/kntu2078-4481.2024.2.14> (date of access: 11.07.2025)
11. Models of Recommendation Formation in Intelligent E-Commerce Systems / O. Yu. Cherednichenko et al. *Information Processing Systems*, 2020, no. 1(160), pp. 32–39. URL: <https://doi.org/10.30748/soi.2020.160.04> (date of access: 11.07.2025)
12. Vashchyshak, I. R., Vashchyshak, S. P. Agro-Photovoltaic Solar Station with IoT Measurement Channels. *Scientific Bulletin of UNFU*, 2020, Vol. 30, no. 2, pp. 129–134. URL: <https://doi.org/10.36930/40300223> (date of access: 11.07.2025)