ISSN 2786-4588 (Print)
ISSN 2786-4596 (Online)

Міністерство освіти і науки України
Херсонський державний аграрно-економічний університет

Таврійський науковий вісник

Технічні науки

Випуск 4
Частина 1

Видавничий дім
«Гельветика»
2025

ISSN 2786-4588 (Print)
ISSN 2786-4596 (Online)

Рекомендовано до друку вченою радою Херсонського державного аграрно-економічного університету (протокол № 1 від 29.08.2025 року)

Таврійський науковий вісник. Серія: Технічні науки / Херсонський державний аграрно-економічний університет. Херсон : Видавничий дім «Гельветика», 2025. Вип. 4. Ч. 1. 452 с.

Журнал включено до міжнародної наукометричної бази Index Copernicus International (Республіка Польща)

Реєстрація суб'єкта у сфері друкованих медіа: Рішення Національної ради України з питань телебачення і радіомовлення № 2933 від 24.10.2024 року.

Суб'єкт у сфері друкованих медіа – Херсонський державний аграрно-економічний університет (вул. Стрітенська, буд. 23, м. Херсон, 73006, office@ksaeu.kherson.ua, тел. +38(050) 571-19-13)

На підставі Наказу Міністерства освіти і науки України від 29.06.2021 № 735 (додаток 4) журнал внесений до переліку фахових видань України категорії «Б» (спеціальності: F3 – Комп'ютерні науки; F4 – Системний аналіз та наука про дані; G13 – Харчові технології; G19 – Будівництво та цивільна інженерія).

Статті у виданні перевірені на наявність плагіату за допомогою програмного забезпечення StrikePlagiarism.com від польської компанії Plagiat.pl.

УДК 004.056
DOI https://doi.org/10.32782/tnv-tech.2025.4.1.12

РОЗПОДІЛЕНА ЗАХИЩЕНА СИСТЕМА ЗБОРУ, ПЕРЕДАЧІ ТА ОБРОБКИ ДАНИХ

Киричек Г. Г. *– кандидат технічних наук,*
доцент кафедри комп'ютерних систем та мереж
Національного університету «Запорізька політехніка»
ORCID ID: 0000-0002-0405-7122

Тягунова М. Ю. *– кандидат технічних наук,*
доцент кафедри комп'ютерних систем та мереж
Національного університету «Запорізька політехніка»
ORCID ID: 0000-0002-9166-5897

Дроздов С. І. *– студент факультету комп'ютерних наук та технологій*
Національного університету «Запорізька політехніка»
ORCID ID: 0009-0006-6781-5708

На даний час використання відкритих або ненадійно захищених протоколів, слабка автентифікація користувачів, відсутність централізованого управління доступом створює сприятливе середовище для кібератак. Тому застосування модульної архітектури, зрозумілого інтерфейсу та рішень, які базуються на кращих практиках проектування IoT-систем, включаючи принципи слабкої зв'язаності, високої доступності та горизонтального масштабування є достатньо актуальними. В роботі описано процес отримання універсального та масштабованого рішення для безпечного збору та обробки даних IoT-пристроїв, яке можна адаптувати для різних напрямків із урахуванням специфічних вимог до безпеки та продуктивності. Метою роботи є проведення досліджень, реалізація розподіленої платформи збору та обробки отриманих даних з сенсорів, керування розподіленими пристроями, а також впровадження системи кіберзахисту для запобігання несанкціонованому доступу до інформації та втраті конфіденційних даних. Об'єктом дослідження є побудована на базі IoT-пристроїв система, яка передбачає можливість масштабування, гнучку конфігурацію та безпечне управління в реальному часі. Предметом дослідження є сукупність технічних і програмних засобів, які забезпечують безпечну комунікацію між IoT-пристроями, включаючи архітектуру взаємодії компонентів, протоколи обміну, криптографічні методи захисту та інтерфейс користувача. Робота пов'язана з необхідністю вдосконалення та впровадження модулів, які б ефективно функціонували в умовах реального навантаження, підтримуючи віддалений доступ, захищений обмін даними та могли адаптуватися до різних типів пристроїв. Серед технологій, які застосовуються в системі маємо: протокол MQTT (Message Queuing Telemetry Transport) як засіб телеметричної передачі повідомлень; TLS (Transport Layer Security) для створення захищеного каналу зв'язку; ESP32 у якості апаратної платформи (мікроконтролер) збору та передачі даних; JSON Web Token, що забезпечує автентифікацію та контроль доступу; MikroTik VPN/ACL, що вирішує питання захисту при маршрутизації та фільтрації трафіку.

Ключові слова: *мікроконтролер, автентифікація, трафік, сенсор, протокол, мережа.*

Kyrychek H. H., Tiahunova M. Yu., Drozdov S. I. Distributed secure system of data collection, transfer and processing

Currently, the use of open or unreliable protocols, weak user authentication, and the lack of centralized access control create a favorable environment for cyberattacks. Therefore, the use of modular architecture, a clear interface, and solutions based on best practices for designing IoT systems, including the principles of weak coupling, high availability, and horizontal scaling,

are quite relevant. The paper describes the process of obtaining a universal and scalable solution for secure data collection and processing of IoT devices, which can be adapted for different areas, taking into account specific security and performance requirements. The purpose of the paper is to conduct research, implement a distributed platform for collecting and processing data received from sensors, manage distributed devices, and implement a cyber protection system to prevent unauthorized access to information and loss of confidential data. The object of the research is a system built on the basis of IoT devices, which provides scalability, flexible configuration and secure management in real time. The subject of the research is a set of technical and software tools that ensure secure communication between IoT devices, including the architecture of component interaction, exchange protocols, cryptographic protection methods and user interface. The work is related to the need to improve and implement modules that would function effectively under real load conditions, supporting remote access, secure data exchange and could adapt to different types of devices. Among the technologies used in the system are: the MQTT (Message Queuing Telemetry Transport) protocol as a means of telemetric message transmission; TLS (Transport Layer Security) to create a secure communication channel; ESP32 as a hardware platform (microcontroller) for data collection and transmission; JSON Web Token, which provides authentication and access control; MikroTik VPN/ACL, which solves the issue of protection when routing and filtering traffic.

Key words: *microcontroller, authentication, traffic, sensor, protocol, network.*

Постановка проблеми. Інтенсивний розвиток цифрових технологій, комп'ютерних мереж і мобільних пристроїв призвів до появи нової парадигми в інформаційних системах – концепції Інтернету речей. Вона передбачає інтеграцію фізичних об'єктів у єдиний інформаційний простір за допомогою сенсорів, мікроконтролерів, засобів зв'язку та програмного забезпечення [1]. IoT-системи забезпечують збір, передачу, обробку та аналіз даних з подальшим прийняттям рішень чи виконанням дій без безпосередньої участі людини [2]. Завдяки широким можливостям та універсальності, IoT-рішення сьогодні впроваджуються у найрізноманітніші сфери: промисловість, аграрний сектор, охорону здоров'я, логістику, смарт міста, будинки та офіси. Але збільшення кількості підключених пристроїв та розширення каналів передачі даних підвищує ризики інформаційної безпеки, що стає критичною проблемою для сучасного інформаційного простору. Окрім того IoT-пристрої, як правило, мають обмежені обчислювальні ресурси та енергоспоживання, що ускладнює впровадження традиційних засобів захисту інформації, таких як складні алгоритми шифрування, повноцінні брандмауери або антивірусні засоби. Крім того, використання відкритих або ненадійно захищених протоколів, слабка автентифікація користувачів, відсутність централізованого управління доступом створює сприятливе середовище для кібератак [2]. Тому застосування модульної архітектури, зрозумілого інтерфейсу та рішень, які базуються на кращих практиках проектування IoT-систем, включаючи принципи слабкої зв'язаності, високої доступності та горизонтального масштабування є достатньо актуальними.

Аналіз останніх досліджень і публікацій. Інтернет речей спирається на мережі фізичних об'єктів, які підтримують роботу вбудованих датчиків, програмного забезпечення та застосовують технології обміну даними з іншими пристроями та системами через мережу Інтернет [3]. Це кардинально змінює підходи до автоматизації та моніторингу процесів у різних сферах [4]. Сучасний стан розвитку IoT характеризується експоненціальним зростанням кількості підключених пристроїв. За даними аналітичної компанії Gartner у 2025 році світ вже має близько 75 мільярдів підключених IoT-пристроїв [5]. Таке швидке зростання обумовлене декількома ключовими факторами: зниження вартості мікроконтролерів і сенсорів; підвищення доступності безпроводових технологій передачі даних; розвиток хмарних обчислень та застосування штучного інтелекту [6]. При цьому сама архітектура типової IoT-системи спирається на чотири основні рівні. Рівень

сприйняття складається з фізичних пристроїв та сенсорів (датчиків), які збирають інформацію з навколишнього середовища [7]. Мережевий рівень забезпечує передачу цих даних через безпроводові канали зв'язку з підтримкою різних базових мережних технологій від Wi-Fi та Bluetooth до технологій стільникових мереж і супутникового зв'язку [8]. Рівень обробки для аналізу отриманої інформації використовує хмарні та граничні обчислювальні ресурси [9]. А рівень застосувань підтримує додатки та сервіси, через які клієнти взаємодіють з IoT-системою [10]. При цьому, особливе значення мають розподілені IoT-системи, які дозволяють балансувати навантаження між множиною вузлів, підвищуючи відмовостійкість подібних систем та підтримуючи масштабованість таких рішень [11]. Подібні системи є особливо ефективними при роботі з Big Data у реальному часі або забезпеченні роботи в умовах нестабільної мережевої інфраструктури [9]. Також, сучасні напрямки застосування методів IoT в процесі прийняття рішень, включають: інтеграцію з технологіями штучного інтелекту; впровадження граничних обчислень з метою зменшення затримок; впровадження енергоефективних протоколів зв'язку і методів забезпечення кібербезпеки [12]. Кібербезпека при цьому має критичне значення у зв'язку із зростанням кількості кібератак на IoT-інфраструктуру.

Постановка завдання. Метою роботи є проведення досліджень, реалізація розподіленої платформи збору та обробки отриманих даних з сенсорів, керування розподіленими пристроями, а також впровадження системи кіберзахисту для запобігання несанкціонованому доступу до інформації та втраті конфіденційних даних. Об'єктом дослідження є побудована на базі IoT-пристроїв система, яка передбачає можливість масштабування, гнучку конфігурацію та безпечне управління в реальному часі. Предметом дослідження є сукупність технічних і програмних засобів, які забезпечують безпечну комунікацію між IoT-пристроями, включаючи архітектуру взаємодії компонентів, протоколи обміну, криптографічні методи захисту та інтерфейс користувача. Виходячи з того, що сучасні IoT-системи стикаються із багатьма викликами у сфері кібербезпеки, визначаємо що ці питання вимагають комплексного підходу до їх вирішення. Дослідження Unit 42 демонструє, що 98 % IoT-трафіку не шифрується, що робить його надзвичайно вразливим для перехоплення та модифікації зловмисниками. Одночасно спостерігається експоненціальне зростання кількості кібератак на IoT-інфраструктуру, при цьому 41 % подібних атак використовує вразливість пристроїв, які мають слабкі засоби автентифікації і погану сегментацію мереж. Також те, що IoT-пристрої характеризуються обмеженими обчислювальними ресурсами та енергоспоживанням, суттєво ускладнює впровадження традиційних засобів захисту інформації. А застосування пристроїв різних виробників з різними протоколами та стандартами безпеки, створює додаткові виклики для забезпечення комплексного захисту. Спираючись на це маємо, що відсутність єдиних стандартів безпеки призводить до того, що загальний рівень захисту системи визначається найслабшим сегментом або елементом системи. Тому для досягнення мети роботи необхідно здійснити аналіз сучасних технологій і протоколів IoT-комунікацій з точки зору їх безпеки, а також визначити архітектурні рішення для побудови розподіленої IoT-системи із високим рівнем захисту, що включає вибір оптимальних криптографічних методів та протоколів безпеки, адаптованих для умов застосування обмежених обчислювальних ресурсів. Практичною частиною є реалізація IoT-системи із використанням сучасних технологій, включаючи мікроконтролери ESP32, сенсори та MQTT-брокер з підтримкою TLS-шифрування на транспортному рівні стеку TCP/IP. Розподілена IoT-система включає: сенсорні пристрої на базі мікроконтролеру

ESP32; канали передачі даних із використанням захищених протоколів; серверну інфраструктуру із засобами кібербезпеки та інтерфейс клієнта із контрольованим доступом. При цьому отримали універсальне та масштабоване рішення для безпечного збору та обробки даних IoT-пристроїв, яке можна адаптувати для різних напрямків із урахуванням специфічних вимог до безпеки та продуктивності.

Виклад основного матеріалу. Діаграми послідовності зазвичай детально відображають хронологічну послідовність взаємодії між об'єктами системи під час виконання конкретного варіанту використання, тому у даному випадку, діаграма демонструє критично важливий сценарій забезпечення безпеки доступу до IoT-платформи через багаторівневу систему перевірки особи користувача та створення захищених робочих сесій (рис. 1). Процес автентифікації ініціюється користувачем через введення ідентифікатора (user_id) та вибір відповідної ролі (admin, operator, viewer) в інтерфейсі Auth GUI. Цей етап включає клієнтську валідацію введених даних для запобігання передачі порожніх або некоректних значень на сервер.

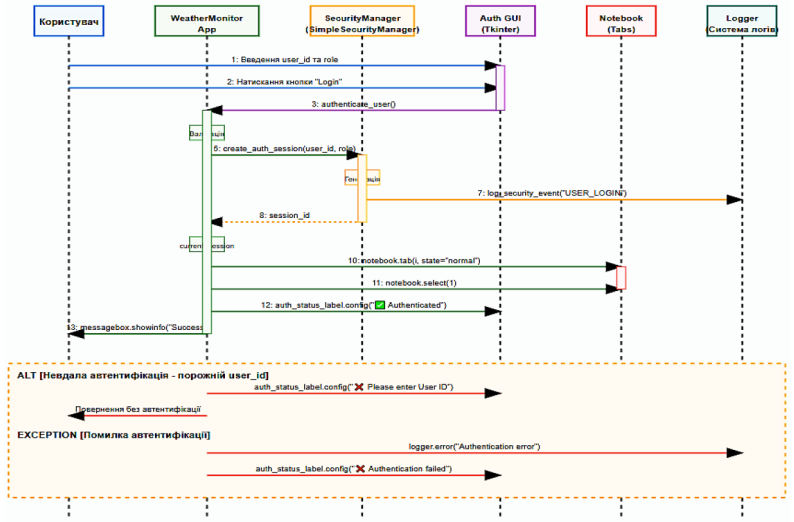

Рис. 1. Процес автентифікації користувача

Всі рішення оптимізовані для забезпечення масштабованості, надійності та ефективності обробки даних при дотриманні принципів Defense in Depth та Zero Trust Security. Архітектура системи побудована на основі гібридної моделі, яка поєднує переваги хмарних технологій для важливих сервісів та локальних обчислень при забезпеченні автономної роботи. Система реалізує принцип слабкої зв'язаності між всіма компонентами, використовуючи MQTT-протокол із забезпеченням стійкості до мережевих збоїв та масштабування. Багаторівнева архітектура включає чіткий розподіл відповідальності між рівнями системи, що забезпечує її модульність та можливість незалежної заміни окремих компонентів на більш сучасні (рис. 2). Локальна мережа організована як захищений периметр з WPA3 шифруванням та використанням частот 2.4/5 ГГц для оптимального покриття. Client Workstation базується на операційних системах Windows 10/11 або Linux Ubuntu 20.04+ з мінімальними вимогами до ресурсів: 512MB RAM та 100MB дискового простору. Python 3.8+ runtime забезпечує кросплатформену сумісність та доступ до широкого екосистему бібліотек для обробки даних та візуалізації.

ESP32-пристрої базуються на мікроконтролері ESP32-WROOM-32 із вбудованими модулями Wi-Fi та Bluetooth. Кожен пристрій оснащений датчиком DHT22 для вимірювання температури та вологості з точністю ±0.5 °C та ±2 % відповідно.

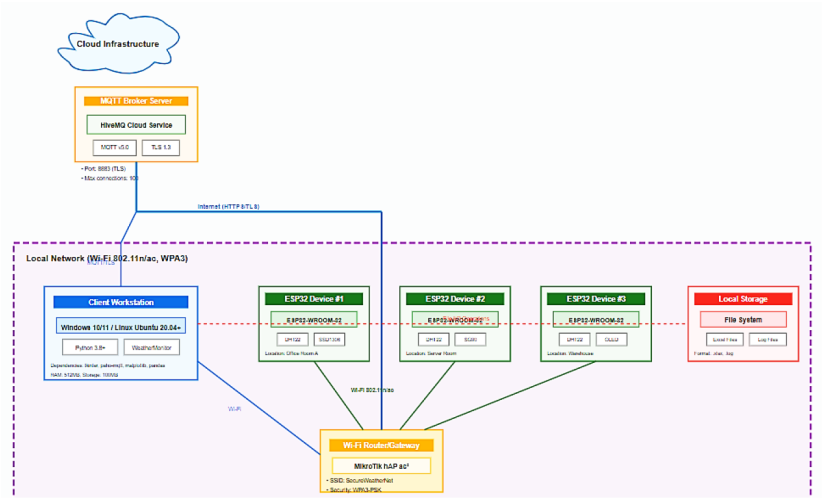

Рис. 2. Діаграма розміщення

Інтерфейс користувача системи базується на принципах User-Centered Design (UCD) та сучасних підходах до створення інтуїтивних інтерфейсів для IoT-систем з підвищеними вимогами до безпеки. Загальна інфраструктура інтерфейсу розроблена з урахуванням специфічних потреб різних категорій користувачів та необхідності забезпечення ефективної взаємодії з розподіленою системою моніторингу в режимі реального часу. Застосовано модульний підхід з чітким розділенням функціональних зон та логічною організацією інформаційних потоків. Інтерфейс реалізує принцип прогресивного розкриття, де базові функції доступні безпосередньо, а додаткові розкриваються через контекстні меню та додаткові панелі. Рисунок 3 демонструє початковий екран автентифікації системи, яка є гібридним середовищем поєднання симуляції Wokwi та веб-інтерфейсу безпеки. Ліва частина екрану відображає симуляцію схеми ESP32 з підключеними компонентами: DHT22 сенсором температури та вологості; OLED-дисплеєм SSD1306 та SG90 системи охолодження. Права частина екрану наводить форму автентифікації з полями введення User ID та вибору ролі клієнта. Нижня частина екрану містить консольну частину середовища, яка надає технічні деталі ініціалізації системи. Це є налаштування периферійних пристроїв, встановлення Wi-Fi з’єднання та підключення до MQTT.

Рисунок 4 наводить основний робочий інтерфейс системи після успішної автентифікації. Центральним елементом є інтерактивний графік, який в реальному часі (з часовими мітками на горизонтальній осі та числовими значеннями на вертикальній) відображає температуру (°C) та вологість (%).

Користувач може динамічно змінювати температуру (в даному випадку встановлена на 61.1 °C) та вологість (61.0 %) для тестування різних сценаріїв роботи системи. Нижня панель інтерфейсу містить індикатори стану системи (OK, WARNING, ALARM), елементи управління системою охолодження (Turn ON/OFF), поле для відправки повідомлень на OLED-дисплей та кнопки збереження даних і виходу з системи. Такий розподіл функцій забезпечує ефективний workflow для операторів

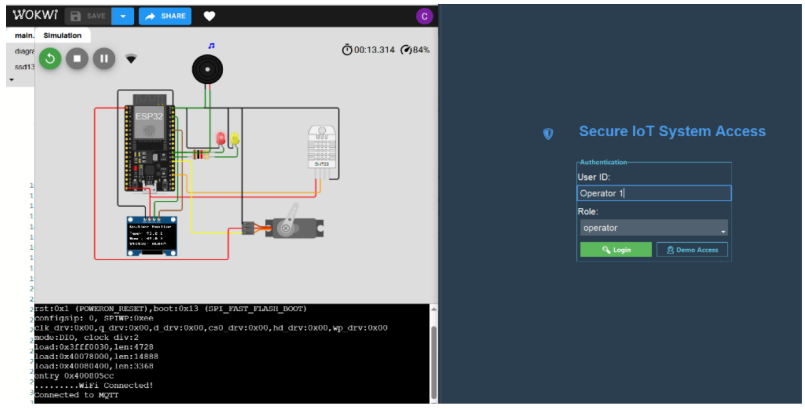

Рис. 3. Процес проходження автентифікації

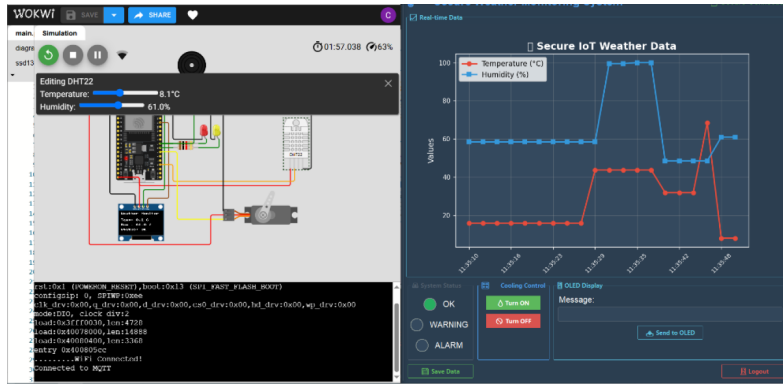

Рис. 4. Інтерфейс моніторингу даних сенсорів

моніторингу. Також маємо можливість дослідити функціональність віддаленого управління пристроями через MQTT-команди, наприклад процес відправки команди управління приладом, де OLED-дисплей відображає інформацію з показниками температури (T: 80.9 °C), вологості (H: 100.0 %) та статусу безпеки (STATUS: ALARM). Або дослідити функціональність відправки текстових повідомлень на OLED-дисплей. При цьому дисплей відображає повідомлення, демонструючи можливість віддаленої комунікації з операторами через локальні дисплеї пристроїв. Консоль показує процес отримання повідомлення через топік «wokwi-weather/message», парсинг JSON-структури та відображення повідомлення на дисплеї (рис. 5).

Модульна структура інтерфейсу дозволяє динамічно перерозподіляти його елементи залежно від доступного простору екрану, зберігаючи при цьому логічну організацію інформації.

Висновки. У роботі проведено дослідження методів та технологій для реалізації розподіленої IoT-системи збору, передачі та обробки телеметричних даних. Система забезпечує безперервний моніторинг температури та вологості з точністю ±0.5 °C та ±2 % відповідно, що відповідає промисловим стандартам точності вимірювань. Система кібербезпеки реалізує багаторівневий захист інформації, використовуючи: TLS-шифрування MQTT-трафіку; JWT-автентифікацію користувачів; рольовий контроль доступу та комплексний моніторинг подій. Архітектура

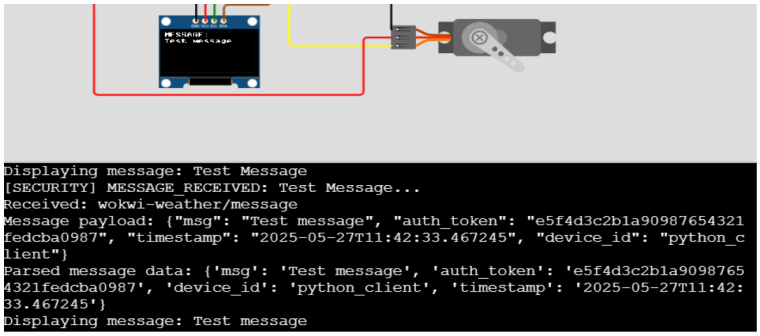

Рис. 5. Інтерфейс відправки повідомлень на OLED-дисплей

системи базується на мікросервісному підході із чітким розділенням відповідальності між компонентами. ESP32-мікроконтролери забезпечують автономний збір даних навіть при тимчасовій втраті мережевого з’єднання, хмарний MQTT-брокер гарантує надійну доставку повідомлень, а клієнтський додаток надає інтуїтивний інтерфейс для моніторингу та управління. Інноваційною є інтеграція середовища Wokwi із реальним програмним забезпеченням, що дозволяє проводити комплексне тестування функціональності без необхідності використання фізичного обладнання. Модульна архітектура системи дозволяє легке масштабування, а підтримка до 100 одночасно підключених пристроїв, забезпечує покриття великих територій, зберігаючи централізоване управління та моніторинг. Реалізована система має перспективи для подальшого розширення функціональності. Планується розширення можливостей аналітики даних через інтеграцію з платформами штучного інтелекту та створення API для інтеграції з корпоративними системами управління.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Kumar R., Sharma S., Patel P. Cryptography Algorithms for Enhancing IoT Security. International Journal of Advanced Computer Science and Applications. 2023. Vol. 14, No. 3. P. 245–257.

2. Sethi P., Sarangi S. Internet of Things: Architectures, Protocols, and Applications. Journal of Electrical and Computer Engineering. 2017. Vol. 2017. Article ID 9324035. 25 p.

3. MQTT Version 5.0 / OASIS Standard. OASIS, 2019. 137 p.

4. Киричек, Г. Г. Керування інформаційними потоками на всіх рівнях ієрархії отримання знань. Радіоелектроніка, інформатика, управління. 2010. № 1. С. 70–78.

5. Zhang L. [et al.]. Efficiency and Security Evaluation of Lightweight Cryptographic Algorithms for Resource-Constrained IoT Devices. Sensors. 2024. Vol. 24, No. 12. Article 4008. 28 p.

6. Johnson M., Smith A., Brown K. Enhancing IoT Security: An Innovative Key Management System for Lightweight Block Ciphers. PMC Sensors. 2023. Vol. 23, No. 18. Article PMC10535244. 15 p.

7. Киричек Г. Г., Гаркуша В. Ю. Віртуалізація хостів на основі Proxmox VE в умовах надлишкового використання ресурсів. *Вчені записки ТНУ імені В. І. Вернадського. Серія «Технічні науки»*. 2021. Вип. 32 (71). № 1. С. 78–84.

8. Chen W., Liu Y., Wang X. A hybrid encryption approach for efficient and secure data transmission in IoT devices. Journal of Engineering and Applied Science. 2024. Vol. 71. Article 459. 18 p.

9. Tiahunova M., Tronkina O., Kirichek G., Skrupsky S. The neural network for emotions recognition under special conditions, CEUR Workshop Proceedings 2864 (2021). 121–134.

10. Коваленко М. В., Савченко Т. П. Кібербезпека в системах Інтернету речей: сучасні виклики та рішення. Науковий вісник Ужгородського національного університету. Серія: Математика і інформатика. 2023. Вип. 1(42). С. 112–125.

11. Rahman M. A., Hossain M. S. IoT-based environmental monitoring systems: A comprehensive survey. IEEE Internet of Things Journal. 2023. Vol. 10, No. 8. P. 6891–6912.

12. Рудьковський О. Р., Киричек Г. Г. Програмний комплекс з підтримки розподіленої взаємодії мережевих пристроїв та додатків. Вчені записки ТНУ ім. В. І. Вернадського. Серія «Технічні науки». 2021.Вип. 32(71). № 2. С. 229–234.

REFERENCES:

1. Kumar R., Sharma S., Patel P. (2023). Cryptography Algorithms for Enhancing IoT Security. International Journal of Advanced Computer Science and Applications, 14(3), 245–257.

2. Sethi P., Sarangi S. (2017). Internet of Things: Architectures, Protocols, and Applications. Journal of Electrical and Computer Engineering, 2017, Article ID 9324035, 25 p.

3. MQTT Version 5.0 / OASIS Standard. OASIS, 2019, 137 p.

4. Kyrychek, H. H. (2010). Keruvannia informatsiinymy potokamy na vsikh rivniakh iierarkhii otrymannia znan. [Management of information streams at all hierarchy levels of training], *Radio electronics computer science control*, 1, 70–78 [in Ukrainian].

5. Zhang L. [et al.]. (2024). Efficiency and Security Evaluation of Lightweight Cryptographic Algorithms for Resource-Constrained IoT Devices. Sensors, 24(12), Article 4008, 28 p.

6. Johnson M., Smith A., Brown K. (2023). Enhancing IoT Security: An Innovative Key Management System for Lightweight Block Ciphers. PMC Sensors, 23(18), Article PMC10535244, 15 p.

7. Kyrychek H. H., Harkusha V. Yu. (2021). Virtualizatsiia khostiv na osnovi Proxmox VE v umovakh nadlyshkovoho vykorystannia resursiv [Virtualization of hosts based on Proxmox VE in conditions of excessive use of resources]. *Scientific notes of TNU named after V. I. Vernadskyi. Series «Technical Sciences»*, 32(71), 1, 78–84 [in Ukrainian].

8. Chen W., *Liu* Y., Wang X. (2024). A hybrid encryption approach for efficient and secure data transmission in IoT devices. Journal of Engineering and Applied Science, Vol. 71, Article 459, 18 p.

9. Tiahunova M., Tronkina O., Kirichek G., Skrupsky S. (2021). The neural network for emotions recognition under special conditions, CEUR Workshop Proceedings 2864, 121–134.

10. Kovalenko M. V., Savchenko T. P. (2023). Kiberbezpeka v systemakh Internetu rechei: suchasni vyklyky ta rishennia [Cybersecurity in Internet of Things systems: modern challenges and solutions], *Scientific Bulletin of Uzhhorod National University. Series: Mathematics and Informatics*, 1(42), 112–125 [in Ukrainian].

11. Rahman M. A., Hossain M. S. (2023). IoT-based environmental monitoring systems: A comprehensive survey. IEEE Internet of Things Journal, 10 (8), 6891–6912.

12. Rudkovskyi O. R., Kyrychek H. H. (2021). Prohramnyi kompleks z pidtrymky rozpodilenoi vzaiemodii merezhevykh prystroiv ta dodatkiv [A software complex supporting the distributed interaction of network devices and applications]. *Scientific notes of TNU named after V. I. Vernadskyi. Series "Technical Sciences"*, 32(71), 2, 229–234 [in Ukrainian].

Дата першого надходження рукопису до видання: 23.08.2025
Дата прийнятого до друку рукопису після рецензування: 19.09.2025
Дата публікації: 30.10.2025

CONTENTS