УДК 004
DOI https://doi.org/10.32782/2521-6643-2024-2-68.4

Погребняк А. В., доктор технічних наук, професор кафедри міжнародного туризму та готельно-ресторанного бізнесу Університету митної справи та фінансів
ORCID: 0000-0003-3214-6410

Яковенко В. О., доктор технічних наук, професор кафедри комп'ютерних наук та інженерії програмного забезпечення Університету митної справи та фінансів
ORCID: 0000-0001-7762-5410

Клим В. Ю., кандидат технічних наук, доцент кафедри кібербезпеки та інформаційних технологій Університету митної справи та фінансів
ORCID: 0000-0002-5887-1955

Яковенко Т. Ю., кандидат економічних наук, доцент кафедри комп'ютерних наук та інженерії програмного забезпечення Університету митної справи та фінансів
ORCID: 0000-0003-1900-8283

ПРОБЛЕМИ ІНТЕГРАЦІЇ ІОТ У КОМП'ЮТЕРНІ МЕРЕЖІ

Стаття розглядає результати дослідження з інтеграції IoT-технологій (Internet of Things, IoT), що дозволяє фізичним пристроям з'єднуватися через мережі та обмінюватися даними без необхідності людського втручання. У цій роботі розглянуто декілька основних наукових статей, які висвітлюють різні аспекти IoT, від його архітектури до викликів безпеки. Аналіз наукових робіт з інтеграції Інтернету Речей (IoT) показує, що ця технологія активно розвивається, охоплюючи різні аспекти, від архітектури до безпеки. Попередні дослідження вказують на важливість подальшого розвитку стандартів, протоколів і технологій для забезпечення безпечної та ефективної інтеграції IoT у різних сферах діяльності. Це, своєю чергою, відкриває нові можливості для інновацій та розвитку в майбутньому.

Метою дослідження визначено аналіз основних проблем інтеграції IoT у комп'ютерні мережі та пропонуються можливі рішення для їх подолання. У межах означеної мети поставлені наступні завдання: надати характеристику глобальної мережі підключених до інтернету пристроїв, які обмінюються даними та взаємодіють між собою; визначити її основні компоненти та рівні, з яких складається її архітектура; порівняти мережеві технології за масштабованістю; проаналізувати та порівняти основні кіберзагрози для IoT; зробити аналіз впливу типу IoT – системи на пропускну здатність мережі; описати особливості основних протоколів, що використовуються IoT- пристроями; проаналізувати переваги використання Software-Defined Networking для вирішення проблеми масштабування; визначити основні методи захисту IoT-систем; порівняти пропускну здатність для різних типів IoT-систем; запропонувати використання енергоефективних технологій для автономної довготривалої роботи IoT-пристроїв; порівняти пропускну здатність та рівні затримки для різних типів IoT-мереж.

Захист даних та забезпечення безпеки мереж IoT є однією з найбільших проблем, оскільки велика кількість підключених пристроїв збільшує вразливість до кібератак. Використання сучасних методів шифрування, аутентифікації та сегментації мережі є ключовими для підвищення безпеки IoT-систем. Інтеграція IoT у комп'ютерні мережі відкриває нові можливості для розвитку інтелектуальних систем у різних сферах, від розумних міст до промислового виробництва. Однак для успішної реалізації необхідно враховувати наведені вище виклики та застосовувати відповідні рішення для їх подолання.

Ключові слова: *фізичні об'єкти, комп'ютерні мережі, архітектура IoT, масштабованість, кібербезпека, пропускна здатність, латентність, протокол, енергоефективність, оптимізація, обсяг даних.*

Pohrebniak A. V., Yakovenko V. O., Klym V. Yu., Yakovenko T. Yu. Challenges of IoT integration into computer networks

This article examines the results of a study on the integration of Internet of Things (IoT) technologies, which enables interconnection among physical devices and exchange data over networks without human intervention. The paper reviews several fundamental research articles covering various aspects of IoT, from its architecture to security challenges. An analysis of IoT integration research indicates the rapid evolution of this technology addressing multiple aspects ranging from architecture

to security. Highlight the significance of developing standards, protocols, and technologies to ensure secure and efficient IoT integration across various fields, unlocking potential for future innovation and advancement.

The research aims to analyze key challenges of IoT integration into computer networks and suggests potential solutions to overcome them. Objectives within this aim include providing an overview of the global network of internet-connected devices that exchange data and interact with each other, identifying the primary components and layers comprising its architecture, comparing network technologies in terms of scalability, and analyzing major cyber threats to IoT. Further goals include examining assessing the effect of different IoT system types on network bandwidth, detailing key protocols used by IoT devices, analyzing the benefits of Software-Defined Networking (SDN) for scalability issues, identifying key IoT protection methods, comparing bandwidth for different IoT systems, recommending energy-efficient technologies for autonomous IoT device operation, and comparing bandwidth and latency levels for various types of IoT networks.

Data protection and IoT network security remain significant challenges due to the increased vulnerability to cyberattacks from a high number of connected devices. Modern encryption, authentication, and network segmentation methods are crucial for enhancing IoT system security. IoT integration into computer networks creates new opportunities for developing intelligent systems across various domains, from smart cities to industrial production. However, successful implementation requires addressing these challenges and applying appropriate solutions to overcome them.

Key words: *physical objects, computer networks, IoT architecture, scalability, cybersecurity, bandwidth, latency, protocol, energy efficiency, optimization, data volume.*

Постановка проблеми. Інтернет речей (Internet of Things, IoT) – це концепція, що дозволяє фізичним пристроям з'єднуватися через мережі та обмінюватися даними без необхідності людського втручання. Це веде до нових можливостей у різних галузях економіки, соціальної сфери, екологічних, політичних сегментах життєдіяльності суспільства.

Традиційні комп'ютерні мережі зазвичай не розраховані на велику кількість з'єднаних пристроїв, які постійно генерують дані. Через це виникають численні виклики, пов'язані з безпекою, масштабованістю, керуванням даними та сумісністю протоколів.

Аналіз останніх досліджень і публікацій. Інтернет Речей (IoT) став однією з найважливіших технологічних інновацій сучасності, яка охоплює різноманітні галузі. Він надає можливості для інтеграції фізичних об'єктів у цифровий світ, що відкриває нові горизонти для бізнесу, науки та повсякденного життя. У цьому аналізі розглянемо декілька основних наукових статей, які висвітлюють різні аспекти IoT, від його архітектури до викликів безпеки.Атзорі Л., Ієра А. та Морабіто Г. (Atzori, L., Iera, A., & Morabito, G. 2010) провели систематичний огляд IoT, акцентуючи на ключових концепціях, таких як об'єкти, що взаємодіють через Інтернет. Вони підкреслили значення даних у формуванні мережі IoT, зазначивши, що інтеграція об'єктів вимагає нових підходів до управління та обробки інформації [1]; Борджіа Е. (Borgia E. 2014) описує основні характеристики IoT, включаючи різноманіття застосувань і відкриті питання, що потребують подальшого дослідження. Він підкреслює важливість розуміння не лише технологічних аспектів, але й соціальних і етичних викликів, пов'язаних із впровадженням IoT [2]; Губбі Дж. та інш. (Gubbi, J. et al. 2013) представляють архітектурні компоненти IoT, акцентуючи увагу на їх інтеграції з чинними технологіями. Вони вказують на необхідність розробки нових стандартів та протоколів для забезпечення ефективної роботи IoT [3]; Лі С. та інш. (Li S. et al. 2015) провели систематичний огляд технологій IoT, наголошуючи на їх здатності до адаптації в різних галузях. Вони зазначають, що майбутній розвиток IoT залежатиме від подальшого вдосконалення архітектурних рішень та адаптації до специфічних умов експлуатації [4]; Занелла А. та інш. (Zanella, A. et al. 2014) розглянули, як IoT може бути впроваджений у розумні міста, зокрема в управлінні енергетичними ресурсами, транспортом та безпекою. Вони описують конкретні приклади використання IoT для підвищення ефективності міських систем [5]; Лі І. та Лі К. (Lee, I. & Lee, K. 2015) аналізують вплив IoT на бізнес-середовище, підкреслюючи потенційні переваги та виклики, з якими стикаються підприємства під час впровадження IoT-рішень [6]; Янг Я. та інш. (Yang, Y. et al. 2017) детально досліджують проблеми безпеки та конфіденційності в IoT. Вони відзначають, що значне зростання IoT створює нові ризики та загрози, якими можуть скористатися шахраї, конкуренти чи зловмисники [7]; Фаруг М. У. та інш. (Farooq, M. U. et al. 2015) акцентують увагу на критичних аспектах безпеки IoT, відзначаючи ризики, пов'язані з вразливостями у системах. Вони пропонують стратегії для покращення безпеки, включаючи використання криптографічних методів [8]; Чан М. та інш. (Chen, M. et al. 2017) аналізують архітектури та стандарти комунікацій між машинами (M2M) в контексті IoT. Вони вказують на важливість розробки ефективних стандартів для забезпечення безперебійної взаємодії між різними пристроями [9]; Аль-Фугаха А. та інш. (Al-Fuqaha, A. et al. 2015) пропонують всебічний огляд технологій, які підтримують IoT, включаючи протоколи, платформи та апаратні засоби. Вони підкреслюють важливість інтеграції цих технологій для створення єдиної екосистеми IoT [10]; В.А. Язіна, А.В. Погребняк, О.В. Сабіров (2021), на прикладі впровадження у систему управління сучасного ресторанного закладу електронного меню, доводять значні переваги цієї інновації як для клієнтів, так і для персоналу підприємства і, у цілому, для ресторанного бізнесу [11].

Аналіз наукових робіт з інтеграції Інтернету Речей (IoT) показує, що ця технологія активно розвивається, охоплюючи різні аспекти, від архітектури до безпеки. Попередні дослідження вказують на важливість

подальшого розвитку стандартів, протоколів і технологій для забезпечення безпечної та ефективної інтеграції IoT у різних сферах діяльності. Це, своєю чергою, відкриває нові можливості для інновацій та розвитку в майбутньому.

Мета дослідження. Стаття присвячена аналізу дослідження з основних проблем інтеграції IoT у комп'ютерні мережі та пропонує можливі рішення для їх подолання.

Виклад основного матеріалу дослідження. Інтернет речей можна визначити як глобальну мережу підключених до інтернету пристроїв, які обмінюються даними та взаємодіють між собою. Тож визначимо основні компоненти IoT (Таблиця 1) [1-3]:

- **Пристрої IoT:** сенсори, камери, контролери.
- **Мережеве обладнання:** маршрутизатори, комутатори, шлюзи.
- **Програмне забезпечення:** платформи для обробки даних та аналітики.
-

Таблиця 1

Основні компоненти системи IoT

Компоненти IoT	Функції компонентів
Сенсорне обладнання	Сенсори, що збирають дані з оточення і передають їх через мережу.
Шлюзи	Пристрої, що забезпечують з'єднання між IoT і основними мережами.
Хмарні сервери	Використовуються для обробки, зберігання та аналізу великих даних.
Програмні платформи	Програмні рішення для керування IoT пристроями і обробки інформації.

Розглянемо рівні, з яких складається архітектура IoT (Таблиця 2) [1-3] :

- **Рівень пристроїв:** тут розміщені всі фізичні сенсори та виконавчі пристрої.
- **Шлюзи та мережевий рівень:** забезпечують зв'язок між пристроями та хмарними серверами.
- **Хмарний рівень:** обробляє та аналізує великі масиви даних.

Таблиця 2

Рівні архітектури IoT

Рівень	Функціонал рівня
Рівень пристроїв	Включає фізичні пристрої, що збирають та передають дані.
Шлюзовий рівень	Виконує функцію з'єднання пристроїв із глобальними мережами через мережеве обладнання.
Хмарний рівень	Обробляє та зберігає дані, надаючи користувачам можливість доступу на відстані до керування пристроями.
Аналітичний рівень	Включає інструменти для аналізу зібраних даних і надання користувачам інформаційних рішень.

Однією із ключових проблем інтеграції IoT є масштабованість. Кількість IoT-пристроїв, підключених до мережі, зростає експоненційно, що створює значне навантаження на мережеву інфраструктуру. Традиційні мережі не завжди здатні обробляти велику кількість одночасних з'єднань та обміну даними, що може перевантажити мережі та знизити їх ефективність (Таблиця 3) [2-4].

Таблиця 3

Порівняння здатності мережевих технологій до масштабування

Мережеві технології	Кількість підключень	Швидкість передачі даних	Складність управління
Wi-Fi	Обмежена	Висока	Середня
Ethernet	Обмежена	Дуже висока	Низька
LoRaWAN	Висока	Низька	Складна
5G	Дуже висока	Дуже висока	Складна

Інтеграція IoT підвищує ризики кібербезпеки, оскільки кожен підключений пристрій може стати потенційною точкою уразливості. Кількість атак на IoT-системи постійно зростає, і, на жаль, не всі пристрої мають достатній рівень захисту. Перелік сучасних кіберзагроз для IoT наведено у Таблиці 4 [3, 4, 6-8].

Інтеграція великої кількості IoT-пристроїв може створювати проблеми з пропускною здатністю мережі, особливо в реальному часі, коли необхідно швидко обробляти й передавати великі обсяги даних. Затримки в передачі можуть критично вплинути на роботу таких систем, як інтелектуальні транспортні мережі, автоматизоване виробництво, сфера послуг та системи охорони здоров'я.(Таблиця 5) [4-7, 15].

Таблиця 4

Основні кіберзагрози для IoT

Тип атаки	Опис загроз
DoS-атака	Перевантаження мережі, що блокує доступ до сервісів.
Атака «людина посередині»	Перехоплення та модифікація даних між пристроями та сервером.
Несанкціонований доступ	Незаконне отримання контролю над пристроєм або мережею.
Шахрайство, фішинг	Використання соціальної інженерії для крадіжки конфіденційних даних.

Таблиця 5

Вплив типу IoT- системи на пропускну здатність мережі

Тип IoT-системи	Кількість даних на пристрій	Час передачі даних	Вимоги до затримки
Розумний дім	Низька	Невеликий	Помірна
Інтелектуальний транспорт	Висока	Критичний	Дуже низька
Охорона здоров'я	Середня	Високий	Низька
Промисловий інтернет речей (IIoT)	Висока	Дуже високий	Дуже низька

Одним із важливих викликів є сумісність різних протоколів, що використовуються IoT-пристроями та традиційними мережами. Протоколи, як-от **MQTT, CoAP** та **HTTP**, не завжди підтримують взаємодію з усіма мережевими пристроями, що може призвести до ускладнень у передачі даних між різними елементами системи. Перелік основних протоколів, що використовуються у IoT наведено у Таблиці 6 [6-8, 10].

Таблиця 6

Основні протоколи, що використовуються у IoT

Протокол	Опис призначення протоколу	Сумісність з традиційними мережами
MQTT	Легкий протокол для обміну повідомленнями	Обмежена
CoAP	Протокол для роботи з ресурсами у реальному часі	Середня
HTTP	Основний протокол для передачі гіпертексту	Висока
Zigbee	Протокол для малопотужних мереж	Низька

Багато IoT-пристроїв живляться від батарейок, що створює необхідність ефективного використання енергії. Інтеграція IoT у комп'ютерні мережі вимагає оптимізації як передачі даних, так і енергоефективності для забезпечення довготривалої роботи пристроїв. Використання енергоощадних технологій, таких як **NB-IoT** (Narrowband IoT), може допомогти вирішити цю проблему [7, 9].

Для вирішення проблеми масштабованості необхідно розробляти архітектури мереж, які підтримують динамічне масштабування та адаптацію до зростання кількості пристроїв. Одним із рішень може бути використання **SDN (Software-Defined Networking),** що дозволяє централізовано управляти мережею та швидко адаптувати її до нових вимог. У Таблиці 7 надано порівняльну характеристику традиційної архітектури та **Software-Defined Networking** [8-10]**.**

Таблиця 7

Переваги використання SDN для IoT

Характеристика	Традиційна архітектура	SDN
Гнучкість	Обмежена	Висока
Управління	Децентралізоване	Централізоване
Масштабованість	Обмежена	Дуже висока
Реагування на зміни	Повільне	Швидке

З метою зниження ризиків, пов'язаних із кібербезпекою, необхідно впроваджувати комплексні рішення для захисту даних та пристроїв. Використання методів **швидкої автентифікації, шифрування даних** та **сегментації мережі** допомагає значно підвищити захищеність IoT-систем. Також важливо використовувати засоби моніторингу для виявлення та попередження атак (Таблиця 8) [5-8].

Щоб уникнути проблем із пропускною здатністю та затримками, необхідно використовувати технології, що оптимізують передачу даних у реальному часі. Одним із таких рішень є використання протоколу **5G,** який забезпечує високу швидкість передачі даних та мінімальні затримки, що особливо важливо для критичних IoT-додатків. Порівняльну Таблицю 9 пропускної здатності наведено нижче [7, 9, 15].

Таблиця 8

Основні методи захисту IoT-систем

Метод захисту	Опис типу захищеності
Шифрування даних	Забезпечує конфіденційність і цілісність переданих даних.
Автентифікація	Перевірка достовірності пристроїв перед з'єднанням із мережею.
Сегментація мережі	Поділ мережі на ізольовані сегменти для зменшення ризиків.
Моніторинг мережі	Виявлення підозрілої активності та запобігання атакам у реальному часі.

Таблиця 9

Порівняння пропускної здатності для різних типів IoT-додатків

Тип IoT-додатка	Вимоги до пропускної здатності	Технології передачі даних
Інтелектуальні транспортні системи	Дуже висока	5G, Wi-Fi 6
Системи охорони здоров'я	Середня	NB-IoT, LTE-M
Розумний дім	Низька	Wi-Fi, Zigbee
Промислові IoT-системи	Висока	Ethernet, 5G

Для підвищення сумісності між різними IoT-протоколами та мережевими технологіями необхідно використовувати **шлюзи протоколів** та платформи для управління пристроями. Ці технології дозволяють поєднувати різні протоколи в єдиній системі та забезпечують ефективну взаємодію між IoT-пристроями.

Для забезпечення тривалої автономної роботи IoT-пристроїв необхідно використовувати енергоефективні технології, такі як **NB-IoT** та **LPWAN.** Вони дозволяють передавати невеликі обсяги даних з мінімальним енергоспоживанням, що особливо важливо для пристроїв, що працюють на батарейках.

Однією з найбільших проблем інтеграції IoT у традиційні комп'ютерні мережі є швидке зростання кількості підключених пристроїв. Згідно з прогнозами, кількість пристроїв IoT продовжуватиме зростати експоненційно. Це створює значне навантаження на наявні мережеві архітектури, які часто не здатні ефективно обробляти та передавати дані від такої кількості пристроїв.

Щоб знайти дані про прогнозоване зростання кількості IoT-пристроїв до 2030 року, можна звернутися до різних джерел. Наприклад, згідно з прогнозом IoT Analytics, очікується, що кількість підключених IoT-пристроїв досягне 18.8 мільярдів у 2024 році, з подальшим зростанням до 2030 року. Цей ріст значною мірою спричинено впровадженням нових технологій, таких як 5G, LTE-M, а також збільшенням кількості пристроїв у промисловому секторі та для розумного дому.

Інший аналіз показує, що глобальний ринок IoT буде продовжувати зростати на 9-10% щорічно, досягнувши до 2030 року значного числа пристроїв через розвиток технологій у галузі штучного інтелекту та промислового Інтернету речей (IIoT). Подібні дані можна знайти в дослідженнях IoT Analytics та Straits Research, які глибоко аналізують розвиток IoT-сектору та ключові тренди [9, 11-15].

Таблиця 10

Прогноз зростання кількості IoT-пристроїв до 2030 року

Рік	Кількість пристроїв (млрд)
2020	12
2023	15
2025	21
2030	29

Окрім зростання кількості пристроїв, інтеграція IoT у мережі також вимагає збільшення пропускної здатності для забезпечення якісної передачі даних у реальному часі. Особливо це стосується промислових систем, де затримки у передачі можуть призвести до серйозних наслідків (Таблиця 11) [9, 10].

Таблиця 11

Вимоги до пропускної здатності для різних типів IoT-мереж

Тип IoT-мережі	Пропускна здатність (Мбіт/с)
Промислові системи	>100
Смарт-домашні системи	10–50
Мобільні IoT-системи	5–15

Для деяких IoT-додатків, таких як системи розумного транспорту чи охорони здоров'я, мінімізація затримок у передачі даних є критично важливою. Технології 5G можуть значно зменшити затримку, забезпечуючи передачу даних практично в реальному часі.(Таблиця 12)[8-10,15] Проте для досягнення цієї мети потрібне подальше розширення мережевої інфраструктури.

Таблиця 12

Порівняння рівнів затримки у різних мережевих технологіях

Технологія передачі даних	Середня затримка (мс)
4G LTE	30–50
Wi-Fi	10–30
5G	<10

Інша серйозна проблема – це ефективне управління величезними обсягами даних, що генеруються IoT-пристроями. Необхідно впроваджувати інноваційні методи для зберігання та аналізу цих даних, щоб забезпечити швидке прийняття рішень та виявлення аномалій у реальному часі.

Часто пристрої IoT працюють в умовах обмеженого енергоспоживання, тому оптимізація витрат енергії є ще одним суттєвим викликом. Технології на основі **NB-IoT** або **LoRa** дозволяють мінімізувати енергоспоживання, однак це може бути недостатнім для деяких видів пристроїв, таких як промислові датчики.

Висновки та перспективи подальших досліджень. Інтеграція IoT у комп'ютерні мережі є складним, але надзвичайно важливим процесом для забезпечення ефективної роботи сучасних систем. У статті було розглянуто основні проблеми, які виникають при цьому, а також можливі рішення для їх подолання.

Зростання кількості IoT-пристроїв створює суттєві виклики для традиційної мережевої архітектури. Використання таких технологій, як SDN та NFV, дозволяє значно підвищити гнучкість та адаптивність мереж для роботи з великим обсягом пристроїв.

Захист даних та забезпечення безпеки мереж IoT є однією з найбільших проблем, оскільки велика кількість підключених пристроїв збільшує вразливість до кібератак. Використання сучасних методів шифрування, аутентифікації та сегментації мережі є ключовими для підвищення безпеки IoT-систем.

Забезпечення високої пропускної здатності та мінімізації затримок у мережах є важливим для ефективної роботи IoT-додатків, особливо в промисловому секторі. Впровадження технологій 5G та Wi-Fi 6 сприяє вирішенню цієї проблеми.

Багато IoT-пристроїв працюють на батарейках, тому ефективне управління енергією є критичним для їх довготривалої роботи. Використання низькоенергетичних технологій, таких як NB-IoT та LoRa, дозволяє значно продовжити термін роботи пристроїв.

Великий обсяг даних, який генерується пристроями IoT, вимагає використання спеціалізованих рішень для їх зберігання, обробки та аналізу. Використання хмарних технологій та технологій периферійних обчислень допомагає оптимізувати управління даними у реальному часі.

Безсумнівно, інтеграція IoT у комп'ютерні мережі відкриває нові можливості для розвитку інтелектуальних систем у різних сферах, від розумних міст до промислового виробництва. Однак для успішної реалізації необхідно враховувати наведені вище виклики та застосовувати відповідні рішення для їх подолання.

Список використаних джерел:

1. Atzori L., Iera A., Morabito G. The Internet of Things: A survey. Computer Networks. 2010. 54(15), P. 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010

2. Gubbi J., Buyya R., Marusic S., Palaniswami M. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems. 2013. 29(7). P. 1645-1660. https://doi.org/10.1016/j.future.2013.01.010

3. Li S., Xu L. D., Zhao S. The Internet of Things: A survey. Information Systems Frontiers. 2015. 17(2). P. 243-259. https://doi.org/10.1007/s10796-014-9492-7

4. Borgia, E. The Internet of Things vision: Key features, applications, and open issues. Computer Communications. 2014. 54. P. 1-31. https://doi.org/10.1016/j.comcom.2014.09.008

5. Perera C., Zaslavsky A., Christen P., Georgakopoulos D. (2014). Context-aware computing for the Internet of Things: A survey. IEEE Communications Surveys Tutorials. 2014. 16(1). P. 414-454. https://doi.org/10.1109/SURV.2013.030214.00183

6. Zanella A., Bui N., Castellani A. P., Vangelista L., Zorzi, M. Internet of Things for smart cities. IEEE Internet of Things Journal. 2014. 1(1). P. 22-32. https://doi.org/10.1109/JIOT.2014.2306328

7. Lee I., Lee K. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business Horizons. 2015. 58(4). P. 431-440. https://doi.org/10.1016/j.bushor.2015.03.008

8. Yang Y., Wu J., Zhang D., Huang, Y. A survey on security and privacy issues in Internet-of-Things. IEEE Internet of Things Journal. 2017. 4(5). P. 1254-1272. https://doi.org/10.1109/JIOT.2017.2694847

9. Farooq M. U., Shafique M. U., Alqurashi A. A survey on security challenges in Internet of Things (IoT). International Journal of Computer Applications. 2015. 119(16). P. 1-8. https://doi.org/10.5120/19547-1280

10. Chen M., Ma Y., Li Y., Wu D., Zhang Y. Machine-to-machine communications: Architectures, standards and applications. IEEE Communications Magazine. 2017. 55(4). P. 21-27. https://doi.org/10.1109/MCOM.2017.1600483

11. IoT Analytics. State of the IoT–Number of Connected Devices Continues to Grow Exponentially. IoT Analytics. 2021. Available at: https://iot-analytics.com/state-of-the-iot-2021-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/

12. Statista. Internet of Things (IoT) connected devices worldwide 2019-2030. Available at: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

13. Straits Research. Global Internet of Things (IoT) Market: Forecast and Trends 2021-2030. Straits Research. Available at: https://straitsresearch.com/report/internet-of-things-iot-market

14. Ericsson. IoT Connections Outlook. Ericsson Mobility Report. 2020. Available at:https://www.ericsson.com/en/reports-and-papers/mobility-report/articles/iot-connections-outlook

15. В.А. Язіна, А.В. Погребняк, О.В. Сабіров (2021). Електронне меню як ефективний інтерактивний сервіс сучасних підприємств ресторанного господарства. Причорноморські економічні студії. 2021. с. 53-56. https://doi.org/10.32843/bses.72-32

References:

1. Atzori L., Iera, A., Morabito, G. (2010) The Internet of Things: A survey. Computer Networks, 54(15), 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010

2. 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

3. Li, S., Xu, L. D., & Zhao, S. (2015). The Internet of Things: A survey. Information Systems Frontiers, 17(2), 243-259. https://doi.org/10.1007/s10796-014-9492-7

4. Borgia, E. (2014). The Internet of Things vision: Key features, applications, and open issues. Computer Communications, 54, 1-31. https://doi.org/10.1016/j.comcom.2014.09.008

5. Perera, C., Zaslavsky, A., Christen, P., & Georgakopoulos, D. (2014). Context-aware computing for the Internet of Things: A survey. IEEE Communications Surveys & Tutorials, 16(1), 414-454. https://doi.org/10.1109/SURV.2013.030214.00183

6. Zanella, A., Bui, N., Castellani, A. P., Vangelista, L., & Zorzi, M. (2014). Internet of Things for smart cities. IEEE Internet of Things Journal, 1(1), 22-32. https://doi.org/10.1109/JIOT.2014.2306328

7. Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business Horizons, 58(4), 431-440. https://doi.org/10.1016/j.bushor.2015.03.008

8. Yang, Y., Wu, J., Zhang, D., & Huang, Y. (2017). A survey on security and privacy issues in Internet-of-Things. IEEE Internet of Things Journal, 4(5), 1254-1272. https://doi.org/10.1109/JIOT.2017.2694847

9. Farooq, M. U., Shafique, M. U., & Alqurashi, A. (2015). A survey on security challenges in Internet of Things (IoT). International Journal of Computer Applications, 119(16), 1-8. https://doi.org/10.5120/19547-1280

10. Chen, M., Ma, Y., Li, Y., Wu, D., & Zhang, Y. (2017). Machine-to-machine communications: Architectures, standards and applications. IEEE Communications Magazine, 55(4), 21-27. https://doi.org/10.1109/MCOM.2017.1600483

11. IoT Analytics. (2021). State of the IoT–Number of Connected Devices Continues to Grow Exponentially. IoT Analytics. Available at: https://iot-analytics.com/state-of-the-iot-2021-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/

12. Statista. (2021). Internet of Things (IoT) connected devices worldwide 2019-2030. Available at: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

13. Straits Research. (2023). Global Internet of Things (IoT) Market: Forecast and Trends 2021-2030. Straits Research. Available at: https://straitsresearch.com/report/internet-of-things-iot-market

14. Ericsson. (2020). IoT Connections Outlook. Ericsson Mobility Report. Available at: https://www.ericsson.com/en/reports-and-papers/mobility-report/articles/iot-connections-outlook

15. V.A. Yazina, A.V. Pohrebnyak, O.V. Sabirov (2021). Elektronne menu yak efektyvnyi interaktyvnyi servis suchasnykh pidpryiemstv restorannoho hospodarstva. Prychornomorski ekonomichni studii, 53-56. https://doi.org/10.32843/bses.72-32