

Моделі побудови мереж інтернету речей для управління інфраструктурою міста

Анастасія Кондакова¹, Олександр Корецький²

¹ Київський національний університет будівництва і архітектури
пр-т Повітряних Сил, 31, м.Київ, Україна, 03037

² Державний університет інформаційно-комунікаційних технологій
вул. Солом'янська, 7, м. Київ, Україна, 03110,

¹ a_kondakova@ukr.net, <https://orcid.org/0000-0003-1302-2244>

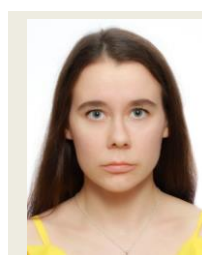
² okoretsky@gmail.com, <https://orcid.org/0009-0001-4809-7556>

Received 17.09.2024, accepted 30.10.2024

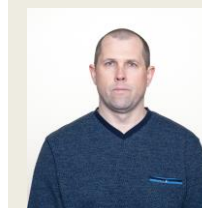
<https://doi.org/10.32347/st.2024.2.1901>

Анотації. У роботі розглядаються сучасні підходи до впровадження технологій IoT для ефективного управління міською інфраструктурою. Основна увага приділена аналізу мережевих архітектур, що використовуються для збирання та передачі даних у системах розумних міст. Порівнюються різні моделі побудови мереж, зокрема однохопові та багатохопові мережі, а також топології WSN. Робота акцентує на перевагах і недоліках цих мереж у контексті енергоспоживання, масштабованості та стабільності. Особлива увага приділяється ієрархічним моделям, що дозволяють знизити енерговитрати та підвищити ефективність мережі. Проаналізовано застосування IoT у ключових сферах міської інфраструктури, таких як транспорт, енергетика та водопостачання. Також детально розглянуто питання кібербезпеки IoT-систем, включаючи автентифікацію, шифрування даних та забезпечення надійності зв'язку. Окремо обговорюється роль CPS та сенсорних вузлів, які забезпечують моніторинг і контроль міських ресурсів у реальному часі. Розглянуто математичні моделі для оптимізації трафіку в мережах IoT, зокрема використання теорії черг для забезпечення QoS. Зроблено висновки щодо ефективності впровадження IoT для управління міськими ресурсами, що дозволяє підвищити надійність міської інфраструктури та покращити умови життя мешканців. Обґрунтовано застосування в IoT-системах мікросервісного програмного забезпечення та визначені напрямки наукових досліджень, спрямованих на його втілення в IoT-системи управління інфраструктурними об'єктами.

Дослідження відкриває нові перспективи для застосування IoT у розумних містах та вказує на необхідність подальшого вивчення



Анастасія Кондакова
Аспірант кафедри
кібербезпеки та
комп'ютерної інженерії,
КНУБА



Олександр Корецький
Аспірант кафедри
штучного інтелекту ДУІКТ

питань безпеки та енергозбереження в таких системах.

Ключові слова: IoT, міська інфраструктура, розумні міста, WSN, енергоефективність, CPS, мікросервісне програмне забезпечення

ПОСТАНОВКА ПРОБЛЕМИ

У сучасних умовах інтенсивної урбанізації та стрімкого зростання міст технології, які дозволяють ефективно управляти міською інфраструктурою, набувають дедалі більшої актуальності. Однією з найбільш перспективних концепцій у цьому контексті є Інтернет речей (далі IoT), що забезпечує обмін даними між пристроями та системами для автоматизованого контролю й управління міськими ресурсами [№][№]. У таких містах, як Сінгапур та Барселона, впровадження IoT сприяло значному підвищенню ефективності використання ресурсів і скороченню операційних витрат,

дозволивши оперативно реагувати на зміни інфраструктурних потреб. Інтеграція IoT з міською інфраструктурою дає змогу підвищити ефективність використання ресурсів, зменшити операційні витрати та покращити якість життя мешканців [№].

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ

Останні дослідження у сфері IoT для розумних міст охоплюють кілька ключових напрямків. Одним із важливих аспектів є управління міськими ресурсами та підвищення енергоефективності. Зокрема, Маркуц [1] акцентує на використанні IoT для автоматизованих систем управління ресурсами, що сприяє енергозбереженню, тоді як Gómez [4] розглядає застосування IoT для моніторингу екологічних параметрів у міському середовищі. Інші дослідження зосереджені на архітектурі мереж та протоколах передачі даних. Публікації [5; 7; 8] описують різноманітні підходи до побудови IoT-мереж у розумних містах, включаючи розробки, які забезпечують масштабованість і стабільність мережевої інфраструктури. Також велика увага приділяється питанням безпеки. Aggarwal [2] і Garcia-Retuerta [3] аналізують виклики кібербезпеки та захисту даних в IoT-системах, що включає проблеми автентифікації та шифрування інформації. Хоча ці питання активно вивчаються, багато аспектів, зокрема кібербезпека та оптимізація енергоспоживання, залишаються невирішеними та потребують подальших досліджень [9; 10].

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою статті є дослідження можливостей ефективного застосування технологій IoT для управління міською інфраструктурою, зокрема через розробку енергоефективних, надійних та безпечних мережевих архітектур. Завданнями є аналіз існуючих моделей побудови однохобових і багатохобових мереж, а також топологій бездротових сенсорних мереж (далі WSN), щоб визначити найбільш оптимальні

підходи для застосування в умовах розумних міст. Особлива увага приділяється питанням енергоспоживання, масштабованості, кібербезпеки та інтеграції IoT-систем у ключові сфери міської інфраструктури, такі як транспорт, енергетика та водопостачання

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Для належної роботи IoT у розумних містах ключовим аспектом є вибір мережевої архітектури, здатної ефективно обробляти та передавати великі обсяги даних. Основним завданням є досягнення балансу між енергоефективністю та надійністю передачі інформації на великі відстані.

Однохобові мережі забезпечують підключення сенсорних вузлів безпосередньо до базової станції. Їх перевагою є висока швидкість передачі даних через мінімальну кількість проміжних вузлів, що зменшує затримки. Однак значне енергоспоживання та обмежена масштабованість у великих міських територіях є недоліками, що обмежують застосування таких мереж у масштабних IoT-системах [1].

На відміну від однохобових систем, багатохобові мережі передають дані через проміжні вузли, що знижує енергоспоживання, оскільки кожен вузол підтримує зв'язок із найближчими вузлами. Така архітектура дозволяє розширити зону покриття без значного збільшення кількості базових станцій і робить мережу більш гнучкою та надійною для використання в умовах розумних міст [7]. Ієрархічна модель є підтипом багатохобової мережі, де деякі вузли виступають кластерними головними вузлами, збираючи дані від інших і передаючи їх на базову станцію. Це зменшує навантаження на мережу, підвищує енергоефективність і забезпечує високу масштабованість та стабільність системи [3].

Багатохобові мережі є особливо актуальними для розумних міст через їхню

здатність адаптуватися до втрат вузлів або змін у мережевих умовах. Вони забезпечують надійність для критичних систем, таких як транспорт, енергетика та водопостачання. Крім того, ці мережі легко адаптуються до збільшення кількості вузлів у міру розширення міста.

Топологія бездротових сенсорних мереж (далі WSN) є важливим аспектом побудови IoT-систем, оскільки вона впливає на стабільність і масштабованість системи. Плоска топологія, у якій усі вузли є рівноправними, є простою і дешевою у побудові, але має обмежену ефективність і масштабованість, що критично для великих міст [7]. У разі збільшення кількості вузлів вона може призводити до перевантаження мережі та затримок у передачі даних.

Ієрархічна топологія, що передбачає кластеризацію вузлів, є більш ефективною, оскільки знижує навантаження на окремі вузли і підвищує енергоефективність. Головні вузли виконують функції обробки та фільтрації даних, що сприяє стабільності та ефективності мережі. Ієрархічні топології добре підходять для великих міст, оскільки забезпечують стійкість і адаптивність [9].

У міському розвитку концепція розумних міст покладається на WSN, оскільки вони дозволяють ефективно управляти великими обсягами даних і мінімізувати енергоспоживання. Наприклад, у транспортних системах WSN можуть використовуватися для моніторингу транспортних потоків і управління світлофорами, що зменшує затори та скорочує час пересування [5].

У сфері енергетики WSN застосовуються для моніторингу споживання енергії будівлями, а також для оптимізації роботи електричних мереж. Сенсорні вузли інтегруються в системи управління електропостачанням для виявлення проблемних ділянок і автоматичного регулювання навантаження. Водопостачальні системи також використовують WSN для моніторингу тиску та рівня води в резервуарах, що

дозволяє своєчасно попереджати аварії або витоки води [6].

Інші типи топологій, як-от зіркоподібна або кільцева, мають обмежене застосування у великих IoT-системах через слабку масштабованість і вразливість до відмов окремих вузлів. Наприклад, у зіркоподібній топології відмова центрального вузла може призвести до збоїв у всій мережі [1].

Сенсорні вузли, що відповідають за збір даних із фізичного середовища, є основним компонентом WSN у розумних містах. Вони можуть вимірювати різні параметри, як-от температура, тиск чи рівень забруднення, і моніторити стан критичної інфраструктури, зокрема мостів, доріг та енергомереж. Енергоефективність є важливою вимогою до таких вузлів, оскільки вони зазвичай працюють на обмежених енергетичних ресурсах. Топологія бездротових сенсорних мереж (далі WSN) є важливим аспектом побудови IoT-систем, оскільки вона впливає на стабільність і масштабованість системи. Плоска топологія, у якій усі вузли є рівноправними, є простою і дешевою у побудові, але має обмежену ефективність і масштабованість, що критично для великих міст [7]. У разі збільшення кількості вузлів вона може призводити до перевантаження мережі та затримок у передачі даних.

Ієрархічна топологія, що передбачає кластеризацію вузлів, є більш ефективною, оскільки знижує навантаження на окремі вузли і підвищує енергоефективність. Головні вузли виконують функції обробки та фільтрації даних, що сприяє стабільності та ефективності мережі. Ієрархічні топології добре підходять для великих міст, оскільки забезпечують стійкість і адаптивність [9].

У міському розвитку концепція розумних міст покладається на WSN,

оскільки вони дозволяють ефективно управляти великими обсягами даних і мінімізувати енергоспоживання. Наприклад, у транспортних системах WSN можуть використовуватися для моніторингу транспортних потоків і управління світлофорами, що зменшує затори та скорочує час пересування [5].

У сфері енергетики WSN застосовуються для моніторингу споживання енергії будівлями, а також для оптимізації роботи електричних мереж. Сенсорні вузли інтегруються в системи управління електропостачанням для виявлення проблемних ділянок і автоматичного регулювання навантаження. Водопостачальні системи також використовують WSN для моніторингу тиску та рівня води в резервуарах, що дозволяє своєчасно попереджати аварії або витoki води [6].

Інші типи топологій, як-от зіркоподібна або кільцева, мають обмежене застосування у великих IoT-системах через слабку масштабованість і вразливість до відмов окремих вузлів. Наприклад, у зіркоподібній топології відмова центрального вузла може призвести до збоїв у всій мережі [1].

Сенсорні вузли, що відповідають за збір даних із фізичного середовища, є основним компонентом WSN у розумних містах. Вони можуть вимірювати різні параметри, як-от температура, тиск чи рівень забруднення, і моніторити стан критичної інфраструктури, зокрема мостів, доріг та енергомереж. Енергоефективність є важливою вимогою до таких вузлів, оскільки вони зазвичай працюють на обмежених енергетичних ресурсах.

Сенсорні вузли можуть бути як стаціонарними, так і мобільними. Стаціонарні вузли забезпечують стабільність передачі даних, тоді як мобільні вузли дозволяють охоплювати більші території для динамічного моніторингу. Однак мобільні вузли потребують оптимізації енергоспоживання та підтримки надійного зв'язку під час руху [7].

Важливу роль відіграють вузли-шлюзи, які забезпечують передачу даних між сенсорними вузлами та центральною системою управління. Вони обробляють дані від сенсорів і передають їх на базові станції або сервери для аналізу. Це зменшує навантаження на сенсорні вузли і знижує енерговитрати. Вузлі-шлюзи мають більше енергетичних та обчислювальних можливостей, що дозволяє їм управляти потоком даних, забезпечувати безпеку комунікацій і координувати роботу різних елементів мережі. Вони можуть також інтегруватися з іншими системами, такими як хмарні платформи або кібер-фізичні системи (далі CPS), що підвищує загальну ефективність.

IoT-технології в міській інфраструктурі створюють можливості для автоматизації процесів управління та підвищення ефективності використання ресурсів. Однією з ключових технологій є кібер-фізичні системи, що забезпечують контроль і моніторинг ресурсів у реальному часі. Одним із важливих напрямів застосування IoT є енергетична сфера. Сенсори можуть моніторити споживання енергії, виявляти проблемні ділянки та оптимізувати роботу електричних мереж, що підвищує надійність енергопостачання і знижує втрати енергії. Автоматизовані системи також дозволяють інтегрувати відновлювані джерела енергії, такі як сонячні та вітрові електростанції, сприяючи сталому розвитку міст.

Інший важливий напрям IoT – управління транспортними системами. Сенсори, розміщені на дорогах і транспортних засобах, дозволяють збирати дані про транспортні потоки, які використовуються для оптимізації роботи світлофорів, громадського транспорту та паркувальних майданчиків. Це знижує рівень заторів і скорочує час пересування мешканців міста, а також зменшує забруднення повітря [5].

У водопостачанні сенсори можуть моніторити тиск у трубопроводах, рівень води в резервуарах і якість води. Дані в реальному часі допомагають попередити

аварії або витoki води, знижуючи витрати на ремонт та експлуатацію.

Оскільки IoT-системи широко використовуються для управління критичними елементами міської інфраструктури, безпека таких систем є пріоритетом. Зростання кількості підключених пристроїв підвищує ризик кібератак, що вимагає надійних методів захисту даних і безпеки мережевих взаємодій [8].

Автентифікація користувачів є одним із ключових методів забезпечення безпеки IoT. Вона гарантує, що лише авторизовані користувачі та пристрої мають доступ до мережі. Однак класичні підходи не завжди підходять для IoT через обмежені обчислювальні потужності сенсорних вузлів. Тому розробляються нові полегшені протоколи автентифікації, які забезпечують безпеку без надмірного навантаження на ресурси [9].

Ще одним важливим аспектом безпеки є шифрування даних. IoT-системи використовують алгоритми AES або RSA для захисту інформації, проте через обмежені ресурси сенсорів часто застосовують полегшені варіанти цих алгоритмів. Також важливими є захищені протоколи зв'язку, як-от TLS або DTLS, що знижують ризик перехоплення даних. Проте складні алгоритми можуть підвищити енергоспоживання, тому необхідно знайти баланс між безпекою та енергоефективністю.

Ситуаційні центри управління є ключовими компонентами IoT-систем у містах. Вони забезпечують координацію міської інфраструктури в режимі реального часу, дозволяючи оптимізувати процеси, як-от керування транспортними потоками та водопостачанням. Дані з сенсорів допомагають автоматично реагувати на аварії або надзвичайні ситуації [6].

Нарешті, для стабільної роботи IoT-систем необхідно впроваджувати стандарти якості обслуговування (далі QoS), що визначають затримку передачі даних, ширину смуги пропускання, надійність зв'язку та безпеку. Наприклад,

затримка передачі даних у транспортних або енергетичних мережах може призвести до серйозних наслідків, як-от затори або перебої в електропостачанні [6].

Ще одним важливим показником є ширина смуги пропускання. У міських IoT-системах кількість підключених пристроїв може бути дуже великою, і для ефективної роботи системи необхідно забезпечити достатню пропускну здатність мережі. Якщо пропускну здатність недостатня, це може призвести до перевантаження мережі та зниження швидкості передачі даних, що негативно вплине на функціонування всієї міської інфраструктури [8]. Особливо важливо забезпечити необхідну пропускну здатність для критичних систем, таких як моніторинг та управління міськими ресурсами. Надійність зв'язку також є ключовим аспектом для IoT-систем, оскільки стабільне та безперебійне з'єднання між усіма компонентами інфраструктури є критично важливим для їхньої безперервної роботи. Наприклад, у разі збоїв у з'єднанні енергетичних мереж або систем безпеки можуть виникати серйозні наслідки, як-от перебої в електропостачанні або затримки у реагуванні на надзвичайні ситуації [9]. Таким чином, забезпечення стабільного зв'язку є важливим завданням для ефективного функціонування розумних міст.

Одним із найважливіших аспектів QoS в IoT-системах є безпека, яка відіграє ключову роль у захисті конфіденційних даних і збереженні цілісності систем. Для цього застосовуються захищені протоколи зв'язку та шифрування даних, що гарантує захист переданої інформації від несанкціонованого доступу. З огляду на зростання кількості IoT-пристроїв у міській інфраструктурі, виникає необхідність оптимізації процесу передачі даних, щоб уникнути перевантажень мережі та забезпечити стабільну роботу всієї системи.

Математичні моделі є важливим інструментом для оптимізації трафіку в мережах IoT, допомагаючи прогнозувати трафік і приймати рішення щодо його

обробки. Однією з найбільш ефективних моделей для аналізу й оптимізації трафіку в IoT-системах є теорія черг, яка дозволяє моделювати поведінку мережі під різними навантаженнями, тим самим забезпечуючи високу якість обслуговування. Основний підхід, заснований на цій теорії, полягає в моделюванні процесу обробки даних, які надходять від численних сенсорних вузлів через вузли-шлюзи та базові станції. У міру збільшення обсягу трафіку теорія черг допомагає уникнути перевантаження каналів зв'язку і підвищити ефективність використання мережевих ресурсів. Використання таких математичних моделей дозволяє передбачати можливі затримки та рівномірно розподіляти навантаження між різними елементами мережі [9].

Різні типи моделей черг можуть бути застосовані для IoT-систем залежно від конкретних сценаріїв. Наприклад, модель M/M/1, де один сервер обслуговує заявки, що надходять із певною частотою, є корисною для прогнозування трафіку у вузлах IoT-систем із обмеженою пропускну здатністю. Для складніших сценаріїв можуть бути використані інші моделі, як-от M/M/c або M/G/1, де кілька серверів обробляють чергу заявок, або ж обробка здійснюється зі змінною швидкістю [9]. Такі підходи дозволяють враховувати різні фактори, що впливають на трафік, зокрема час доби, інтенсивність транспортних потоків або інші чинники міського середовища.

Агрегований трафік від IoT-пристроїв у розумних містах змінюється залежно від різних умов, наприклад, часу доби або інтенсивності транспортних потоків. Моделі, що використовують агреговані потоки даних, дозволяють прогнозувати зміни трафіку в реальному часі та динамічно адаптувати роботу мережі для зменшення затримок [10]. Застосування таких моделей є важливим у системах управління міським транспортом, де вони допомагають оптимізувати роботу світлофорів, скоротити час очікування для водіїв і знизити загальне навантаження на транспортну інфраструктуру. Подібні

підходи можуть бути застосовані для управління іншими міськими ресурсами, такими як електромережі або системи водопостачання [8].

Один із ключових аспектів, який враховують у математичних моделях управління трафіком IoT-систем, — це параметри QoS. Ці параметри включають затримку передачі даних, ширину смуги пропускання, надійність зв'язку та пріоритетність даних. Застосування теорії черг дозволяє оптимізувати ці показники для досягнення високої ефективності роботи системи. Наприклад, такі моделі допомагають визначити оптимальні рівні затримок і пропускну здатності для кожного типу трафіку, що дозволяє забезпечити пріоритетну обробку критичних даних, таких як інформація про аварії чи небезпеки [9].

Важливим фактором підвищення ефективності управління трафіком IoT-систем в процесі управління інфраструктурою міста є методи, способи та вид програмного забезпечення яке буде застосовуватися в межах як управління самою системою так і застосування самої системи, пов'язаними з нею елементами IoT та кінцевими користувачами.

Існуючі тенденції розвитку способів та методів розробки та застосування програмних продуктів в сучасних мережах IoT, з врахуванням масованого втілення телекомунікаційних мереж та систем п'ятого покоління, а саме 5G/IMT-2020, виводить на перший план застосування таких типів архітектури програмного забезпечення (ПЗ) як безсерверні та мікросерверні масиви ПО [11,12]. Їх перевагами є відсутність проміжних елементів накопичення та обробки даних, що значно підвищує швидкість функціонування мережі та отримання результатів її застосування. При цьому саме мікросервісна архітектура ПЗ забезпечує можливість одночасного ефективного застосування різними користувачами ПЗ різного призначення в інфраструктурних рішеннях, до яких в першу чергу відносяться IoT-систем.

Побудована по мікросервісній архітектурі ПЗ уявляє собою набір окремих програмних продуктів та логіку їх застосування. При цьому побудоване таким чином ПЗ може включати в себе окремі функціональні блоки а бо мати атомарну структуру [11, 12].

В свою чергу, саме найбільш сучасна на перспективна атомарна структура мікросервісного ПЗ дозволяє більш ефективно використати вільні обчислювальні можливості мережі, мати можливість до швидкого клонування окремих елементів ПО, активно застосовувати при функціонуванні сумісно з граничними туманні обчислення та залучати до управління мікросервісного ПЗ елементи штучного інтелекту (ШІ). Особливо важливе залучення ШІ при аналізі трафіку запитів до масиву мікросервісного ПО на етапі визначення навантаження на IoT-систему, виключення впливу додаткових затримок і змін структури потоків корисних даних в мережі [12, 13].

Важливою властивістю мікросервісног підходу до побудови ПЗ є можливість до мінімізації якості розробки та взаємодії різних елементів такого ПЗ, при створення різними виробниками та залученні до їх застосування різних програмно-апаратних комплексів.

Зі всього переліку чинників, негативних факторів та параметрів, які можуть чинити вплив на якість функціонування IoT-системи в умовах застосування масивів мікросервісного ПЗ, створеного, як сукупність елементів від різних розробників та реалізованого на різних типах програмно-апаратних комплексів найбільш значущим буде чинник затримки, який визначається часом відклику мережі на запит окремого користувача [11, 12].

Є очевидним, що наукові дослідження по мінімізації вказаного часу затримки повинні проводитись в напрямку своєчасного аналізу навантаження на контролери програмно-орієнтованої мережі. Результати аналізу якого, через подальший розподіл трафіку запитів

можуть забезпечити виключення впливу як особливостей розробки елементів ПЗ так і вплив можливостей програмно-апаратних комплексів на загальну ефективність управління всієї IoT-системи [13, 14].

Таким чином, побудови мереж інтернету речей для управління інфраструктурою міста при умові залучення до її функціонування мікросервісного ПЗ вимагає проведення ряду наукових досліджень. Основними з напрямків якого можуть бути:

- розробка механізмів аналізу навантаження в IoT-системах, які б дозволили мінімізувати час визначення додаткових затримок трафіку і зміни структури потоків корисних даних.

- побудова структури взаємодії туманних та граничних обчислень в межах мікросервісного ПЗ з урахуванням змін динамічності користувачів;

- розробка нових, науково обґрунтованих моделей взаємодії туманних і граничних обчислень, які, за рахунок раціонального вибору пристроїв туманних обчислень які повинні забезпечити функціонування мікросервісного ПЗ при умові мінімізації часу виконання завдань;

- розробка та удосконалення методик та методів прогнозування навантаження на контролер програмно конфігурованих мереж, які повинні забезпечити виключення залежності ПЗ управління мережами від особливостей функціонування апаратно-програмованих комплексів різних виробників.

Вирішення вище поданих завдань в цілому, через зменшення часу відпрацювання окремих запитів та часткових завдань, буде сприяти підвищенню якості функціонування мереж інтернету речей при залученні її до управління інфраструктурою міста.

ВИСНОВКИ

Таким чином, математичні моделі, зокрема теорія черг, є важливими інструментами для управління трафіком в IoT-системах розумних міст. Вони дозволяють не тільки уникнути

перевантажень, але й забезпечити стабільну та ефективну роботу системи, що є критично важливим для міської інфраструктури великих агломерацій. Успішне впровадження IoT-систем для управління міською інфраструктурою відкриває нові можливості для оптимізації використання ресурсів, підвищення надійності міських сервісів і покращення умов життя мешканців. Однак для досягнення цих цілей необхідно ретельно підходити до вибору мережевої архітектури, забезпечення безпеки і управління агрегованим трафіком, перейти до застосування найбільш раціональної архітектури програмного забезпечення для управління трафіком системи та її застосування при управлінні міською інфраструктурою.

В якості раціональної архітектури програмного забезпечення в роботі запропоновано застосувати мікросервісне програмне забезпечення. А саме, визначені його особливості та переваги і подані напрямки подальших наукових досліджень, які будуть направлені на ефективне застосування вказаного програмного забезпечення для управління інфраструктурою міста через IoT-систему.

REFERENCES

1. **Markuts V.** (2023). Zastosuvannia tekhnolohii Internetu rechei v avtomatyzovanykh systemakh upravlinnia resursamy. *Stratehiia ekonomichnoho rozvytku Ukrainy*, No.52, 97–111. <https://doi.org/10.33111/sedu.2023.52.097.111>,
2. **Aggarwal A.** (2019). Internet of things driven perceived value co-creation in smart cities of the future: a PLS-SEM based predictive model. *Journal of Computational and Theoretical Nanoscience*, Vol. 16. No. 9. 4053–4058. DOI: <https://doi.org/10.1166/jctn.2019.8292>.
3. **Garcia-Retuerta, D., Chamoso, P., Hernández, G., Guzmán, A., Yigitcanlar, T., Corchado, J.** (2021). An efficient management platform for developing smart cities: Solution for real-time and future crowd detection. *Electronics*, Vol. 10 (7), 765. <https://doi.org/10.3390/electronics10070765>.
4. **Gómez J. E.** (2017). IoT for environmental variables in urban areas. *Procedia computer science*, Vol. 109, 67–74. <https://doi.org/10.1016/j.procs.2017.05.296>.
5. IoT-enabled smart cities: A hybrid systematic analysis of key research areas, challenges, and recommendations for future direction | Discover Cities [Springer] Available at: <https://link.springer.com/article/10.1007/s42162-022-00195-2>
6. **Madakam S., Ramaswamy R., Date H.** (2019). Quality of life. Palava smart city: A case study". *Global Business Review*, Vol. 20 (3), 708–742. DOI: <https://doi.org/10.1177/097215091772182>
7. Networking Architectures and Protocols for IoT Applications in Smart Cities: Recent Developments and Perspectives [MDPI] Available at: <https://www.mdpi.com/2079-9292/12/11/2490>
8. Networking architectures and protocols for smart city systems | Journal of Internet Services and Applications [SpringerOpen] Available at: <https://jisajournal.springeropen.com/articles/10.1186/s13174-018-0097-0>
9. On Wireless Sensor Network Models: A Cross-Layer Systematic Review [MDPI] Available at: <https://www.mdpi.com/2224-2708/12/4/50>
10. Wireless Sensor Networks: Applications | IntechOpen Available at: <https://www.intechopen.com/chapters/73287>
11. **Ekaterina Oleynik, Sergey Revniykh** (2011). GLONASS Status and Modernization. CGSIG Meeting, September. https://web.archive.org/web/20130921061015/http://www.navcen.uscg.gov/pdf/cgsicMeetings/51/3_GLONASS_CGSI_C_Oleynik.pdf
12. **Shin Y., Kim E.** (2018). PF-DOP hybrid path planning for safe and efficient navigation of unmanned vehicle systems. In Proceedings of the 31st International Technical Meeting of the Satellite Division of the Institute of Navigation, ION GNSS+ 2018, Miami, FL, USA, 24–28 September 2018; Institute of Navigation: Manassas, VA, USA, 2501–2517. DOI: 10.33012/2018.15978.
13. **Koretskyi Oleksandr** (2024) Architecture of multifunctional application software microservices. *Сучасний захист інформації*, 3(59), 85–93. DOI:10.31673/2409-7292.2024.030009.
14. **Y. Romani O.** (2022). Tibermacine and C. Tibermacine, "Towards Migrating Legacy Software Systems to Microservice-based Architectures: a Data-Centric Process for Microservice Identification," 2022 IEEE 19th International Conference on Software Architecture Companion (ICSA-C), Honolulu,

HI, USA, 2022, pp. 15-19, doi: 10.1109/ICSA-C54293.2022.00010.

Models for building Internet of Things networks for city infrastructure management

Anastasia Kondakova, Oleksandr Koretskyi,

Abstracts. The work considers modern approaches to the implementation of IoT technologies for effective management of urban infrastructure. The main focus is on the analysis of network architectures used for data collection and transmission in smart city systems. Various network construction models are compared, including single-hop and multi-hop networks, as well as WSN topologies. The work focuses on the advantages and disadvantages of these networks in the context of energy consumption, scalability and stability. Special attention is paid to hierarchical models that allow to reduce energy costs and increase network efficiency. The application of IoT in key areas of urban infrastructure, such as transport, energy and water supply, is analyzed. The issue of cyber security of IoT systems,

including authentication, data encryption and ensuring communication reliability, is also discussed in detail. The role of CPS and sensor nodes that provide real-time monitoring and control of urban resources is discussed separately. Mathematical models for traffic optimization in IoT networks are considered, in particular, the use of queuing theory to ensure QoS. Conclusions have been drawn regarding the effectiveness of IoT implementation for urban resource management, which allows to increase the reliability of urban infrastructure and improve the living conditions of residents. The use of microservice software in IoT systems is substantiated and the directions of scientific research aimed at and its implementation in IoT-systems of management of infrastructure objects.

The study opens up new perspectives for the application of IoT in smart cities and indicates the need for further study of security and energy conservation issues in such systems.

Keywords: IoT, urban infrastructure, smart cities, WSN, energy efficiency, CPS, microservice software