КОМП'ЮТЕРНІ НАУКИ

УДК 004.75 https://doi.org/10.31713/vt2202415

Степанюк О. Ю., студент (Національний університет водного господарства та природокористування, м. Рівне, stepaniuk_em23@nuwm.edu.ua)

ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ ТА МАСШТАБУВАННЯ ІНТЕРНЕТУ РЕЧЕЙ

У статті розглянуто переваги та перспективи впровадження Інтернету речей (IoT), акцентуючи увагу на його здатності підвищувати ефективність, автоматизувати процеси та оптимізувати використання ресурсів. Обговорюються ключові виклики, пов'язані з кібербезпекою та продуктивністю IoT-систем, що виникають у зв'язку зі зростанням кількості підключених пристроїв. Наголошується на важливості врахування цих аспектів на ранніх етапах розробки та впровадження технології, щоб забезпечити її успішне і безпечне застосування в різних галузях.

Ключові слова: **Інтернет речей; IoT; кібербезпека; продуктивність; автоматизація; оптимізація ресурсів.**

I. Вступ

Інтернет речей (англ. *Internet of Things, IoT*) – концепція мережі, що складається із взаємозв'язаних фізичних пристроїв, які мають вбудовані датчики, а також програмне забезпечення, що дозволяє здійснювати передачу і обмін даними між фізичним світом і комп'ютерними системами в автоматичному режимі, за допомогою використання стандартних протоколів зв'язку. Окрім датчиків, мережа може мати виконавчі пристрої, вбудовані у фізичні об'єкти і пов'язані між собою через дротові чи бездротові мережі. Ці взаємопов'язані пристрої мають можливість зчитування та приведення в дію, функцію програмування та ідентифікації, а також дозволяють виключити необхідність участі людини, за рахунок використання інтелектуальних інтерфейсів.

II. Переваги та можливості інтернету речей

Використання технології Інтернету речей відкриває численні переваги та можливості для бізнесу та суспільства в цілому. Ось

основні з них:

1. *Підвищення ефективності та автоматизації процесів:* IoT дозволяє інтегрувати різноманітні пристрої, системи та дані в єдину мережу, що забезпечує автоматичний обмін інформацією в режимі реального часу. Це сприяє підвищенню ефективності операційних процесів, зменшенню часу реакції та покращенню управління ресурсами. Наприклад, у виробничих процесах IoT забезпечує зменшення простоїв обладнання та оптимізацію використання енергії завдяки аналізу даних в реальному часі та автоматичному керуванню процесами.

2. Підтримка прийняття рішень на основі даних: завдяки підключенню до IoT, пристрої можуть збирати, аналізувати та інтерпретувати великі обсяги даних, що дозволяє організаціям приймати більш обґрунтовані рішення. Наприклад, застосування машинного навчання (ML) у поєднанні з IoT дозволяє прогнозувати можливі збої в роботі обладнання та вчасно проводити технічне обслуговування, що зменшує ризик несподіваних простоїв та підвищує безпеку.

3. Покращення якості обслуговування клієнтів: IoT може підвищити рівень обслуговування клієнтів завдяки впровадженню "розумних" пристроїв, які можуть автоматично реагувати на потреби користувачів. Наприклад, у роздрібній торгівлі IoT дозволяє персоналізувати пропозиції та рекомендації на основі попередніх покупок і поведінкових даних клієнтів, що підвищує задоволеність споживачів.

4. *Інновації у сфері безпеки:* зі зростанням кількості підключених до IoT пристроїв зростає і потреба у посиленні кібербезпеки. Впровадження нових протоколів безпеки, таких як блокчейн для захищених транзакцій даних та удосконалені методи шифрування, дозволяють знижувати ризики кіберзагроз та забезпечувати захист даних і пристроїв від несанкціонованого доступу.

5. *Підтримка стійкого розвитку:* IoT сприяє раціональнішому використанню ресурсів і зниженню екологічного впливу. Наприклад, у сільському господарстві застосування IoT дозволяє оптимізувати полив та використання добрив, що зменшує споживання води та хімікатів і підвищує врожайність [1].

Таким чином, IoT відкриває широкі можливості для оптимізації процесів, підвищення безпеки та поліпшення якості життя, роблячи його важливою складовою сучасних технологічних стратегій багатьох організацій.

III. Проблеми впровадження та масштабування

Однак на шляху до реалізації масштабних проєктів та отримання значної вигоди постають і серйозні проблеми. Першою з них є проблема кібербезпеки. Несанкціонований доступ до мережі приватного розумного будинку, промислового підприємства або медичного закладу може призвести до серйозних наслідків. Такими можуть бути як втрата персональних або корпоративних даних, так і збої у роботі систем безпеки та управління. Для запобігання цьому використовуються різні методи захисту.

Згідно з [2] визначаються наступні цілі безпеки IoT:

1. Ідентифікація – усі суб'єкти в системі IoT повинні мати можливість ідентифікувати інших учасників. Їм потрібно знати про інші сутності в мережі. Крім того, об'єкти повинні відрізняти дружні об'єкти від потенційно зловмисних. У більшості випадків пристрої IoT знаходяться в певному контексті, наприклад, належать до групи, розташовані в певній будівлі, належать певній організації. Таким чином, ідентифікація відноситься до процесу заявлення даної ідентичності.

2. Автентифікація та авторизація – перш ніж дозволити доступ до ресурсу з обмеженим доступом (наприклад, до конфіденційної інформації), сенсорні пристрої, користувачі та вузли шлюзу повинні бути автентифіковані, тобто їх ідентичність повинна бути перевірена. Необхідно переконатися, що вони є тими, за кого себе видають. Після того, як особу було перевірено, необхідно переконатися, що об'єкт, який розглядається, має доступ до даних, ресурсів або додатків у системі.

3. Цілісність – необхідно переконатися, що дані або повідомлення не були змінені, тобто модифіковані, відредаговані або знищені під час їх обміну та передачі, зберігання та обробки.

4. Конфіденційність – секретна інформація повинна бути захищена від несанкціонованого розголошення як під час транспортування, так і в межах зберігання.

5. Приватність – під час збирання, обробки, зберігання та видалення даних необхідно забезпечити належне дотримання прав осіб щодо використання особистої інформації. Зазвичай це передбачає дотримання контрактів, політики та застосування керівних постанов або законів, наприклад, у Європі Загальний регламент захисту даних (GDPR), який діє з 2020 року.

6. Доступність – система та її служби мають бути доступними, коли це необхідно. Таким чином, доступність відноситься до ймовірності того, що система (або компонент) працює в певний момент

часу. Це включає в себе як надійність, тобто відповідність певним стандартам продуктивності в даному контексті, так і ремонтопридатність, тобто здатність від'єднувати, виправляти та модифікувати компоненти, не перешкоджаючи службі та не порушуючи попередньо визначені порогові значення.

*7. Неспростовність – зі зловмисним, але спочатку невидимим наміром, будь-яка особа не повинна мати можливість приховати свої дії. Таким чином, неспростовність гарантує, що жодна організація не може стверджу*вати, що транзакція не відбулася, коли вона насправді відбулася, або навпаки. Це гарантує, що обставини можуть бути вирішені, коли різні сторони в системі мають різні погляди на те, що сталося, наприклад, під час збою мережі.

Ретельне дотримання систематизованих рекомендацій безпеки підвищує надійність мереж та зменшує ризики при їх впровадженні.

Іншою серйозною проблемою при впровадженні мереж Інтернету речей є продуктивність. Заходи безпеки зазвичай базуються на «дорогих» схемах, як-от шифрування та підписання, без явного врахування споживання ресурсів. Однак пристрої IoT мають обмежені ресурси з точки зору обчислень, пам'яті, сховища, мережі та енергії, що ускладнює їх належний захист. Пристрої IoT, як правило, компактні та легкі, не містять велику батарею. Крім того, оскільки вони повинні працювати автономно, не вимагаючи втручання людини для частої заміни батареї, вони повинні обмежувати споживання енергії та працювати з енергоефективністю. Крім того, пристрої IoT також повинні заощаджувати ресурси щодо пам'яті. Якщо немає місця для довговічної батареї, часто не вистачає місця для більшої пам'яті. Те саме стосується процесорів: складність процесорів і датчиків обмежена через простір і вагу. Оскільки розгортання IoT вже має проводитися в каналах зв'язку з втратами та низькою пропускною здатністю, існує обмежена здатність для великих накладних витрат. Отже, часто розробникам доводиться знаходити компроміс між продуктивністю та захищеністю мережі [3; 4].

Іншими аспектами продуктивності за [5] є:

1. Масштабування обчислень – зі збільшенням кількості підключених пристроїв зростає і обсяг даних, які потрібно обробляти. Хмарні платформи повинні бути здатні масштабувати свої обчислювальні ресурси, щоб підтримувати ефективну обробку великих обсягів даних. Це включає динамічне розподілення ресурсів для забезпечення безперебійної роботи систем навіть під час пікових навантажень.

2. Обробка даних у реальному часі – для багатьох IoT-застосунків критично важливо забезпечити обробку даних у реальному часі. Наприклад, у системах безпеки або промислових контролерах затримка навіть у декілька секунд може призвести до небажаних наслідків. Хмарні платформи повинні забезпечувати низьку латентність і високу швидкість обробки даних, щоб гарантувати належну реакцію систем на події.

3. Надійність та стійкість до відмов – продуктивність системи також залежить від її здатності до відновлення після збоїв. Хмарні платформи повинні мати механізми для автоматичного резервного копіювання даних та відновлення після відмов. Це забезпечує безперебійність роботи IoT-додатків, навіть у разі виходу з ладу окремих компонентів системи.

4. Оптимізація використання ресурсів – ефективне використання обчислювальних ресурсів у хмарі є важливим для підтримання високої продуктивності. Оптимізація включає в себе розподіл завдань між різними вузлами хмарної платформи, щоб уникнути перевантаження окремих серверів. Також важливим є ефективне управління пам'яттю та мережевими ресурсами.

5. Забезпечення якості обслуговування (Quality of service, QoS) – хмарні провайдери повинні дотримуватися встановлених параметрів якості обслуговування (QoS) для забезпечення надійної роботи IoT-додатків. Це включає підтримання стабільного з'єднання, мінімізації затримок та забезпечення необхідної пропускної здатності мережі. Для цього можуть використовуватися спеціальні алгоритми управління трафіком і пріоритизації даних.

Для досягнення високої продуктивності в інтегрованих IoT та хмарних системах необхідно враховувати всі перелічені фактори. Масштабованість, низька затримка, надійність і оптимізація використання ресурсів є ключовими компонентами, які визначають ефективність роботи таких систем. Розробка і впровадження передових технологій управління продуктивністю дозволить забезпечити стабільну та швидку роботу IoT-додатків, що базуються на хмарних обчисленнях.

IV. Висновки

Інтернет речей (IoT) є однією з найперспективніших технологій сучасності, що має потенціал революціонізувати різні галузі, від промисловості та сільського господарства до медицини та розумних міст. Завдяки можливості підключення та взаємодії широкого спектру пристроїв, IoT забезпечує підвищення ефективності

процесів, автоматизацію завдань та більш глибоке розуміння даних, що веде до покращення ухвалення рішень та оптимізації ресурсів. Це дає змогу підприємствам знижувати витрати, підвищувати продуктивність та забезпечувати вищу якість послуг для кінцевих споживачів.

Проте, впровадження IoT також несе в собі певні виклики, серед яких особливо виділяються питання кібербезпеки та продуктивності. Оскільки кількість підключених пристроїв зростає, збільшується й кількість потенційних вразливостей, які можуть бути використані зловмисниками для атак. Це створює необхідність розробки та впровадження надійних механізмів захисту, що повинні бути інтегровані на ранньому етапі розробки IoT-рішень.

Крім того, питання продуктивності IoT-систем є ще однією важливою проблемою, оскільки велика кількість підключених пристроїв та передача великих обсягів даних можуть призвести до значних навантажень на мережу та обчислювальні ресурси. Це вимагає оптимізації архітектури систем, забезпечення ефективного використання ресурсів та впровадження масштабованих рішень.

Таким чином, незважаючи на значні переваги IoT, важливо усвідомлювати та враховувати потенційні проблеми, пов'язані з цією технологією. Впровадження IoT має здійснюватися з урахуванням аспектів кібербезпеки та продуктивності, що забезпечить успішну інтеграцію цієї технології в різні сфери та її ефективне використання в майбутньому.

1. Soureesh De, Arpan Kumar Kar. Exploring IoT Applications in Industry 4.0 – Insights from Review of Literature. IoT, Big Data and AI for Improving Quality of Everyday Life: Present and Future Challenges. 2023. **2.** Landscape of IoT security / Eryk Schiller etc. *Computer Science Review*. May 2022. Vol. 44. **3.** Minoli D., Sohraby K., Kouns J. IoT security (IoTsec) considerations, requirements, and architectures. *Consumer Communications & Networking Conference (CCNC), IEEE* : 14th Annual. Piscataway, NJ, US 2017. Pp. 1006–1007. **4.** Hellaoui H., Koudil M., Bouabdallah A. Energy-efficient mechanisms in security of the internet of things: A survey. *Elsevier Comput. Netw*. 2017. Vol. 127. Pp. 173–189. **5.** IoT and Cloud Computing Issues, Challenges and Opportunities: AReview / Mohammed Sadeeq etc. *Qubahan Academic Journal*. 2021. Vol. 1(2). Pp. 1–7.

REFERENCES:

1. Soureesh De, Arpan Kumar Kar. Exploring IoT Applications in Industry 4.0 – Insights from Review of Literature. IoT, Big Data and AI for Improving Quality of

Everyday Life: Present and Future Challenges. 2023. **2.** Landscape of IoT security / Eryk Schiller etc. *Computer Science Review*. May 2022. Vol. 44. **3.** Minoli D., Sohraby K., Kouns J. IoT security (IoTsec) considerations, requirements, and architectures. *Consumer Communications & Networking Conference (CCNC), IEEE* : 14th Annual. Piscataway, NJ, US 2017. Pp. 1006–1007. **4.** Hellaoui H., Koudil M., Bouabdallah A. Energy-efficient mechanisms in security of the internet of things: A survey. *Elsevier Comput. Netw*. 2017. Vol. 127. Pp. 173–189. **5.** IoT and Cloud Computing Issues, Challenges and Opportunities: AReview / Mohammed Sadeeq etc. *Qubahan Academic Journal*. 2021. Vol. 1(2). Pp. 1–7.

Stepaniuk O. Y., Senior Student (National University of Water and Environmental Engineering, Rivne, stepaniuk_em23@nuwm.edu.ua)

PROBLEMS AND PROSPECTS OF THE DEVELOPMENT AND SCALING OF THE INTERNET OF THINGS

This article explores the advantages and prospects of implementing the Internet of Things (IoT), emphasizing its potential to enhance efficiency, automate processes, and optimize resource utilization. Key challenges related to cybersecurity and IoT system performance, arising from the increasing number of connected devices, are discussed. The importance of considering these aspects at the early stages of technology development and implementation is highlighted to ensure its successful and secure application across various sectors.

Keywords: **Internet of Things; IoT; cybersecurity; performance; automation; resource optimization.**