

АНАЛІЗ ПРОБЛЕМ ПРИ РЕАЛІЗАЦІЇ ТЕХНОЛОГІЇ ІНДУСТРІАЛЬНОГО ІНТЕРНЕТА РЕЧЕЙ

¹Кононова І. В., ¹Самусь Д.В., ²Самусь Г.І.

¹Навчально-науковий інститут телекомунікаційних
систем КПІ ім. Ігоря Сікорського, Україна

²Конотопський інститут Сумського державного університету
E-mail: dimasamus99@gmail.com

ANALYSIS OF PROBLEMS IN THE IMPLEMENTATION OF INDUSTRIAL INTERNET OF THINGS TECHNOLOGY

The article examines the essence and aspects that need to be taken into account when considering the Internet of Things, in particular, attention is paid to the importance of industrial IoT. The main problems of IoT technologies are identified.

На сьогодні, в епоху цифрової революції 4.0 важливу роль в житті людини відіграє застосування Інтернету речей (IoT). Першою метою впровадження IoT шляхом оснащення всіх об'єктів у світі мініатюрними пристроями ідентифікації було перетворення повсякденного життя, внесення до нього більшого комфорту, упорядкованості та прогнозованості [1].

Слід зазначити наступні аспекти, які потрібно враховувати під час впровадження рішень IoT: системний, інтелектуальний, інформаційний, проектний, управлінський. Так, системний аспект дозволяє розглядати систему, технологію чи процес із системних позицій. Інтелектуальний аспект вимагає поділу IoT-пристроїв за функціями на «розумні» та «інтелектуальні». Інформаційний аспект дозволяє розглядати IoT як міжмережеву взаємодію фізичних пристроїв (підключених чи інтелектуальних пристроїв). Проектний аспект дозволяє розглядати схему IoT як інформаційну конструкцію. Управлінський аспект вимагає розглядати IoT як систему із мережним або субсидіарним управлінням.

Важливе значення має IoT для моніторингу оточуючого середовища, управління інфраструктурою, в медицині, в будівництві, в інтеграції засобів зв'язку, управлінні та обробці інформації [1]. Загалом можна виділити сім галузей застосування технології IoT (рис.1), а саме: людина, будинок, офіс, підприємство, виробничий об'єкт, місто, зовнішній параметр.

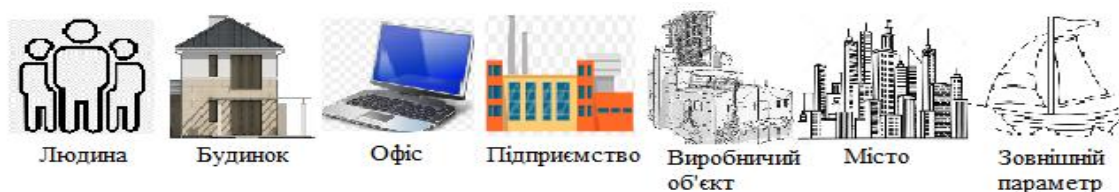


Рис.1. Галузі застосування технології IoT.

Глобальним сегментом IoT для корпоративного (галузевого) застосування є індустріальний Інтернет речей (Industrial Internet of Things, IIoT) – Інтернет речей для корпоративного або галузевого використання – система об'єднаних комп'ютерних мереж та підключених промислових об'єктів із вбудованими датчиками та програмним забезпеченням для збору та обміну даними, з можливістю віддаленого контролю та управління в автоматизованому режимі, без участі людини [2].

Для позначення вузького промислового сегменту IoT застосовується термін «промисловий Інтернет речей». Впровадження IIoT в обробній промисловості може призвести до збільшення ефективності виробництва, що стане поштовхом до четвертої промислової революції (Industry 4.0) [2]. Отже, IIoT – це еволюція розподіленої системи управління (DCS), яка дозволяє підвищити рівень автоматизації за рахунок використання хмарних обчислень для уточнення та оптимізації управління процесом.

IIoT використовує технології кібербезпеки, хмарні обчислення, граничні обчислення, мобільні технології, міжмашинну взаємодію, 3D-друк, передову робототехніку, аналіз великих обсягів даних, IoT, технологію RFID та когнітивні обчислення. Виділимо п'ять найважливіших з них: 1. Кіберфізичні системи – інформаційно-технологічна концепція, що передбачає інтеграцію обчислювальних ресурсів у фізичні процеси [3]. 2. Хмарні обчислення дозволяють надавати ІТ-послуги, ресурси при цьому завантажуються та вилучаються без прямого підключення до сервера [4]. 3. Крайові обчислення – парадигма розподілених обчислень, що наближає комп'ютерне сховище даних до місця, де вони потрібні [5]. 4. Аналітика великих даних – процес вивчення великих і різноманітних наборів даних або великих обсягів даних [6]. 5. Штучний інтелект та машинне навчання [7].

Системи IIoT часто сприймаються як багаторівнева модульна архітектура цифрових технологій. Рівень пристрою визначається фізичним компонентом: CPS, датчиком чи машиною. Мережевий рівень включає фізичні мережеві шини, хмарні обчислення та протоколи зв'язку, що агрегують та транспортують дані на сервісний рівень. Сервісний рівень складається з додатків, які працюють з даними та об'єднують їх у інформацію, що відображається на панелі приладів драйвера.

Для того, щоб IoT впровадити в більш широке використання, необхідно вирішити низку проблем. Деякі з цих проблем мають технічний характер, інші – суто структурний. Наприклад, користувачі повинні почати довіряти системам, що працюють на основі IoT, а компаніям необхідно при прийнятті рішень використовувати підходи на основі цифрових даних.

Розглянемо основні проблеми при реалізації технологій IIoT:

1. Сумісність пристроїв. Здатність пристроїв та систем IIoT працювати спільно має вирішальне значення для реалізації всіх можливостей IIoT - додатків. Прийняття відкритих стандартів є одним із способів забезпечення сумісності.

2. Конфіденційність. У більшості користувачів викликають занепокоєння проблеми конфіденційності особистих даних, що збираються

мільярдами пристроїв, та незаконного їх використання, організації непокоїть можливість незаконного доступу до комерційної конфіденційної інформації.

3. Захист даних. Організації, що збирають дані з мільярдів пристроїв, повинні мати можливість захистити ці дані від несанкціонованого доступу бо поширення інформаційних технологій на нові пристрої створює набагато більше потенційних вразливостей.

4. Захист інтелектуальної власності. Щоб розкрити величезний потенціал IoT, потрібно чіткіше розмежувати права та обов'язки учасників правовідносин, що виникають у зв'язку із застосуванням технологій IoT, і визначити, які права поширюються на дані, створювані різними підключеними пристроями.

Усі вищезазначені проблеми пов'язані з питаннями безпеки.

Отже, промисловий Інтернет речей - це мережа пристроїв, які пов'язані між собою за допомогою комунікаційних технологій. Одним із складних завдань у розвитку концепції Інтернет речей (IoT) у багатьох додатках є складні проблеми забезпечення інформаційної безпеки у широкому спектрі захисту від загроз зловмисника. Ці проблеми особливо актуальні, оскільки прогнозується зростання потреби користувачів в IoT.

Безпека інтернету речей передбачає захист інтернет-пристроїв та мереж, до яких вони підключені, від онлайн-загроз та зломів. Це досягається шляхом виявлення, моніторингу та усунення потенційних вразливостей безпеки на пристроях.

Література

1. Industrial Internet of Things Platform Comparison // M&S Consulting : [site]. 2016. 08 Febr. URL: <https://www.mandsconsulting.com/industrial-iot-platform-comparison/> (date of access: 21.02.2023).
2. Industrial Internet of Things, IIoT. URL: <https://www.it.ua/knowledge-base/technology-innovation/promyshlennyjinternet-veshej> (the date of access: 20.02.2023).
3. The industrial internet of things (IIoT): An analysis framework / H. Boyes [et al.] // Computers in Industry. 2018. Vol. 101. P. 1–12. URL: <https://doi.org/10.1016/j.compind.2018.04.015>. (date of access: 16.02.2023).
4. Frankenfield J. Cloud Computing // Investopedia : [site]. 2020. 28 July. URL: <https://www.investopedia.com/terms/c/cloud-computing.asp> (date of access: 22.03.2023).
5. Hamilton E. What is Edge Computing: The Network Edge Explained // Cloudwards : [site]. 2018. 27 Dec. URL: <https://www.cloudwards.net/what-is-edge-computing/> (date of access: 11.02.2023).
6. Chai W., Labbe M., Stedman C. Big data analytics // SearchBusinessAnalytics.com : [site]. 2021. URL: <https://searchbusinessanalytics.techtarget.com/definition/big-data-analytics> (date of access: 3.03.2023).
7. Artificial Intelligence (AI) // Techopedia: [site]. 2020. 27 March. URL: <https://www.techopedia.com/definition/190/artificial-intelligence-ai> (date of access: 15.03.2023).