ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА СИСТЕМНОГО АНАЛІЗУ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Автоматизація виробничих процесів за допомогою інтернету речей (IoT)»

на здобуття освітнього ступеня бакалавра
зі спеціальності 124 Системний аналіз
(код, найменування спеціальності)
освітньо-професійної програми Системний аналіз
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ *Мирослав БОНДІК*
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувачка вищої освіти гр. САД-41
Мирослав БОНДІК
Ім'я, ПРІЗВИЩЕ

Керівник: Ровіл НАФЄЄВ
ст викладач каф. СА. Ім'я, ПРІЗВИЩЕ

Рецензент: _____
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут телекомунікацій

Кафедра Системного аналізу

Ступінь вищої освіти бакалавр

Спеціальність 124 Системний аналіз

Освітньо-професійна програма Системний аналіз

ЗАТВЕРДЖУЮ
Завідувач кафедрою Ровіл НАФЄЄВ
_____Ім'я, ПРІЗВИЩЕ
«_____» _____ 2024р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Бондік Мирослав Дмитрович
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Автоматизація виробничих процесів за допомогою інтернету речей (IoT)
керівник кваліфікаційної роботи к.ф.-м.н. Нафєєв Ровіл Касимович
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «__ _____» _____2024р. № _____
2. Строк подання кваліфікаційної роботи «_____» _____ 2024р.
3. Вихідні дані до кваліфікаційної роботи: Інформаційно-аналітичний метод, інтернет-ресурси, IoT речі, автоматизація

Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз предметної області
2. Дослідження ролі IoT – технологій в промислових мережах
3. Охорона праці та безпека в надзвичайних ситуаціях
4. Перелік ілюстративного матеріалу: *презентація*
5. Дата видачі завдання «_____» _____ 2024р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Збір даних		Виконано
2	Обробка матеріалу		Виконано
3	Аналіз предметної області		Виконано
4	Дослідження ролі IoT – технологій в промислових мережах		Виконано
5	Охорона праці та безпека в надзвичайних ситуаціях		Виконано
6	Інтеграція алгоритму рекомендаційної системи		
7	Висновки за результатами аналізу		Виконано
8	Розробка презентації		Виконано
9	Передзахист		Виконано
10	Здача в деканат		Виконано

Здобувач вищої освіти _____ Мирослав БОНДІК
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Ровіл НАФЄЄВ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут телекомунікацій

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувачка Бондік М.Д. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 124 Системний аналіз
(код, найменування спеціальності)
освітньо-професійної програми Системний аналіз
(назва)
на тему: «Автоматизація виробничих процесів за допомогою інтернету речей (IoT)».

Кваліфікаційна робота і рецензія додаються.

Директор ННІ _____ Владислав КРАВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувачка Бондік Мирослав Дмитрович під час написання кваліфікаційної роботи показала гарну теоретичну підготовку, володіння необхідними знаннями з системного аналізу, користуватися навчальною, довідковою і науково-технічною літературою. Працюючи над завданнями, які доручались керівником, проявила ініціативність, сумлінність та хист до інженерної роботи.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувачки Бондік М.Д. на оцінку «відмінно» та присвоїти їй кваліфікацію **«***Бакалавр з системного аналізу».*

Керівник кваліфікаційної роботи _____ Ровіл НАФЄЄВ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

«____»_____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Бондік М.Д. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедрою Системний аналіз _____ Ровіл НАФЄЄВ
(назва) *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувачка вищої освіти Бондік Мирослав Дмитрович
(прізвище, ім'я, по батькові)
на тему «Автоматизація виробничих процесів за допомогою інтернету речей (IoT).»

Актуальність.

Дослідження IoT-технологій в промислових комп'ютерних мережах є важливим науково-технічним завданням, оскільки розглядає аспекти організації отримання, обміну та передавання інформації від IoT пристроїв і активного мережевого обладнання разом з забезпеченням їх захисту.

Пристрої та застосунки різноманітного роду заполонили наше життя. Серед них є багато "розумних", які моніторять важливі аспекти та активності, надають статистику та рекомендації. Серед них варто виділити критично важливі технології, що базуться на промислових підходах і відносяться до IIoT. Промисловий IoT несе набагато більшу долю відповідальності за своє використання та функціонування, тому що пов'язаний з критично важливими виробничими активностями і безпекою людей.

Позитивні сторони.

1. Виявлено, що впровадження IT технологій дало змогу продовжити роботу, створити безпечні умови праці намісцях та надати віддалений доступ до робочого місця.
2. Виявлено ряд рішень, що відрізняються параметрами зони покриття, споживання енергії, щільності об'єктів, обсягом та храктером даних, які передаються, витратами на встановлення та обслуговування, безпекою.

Недоліки.

1. В роботі мають місце деякі неточності в перекладі технічних термінів.
2. В текстовій частині пояснювальної записки дипломної роботи надано не всі посилання на джерела інформації.

Висновок: *кваліфікаційна бакалаврська робота заслуговує оцінку "відмінно", а здобувач* Бондік Мирослав Дмитрович *заслуговує присвоєння кваліфікації: «Бакалавр з системного аналізу».*

Рецензент: _____ _____
науковий ступінь, вчене звання *підпис* *Ім'я, ПРІЗВИЩЕ*

РЕФЕРАТ

Робота містить 72 сторінки, 7 рисунків, 22 використаних джерел.

У роботі виконано дослідження IoT-технологій в промислових комп'ютерних мережах, що дало змогу визначити ключові аспекти впровадження даних технологій.

Перший розділ кваліфікаційної роботи описує роль індустрії четвертого покоління та місце технології IoT при технологічній трансформації промислового розвитку.

Другий розділ кваліфікаційної роботи присвячений дослідженню впливу цифрової трансформації виробництва в умовах пандемії COVID-19. Виявлено, що впровадження IT технологій дало змогу продовжити роботу і створити безпечні умови праці намісцях. Отримано висновок, що IIoT – це мережа інтелектуальних пристроїв, які відстежують, збирають і аналізують дані в промислових екосистемах.

Метою дослідження є IoT-технології в промислових комп'ютерних мережах. Об'єкт дослідження – процес отримання, передавання та захисту даних в мережах. Предмет дослідження – теорія проектування телекомунікаційних мереж, теорія передавання даних, теорія захисту інформації.

Ключові слова: МЕРЕЖІ, ІОТ-ТЕХНОЛОГІЇ, БЕЗДРОТОВІ МЕРЕЖІ, ІОТ БЕЗПЕКА, ІНДУСТРІЯ 4.0.

ЗМІСТ

Вступ 7
1 Аналіз предметної області 10
1.1 Роль індустрії четвертого покоління 10
1.2 Переваги індустрії I 4.0 13
1.3 Кіберфізичні системи в Індустрії 4.0 18
1.4 Порівняння Індустрії 4.0 та IoT 22
1.5 Висновки до першого розділу 24
2 Дослідження ролі Iот-технологій в промислових комп'ютерних мережах 25
2.1 Цифрова трансформація промисловості 25
2.2 Роль IoT в промислових мережах 27
2.3 Дослідження відмінностей між IoT та IIoT 30
2.4 Дослідження безпеки IoT 34
2.5 Бездротові технології як основа роботи IoT 40
2.6 Дослідження типів бездротових мереж для IoT 43
2.7 Дослідження приватних 5G мереж для IoT 50
2.8 Висновки до другого розділу 56
3 Охорона праці та безпека в надзвичайних ситуаціях 57
3.1 Охорона праці 57
3.1.1 Безпечні умови праці при монтажі комп'ютерної мережі 57
3.2 Безпека в надзвичайних ситуаціях 62
3.2.1 Ультразвук та інфразвук, його вплив на організм людини 62
3.3 Висновки до третього розділу 65
Висновки 66
Список літературних джерел 68

ВСТУП

Україна проходить важливий етап цифрової трансформації. Разом з такими значними досягненнями, як “Дія” країна переймає найновіші технології та підходи, що зараз розвиваються в світі. В умовах технологічного розвитку Індустрії 4.0 важливим постає питання дослідження ролі IoT-технологій в промислових комп’ютерних мережах.

Пристрої та застосунки різноманітного роду заполонили наше життя. Серед них є багато “розумних”, які моніторять важливі аспекти та активності, надають статистику та рекомендації. Серед них варто виділити критично важливі технології, що базуться на промислових підходах і відносяться до IIoT. Промисловий IoT несе набагато більшу долю відповідальності за своє використання та функціонування, тому що пов’язаний з критично важливими виробничими активностями і безпекою людей.

Актуальність теми. Дослідження IoT-технологій в промислових комп’ютерних мережах є важливим науково-технічним завданням, оскільки розглядає аспекти організації отримання, обміну та передавання інформації від IoT пристроїв і активного мережевого обладнання разом з забезпеченням їх захисту.

Мета і завдання дослідження. Метою роботи є дослідження IoT-технологій в промислових комп’ютерних мережах, що дасть змогу визначити новітні підходи в організації роботи таких мереж для забезпечення підтримки IoT-технологій, надасть рекомендації для їх майбутнього розвитку та висвітлить питання безпеки інформації. Досягнення поставленої мети передбачає виконання наступних завдань: дослідити поняття кіберфізичних систем в Індустрії 4.0, провести порівняння IoT та IIoT-технологій, визначити роль IoT в Індустрії 4.0, дослідити безпеку та перспективні технології обміну інформацією IoT.

Об’єкт дослідження – процес отримання, передавання та захисту даних в мережах.

Предмет дослідження – теорія проектування телекомунікаційних мереж, теорія передавання даних, теорія захисту інформації.

Практичне значення одержаних результатів. Описано роль індустрії четвертого покоління та місце технології IoT при технологічній трансформації промислового розвитку. Наведено переваги Індустрії 4.0, що показують важливість використання новітніх технологій для створення швидшого, продуктивнішого, надійнішого, адаптивнішого та безпечнішого середовища у промисловості. Як наслідок, отримується можливість формування нових моделей доходів. Розглянуто поняття кіберфізичних систем і подано визначення цього феномену разом з використанням IoT в ньому. Визначено, що кіберфізичні системи та IoT є нерозривно зв’язані та доповнюють один одного. Проведено порівняння кіберфізичних систем та IoT, що дало змогу узагальнити їх подібність через базування на промисловому Інтернеті та Internet of Everything для виконання функцій покладених на них в конкретних задачах.

Наукова новизна розробки: досліджено впливу цифрової трансформації виробництва в умовах пандемії COVID-19. Виявлено, що впровадження IT технологій дало змогу продовжити роботу, створити безпечні умови праці на місцях та надати віддалений доступ до робочого місця. Проведено дослідження впливу промислового інтернету речей IIoT на роботу промисловості, що показало покращення якості продукції, скорочення часу простоїв, підвищення автоматизації на заводах, оптимізації процесів, створення розумного виробництва та контролю продуктивності. Здійснено дослідження відмінностей між IoT та IIoT, в результаті якого отримано висновок, що IIoT – це мережа інтелектуальних пристроїв, які відстежують, збирають і аналізують дані в промислових екосистемах. Подано архітектуру IIoT, що може бути використана для створення систем з прогнозним

обслуговуванням, обслуговуванням на місцях, відстеженням активів для покращення управління об’єктами. Виявлено, що найбільші ризики для впровадження IIoT пов’язані з безпекою використання. Для задоволення ризиків безпеки потрібно захищати віддалений доступ до IoT пристроїв, а також до сховищ даних і каналів зв’язку. Проведено дослідження бездротових технологій, як основи роботи IoT технології. Виявлено ряд рішень, що відрізняються параметрами зони покриття, споживання енергії, щільності об’єктів, обсягом та храктером даних, які передаються, витратами на встановлення та обслуговування, безпекою. Як частковий випадок організації надійної та захищеної, високопродуктивної бездротової технології для IIoT, досліджено приватні 5G мережі. Рішення щодо їх впровадження мають базуватись на доступності технології в країні, необхідністю використання ліцензованого чи обмежено ліцензованого частостного простору.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Роль індустрії четвертого покоління

Індустрія 4.0 революціонізує спосіб, у який компанії виробляють, покращують і розповсюджують свою продукцію. Виробники інтегрують нові технології, зокрема Інтернет речей (Internet of Things (IoT)), хмарні обчислення та аналітику, а також штучний інтелект і машинне навчання у свої виробничі потужності та у свою діяльність [1-8].

Розумні фабрики оснащені передовими датчиками, вбудованим програмним забезпеченням і робототехнікою, збирають і аналізують дані та дозволяють краще приймати рішення. Ще більша цінність створюється, коли дані виробничих операцій поєднуються з оперативними даними з Enterprise Resource Planning (ERP), ланцюга постачання, обслуговування клієнтів та інших корпоративних систем для створення абсолютно нових рівнів видимості та розуміння на основі раніше закритої інформації.

Ці цифрові технології призводять до підвищеної автоматизації, прогнозованого обслуговування, самостійної оптимізації вдосконалення процесів і нового рівня ефективності та оперативності реагування на потреби клієнтів, які раніше були неможливими.

Розвиток розумних фабрик надає неймовірну можливість для обробної промисловості вступити в четверту промислову революцію. Аналіз обсягів великих даних, зібраних із датчиків на заводі, забезпечує видимість виробничих активів у реальному часі та може надати інструменти для виконання прогнозного технічного обслуговування, щоб мінімізувати час простою обладнання.

Використання високотехнологічних пристроїв IoT на розумних фабриках призводить до підвищення продуктивності та покращення якості. Заміна бізнес-моделей перевірки вручну візуальною статистикою на основі

штучного інтелекту зменшує виробничі помилки та економить гроші і час. З мінімальними інвестиціями персонал контролю якості може налаштувати смартфон, підключений до хмари, щоб контролювати виробничі процеси практично з будь-якого місця. Застосовуючи алгоритми машинного навчання, виробники можуть виявляти помилки відразу, а не на пізніших етапах, коли ремонтні роботи коштують дорожче.

Концепції та технології Industry 4.0 можна застосовувати в усіх типах промислових компаній, включаючи дискретне та процесне виробництво, а також нафтогазову, гірничодобувну та інші промислові сегменти.

Розглянемо чотири етапи революцій у промисловості (рисунок 1.1).

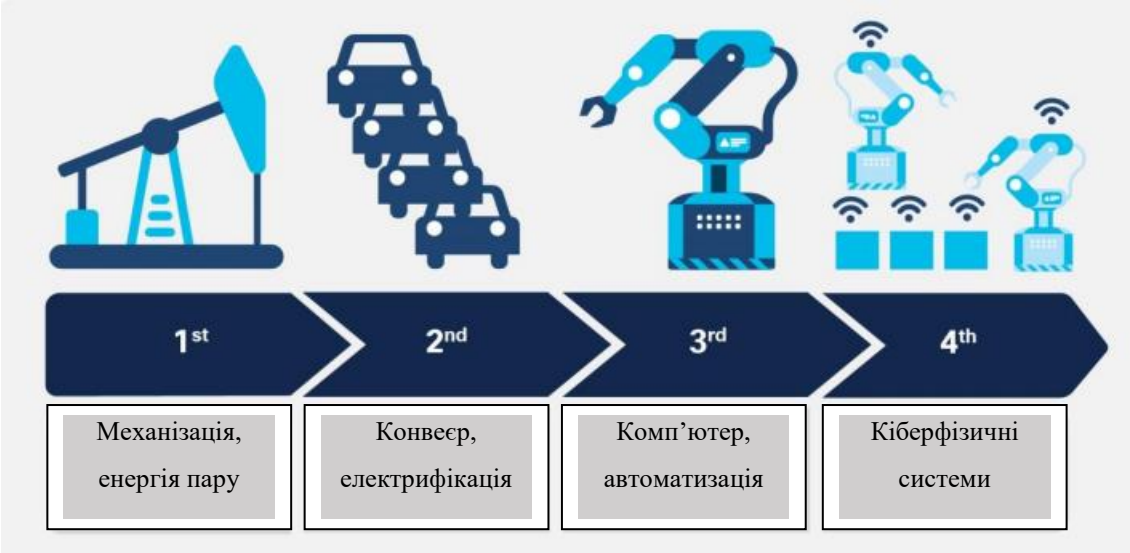


Рисунок 1.1 – Етапи революцій в промисловості

Перша промислова революція була дійсно революцією завдяки винаходу парових машин, використанню енергії води та пари, призведе до промислової трансформації суспільства за допомогою потягів, механізації виробництва і іншого.

Друга промислова революція зазвичай розглядається як період, коли електрика та нові виробничі винаходи, які вона уможливила, наприклад

конвеєр, призвели до масового виробництва та певною мірою до автоматизації.

Третя промислова революція була пов’язана з появою комп’ютерів, комп’ютерних мереж (WAN, LAN, MAN), розвитком робототехніки у виробництві, зв’язком і народженням Інтернету, що змінив правила передачі інформації. З’явились нові методи обробки даних та можливість спільного доступу, а також еволюція версій електронних пристроїв, що створило умови появи середовищ із набагато більшою автоматизацією.

Під час четвертої промислової революції ми переходимо від «просто» Інтернету та моделі клієнт-сервер до повсюдної мобільності, поєднання цифрових і фізичних середовищ (у виробництві це називається кіберфізичними системами), конвергенції IT та OT та всього іншого. Раніше згадані технології (Інтернет речей, великі дані, хмара тощо) з додатковими прискорювачами, такими як передова робототехніка та штучний інтелект/когнітивні засоби, дозволяють Industry 4.0 з автоматизацією та оптимізацією абсолютно новими способами, що дає широкі можливості для інновацій та повного автоматизування і переходу галузі на новий рівень.

Сучасні виробники стикаються з низкою проблем. До них належать:

– продуктивність: робити більше з меншими ресурсами за менших витрат;

– інновації: покращення виробництва, запровадження нових бізнес-моделей і швидше впровадження нових продуктів і послуг;

– обслуговування клієнтів: задоволення та перевищення потреб клієнтів за оптимальною ціною;

– конкурентоспроможність: вирішення викликів глобалізованої економіки.

На основі цих викликів у Німеччині народилася Індустрія 4.0 (I4.0), яка була запущена в 2011 році. Вона стосується запровадження четвертої промислової революції у виробничому секторі, злиття кібернетичного та

фізичного світів для підвищення вартості та конкурентоспроможності в глобальний ринок. Використовуючи чотири принципи дизайну: сумісність, прозорість інформації, технічну допомогу та децентралізоване прийняття рішень, а також базуючись на дев'яти стовпах великих даних, доповненої реальності, моделювання/цифрового двійника, Інтернету речей, хмарних обчислень, кібербезпеки, системної інтеграції, адитивного виробництва та автономних системах, заводи можуть бути трансформовані відповідно до майбутніх потреб. Шлях до І4.0 не буде гладким, доведеться подолати багато проблем, таких як безпека, впровадження, підключення, стандартизація та старіння робочої сили. Проте найбільшою проблемою буде, мабуть, робота із застарілими системами. Системи, які успішно працюють багато років. З цієї причини І4.0 слід розглядати як багаторічний шлях. Дійсно, деякі прогнозують, що І4.0 буде повністю реалізований до 2030 року. Це подорож, яку потрібно ретельно спланувати, профінансувати та здійснити, щоб отримати якомога повнішу користь. Однак, якщо не прийняти І4.0, це може призвести до недостатньої ефективності та конкурентоспроможності. Основою І4.0 повинна бути безпечна, надійна та ефективна комунікаційна інфраструктура, щоб гарантувати, що машини, датчики та люди можуть підключатися найефективнішим способом.

1.2 Переваги індустрії І 4.0

Незалежно від того, чи це буде називатись Industry 4.0, Smart Industry чи Industrial Internet, виробники отримають чимало переваг від зміни способу роботи [9-14].

Основна мета Industry 4.0 – зробити виробництво і пов'язані з ним галузі, такі як логістика – швидшими, ефективнішими та орієнтованими на клієнта, водночас виходячи за рамки автоматизації та оптимізації і виявляючи нові бізнес-можливості та моделі.

Більшість переваг І 4.0, очевидно, подібні до переваг цифрової трансформації виробництва, використання Інтернету речей у виробництві, оптимізації операційних і бізнес-процесів, інформаційних екосистем цінностей, цифрової трансформації в цілому та промислового Інтернету.

Підвищення продуктивності завдяки оптимізації та автоматизації. Це одна з першочергових цілей проектів І 4.0. Іншими словами: економія витрат, підвищення прибутковості, зменшення відходів, автоматизація для запобігання помилкам і затримкам, прискорення виробництва для роботи в режимі реального часу та функції загального ланцюжка створення вартості, де швидкість має вирішальне значення для всіх, оцифрування паперових документів, можливість швидше втручатися у випадку виробничих проблем тощо є перевагами розгортання І 4.0.

Не випадково, що з точки зору витрат основним варіантом використання, в який виробники інвестують свої бюджети Інтернету речей (IoT), є виробничі операції (колосальні 102,5 мільярда доларів США на загальну суму IoT і 178 мільярдів доларів США у всіх варіантах використання виробництва у 2016 році). Industry 4.0 пропонує різні рішення для оптимізації, від оптимізованого використання активів і плавніших виробничих процесів до кращої логістики та управління запасами.

Дані в режимі реального часу для ланцюжка поставок у режимі реального часу в економіці реального часу. Багато переваг підвищення продуктивності пов’язані з внутрішніми цілями витрат і оптимізації процесів. Проте в той же час деякі також вписуються в перспективу посилення клієнтоорієнтованості.

Індустрія 4.0 стосується всього життєвого циклу продукції, і виробництво, очевидно, не стоїть на самоті. Якщо подивитись на весь ланцюжок створення вартості та екосистему, в якій знаходяться виробничі операції, побачимо багато зацікавлених сторін. Це все клієнти. Крім того, клієнти хочуть підвищити продуктивність, незалежно від того, де вони

знаходяться в ланцюжку постачання. Якщо кінцевий споживач хоче отримати якісні продукти швидко та має підвищені очікування щодо досвіду клієнтів, якості, обслуговування та продуктів, які постачаються в потрібний їм час, це впливає на весь ланцюжок постачання, аж до виробництва та далі.

Швидкість – це не лише конкурентна перевага та очікування клієнтів у економіці, що все більше працює в режимі реального часу, а також питання узгодження, витрат і створення цінності. Більш того, клієнти просто цього очікують.

Індустрія 4.0, розумні виробництва, ланцюжки постачання, поінформовані клієнти, узгодження: це все про дані, від фактичних операцій до доставки продукту кінцевому споживачу та далі.

Чим більше даних буде зібрано на ранній стадії та чим своєчасніше ці дані отримають там, де це важливо, коли це важливо, тим більше цінності в ланцюжку постачання. Фактично, це суть одного з трьох вимірів RAMI 4.0, моделі еталонної архітектури Industry 4.0.

Вища безперервність бізнесу завдяки розширеним можливостям обслуговування та моніторингу. Коли промисловий актив виходить з ладу, його потрібно відремонтувати. Це вимагає часу, грошей і дуже часто багато пересування людей підтримки та інженерів.

Коли ключовий промисловий актив, такий як промисловий робот на заводі з виробництва автомобілів зламається, здається, не тільки робот зламався. Це впливає на виробництво, що коштує купу грошей і незадоволених клієнтів, а іноді виробництво може бути повністю перервано. Це найстрашніший кошмар для кожного, оскільки безперервність бізнесу є надзвичайно серйозною проблемою.

Окрім роботи по заміні/ремонту, ресурсів і витрат, репутація може бути пошкоджена, замовлення можуть бути скасовані, а з кожною годиною гроші втрачаються. Якщо промислові активи підключені та їх можна контролювати (наприклад, моніторинг стану здоров’я) через Інтернет речей,

а проблеми вирішуються ще до того, як вони виникнуть, переваги можуть бути величезні. Можна налаштувати сповіщення, активи можна проактивно підтримувати, може стати можливим моніторинг і діагностика в реальному часі, інженери можуть виправляти проблеми, якщо вони виникають на відстані і т.д. Крім того, шаблони й уявлення з'являються для оптимізації в тих сферах, де, здається, частіше виникають проблеми і відкривається світ нових послуг з обслуговування. Не дивно, що управління активами та обслуговування є другою за величиною сферою інвестицій в Інтернет речей у виробництві.

Продукти кращої якості: моніторинг у режимі реального часу, покращення якості за допомогою Інтернету речей та коботування. Якщо у виробничій системі та її ширшому середовищі все пов'язано з інтелектуальними датчиками, програмним забезпеченням, технологіями Інтернету речей, системами аналізу та клієнтом, можна покращити якість своєї продукції. Автоматизація, безперечно, відіграє тут велику роль, а також типові компоненти кіберфізичних систем та Інтернет речей, за допомогою яких аспекти якості можна відстежувати в режимі реального часу при цьому роботи зменшують кількість помилок.

З іншого боку, це один із ризиків і викликів, які потрібно вирішити: чим більше автоматизуєте, тим менше роботи для людей. Те саме стосується інших згаданих переваг, таких як технічне обслуговування (чим менше потрібні інженери для підтримки, тим менше інженерів потрібно). Роботи не скоро займуть усі робочі місця людей. Багато компаній збільшили використання роботів і в той же час найняли більше людей. Причина, чому згадуєтсья про це в контексті якості, полягає в тому, що це одна з областей, де з'являються коботи (коботи – це модний термін для вдосконалених роботів, що підходять для співпраці між людиною та машиною).

Кращі умови праці та стійкість. Якщо говорити про людей, то людський (і соціальний) вимір є всюдисущим в Індустрії 4.0. Крім того, якщо

подивитись на можливості та переваги, то людський, соціальний і навіть стійкий аспект є ключовим у цілях Індустрії 4.0.

Покращення умов праці на основі даних про температуру, вологість та інші дані в реальному часі на заводі чи складі, швидке виявлення та посилений захист у разі інцидентів, виявлення наявності газів, радіації тощо, кращі можливості спілкування та співпраці, зосередження на Ініціативі щодо ергономіки, чистого повітря та чистих фабрик безумовно є в Industry 4.0, оскільки ЄС хоче бути лідером у технологіях чистого повітря та будь-чого.

Персоналізація та налаштування для “нового” споживача. Відомо, що поведінка та вподобання споживачів змінилися. Цифрові інструменти змінили спосіб нашої роботи, покупок і життя.

Люди також стали більш вимогливими, зокрема щодо швидкої відповіді та своєчасної інформації/доставки. Крім того, споживачі також люблять певну персоналізацію залежно від контексту. Взяти, наприклад, спортивне взуття. Вже не тільки достатньо кількох кольорів одного взуття, потрібна можливість налаштувати їх у будь-який спосіб.

Крім того, має місце ще одне явище, яке порушує традиційні ланцюжки поставок. Споживачі все частіше отримують (і хочуть) можливості безпосередньо взаємодіяти з брендом і його виробничими можливостями. Цифрові платформи для налаштування продуктів, як зазначено, скорочені маршрути між виробництвом і доставкою, можливості спільного створення тощо. У багатьох виробничих середовищах це вже трапляється. І це стосується не лише споживчого середовища. Ми все частіше бачимо налаштування в контексті B2B, навіть якщо це просто наклеювання ярлика, додавання спеціальної функції або адаптація будь-якої характеристики продукту.

Якщо існує потреба пропонувати ці послуги у великих масштабах і навіть перетворити їх на конкурентну перевагу, автоматизація та кілька технологій і процесів у І 4.0 стануть необхідністю. Приклад із реального

життя без розголошення подробиць: великий банк хоче використовувати спеціальне офісне обладнання для використання в усіх своїх відділеннях (контекст клієнта) із власним виглядом, відчуттями та функціями в рамках ребрендингу.

Покращена адаптивність. Така ж масштабованість і гнучкість, які ми очікуємо від підтримки IT-сервісів і технологій, таких як хмара, очікуються у виробництві. Це частково пов’язано з попередньою темою налаштування, але головним чином стосується використання технологій, великих даних, штучного інтелекту, роботів і кіберфізичних систем для прогнозування та задоволення сезонного попиту, коливань у виробництві, можливості скорочувати або розширювати; іншими словами: усі коригування, які інколи є більш-менш передбачуваними, можуть бути зроблені більш передбачуваними або непередбачуваними, але з ними можна впоратися завдяки підвищеній видимості, гнучкості та можливості використовувати активи відповідно до оптимальних виробничих вимог з точки зору час і масштаб.

Розвиток інноваційних можливостей і нових моделей доходів. Існує можливість трансформувати процеси, конкретні функції, обслуговування клієнтів, досвід і набори навичок, але врешті-решт справжня цінність генерується шляхом використання нових, часто інформаційно інтенсивних, джерел доходу та екосистем, уможливлюючи інноваційні можливості, наприклад, у розгортанні сервісні можливості для клієнтів, розширені послуги з обслуговування тощо.

1.3 Кіберфізичні системи в Індустрії 4.0

Кіберфізичні системи (Cyber-Physical Systems (CPS)) є будівельними блоками в Індустрії 4.0, з одного боку, і частиною бачення Індустрії 4.0, з іншого [15-20].

Кіберфізичні системи – це комбінації інтелектуальних фізичних компонентів, об’єктів і систем із вбудованими обчислювальними засобами та можливостями зберігання, які під’єднуються через мережі та є засобом реалізації концепції розумної фабрики Індустрії 4.0 у сфері Інтернету речей, даних і послуг, з фокусом на процесах.

Простіше кажучи, як вказує термін, кіберфізичні системи стосуються поєднання цифрового (кібер) і фізичного в промисловому контексті просторів.

Даний термін більше підходить до операційних технологій (OT) конвергентного світу IT/OT, який є типовим для Industry 4.0 та Industrial Internet. Отже, якщо потрібно зрозуміти Індустрію 4.0 або промисловий Інтернет, тоді знадобиться розуміння деяких важливих термінів експлуатації, виробництва та механіки.

Кіберфізичні системи в поданні Industry 4.0 базуються на найновіших системах керування, системах вбудованого програмного забезпечення, а також на IP-адресах (зв’язок з Інтернетом речей стає чіткішим, хоча строго обидва вони не однакові.

У контексті індустрії 4.0 механіки, інженерії тощо кіберфізичні системи розглядаються як наступний етап еволюції постійного вдосконалення вдосконалення та інтеграції функцій (рисунок 1.2).

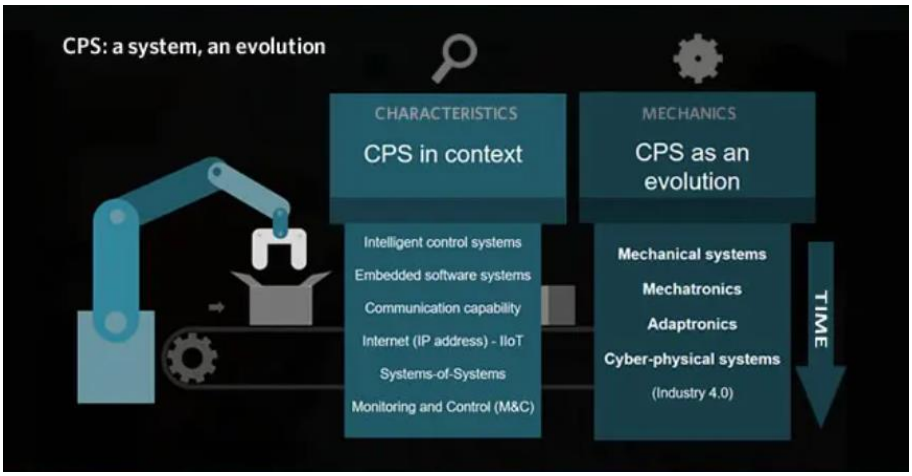
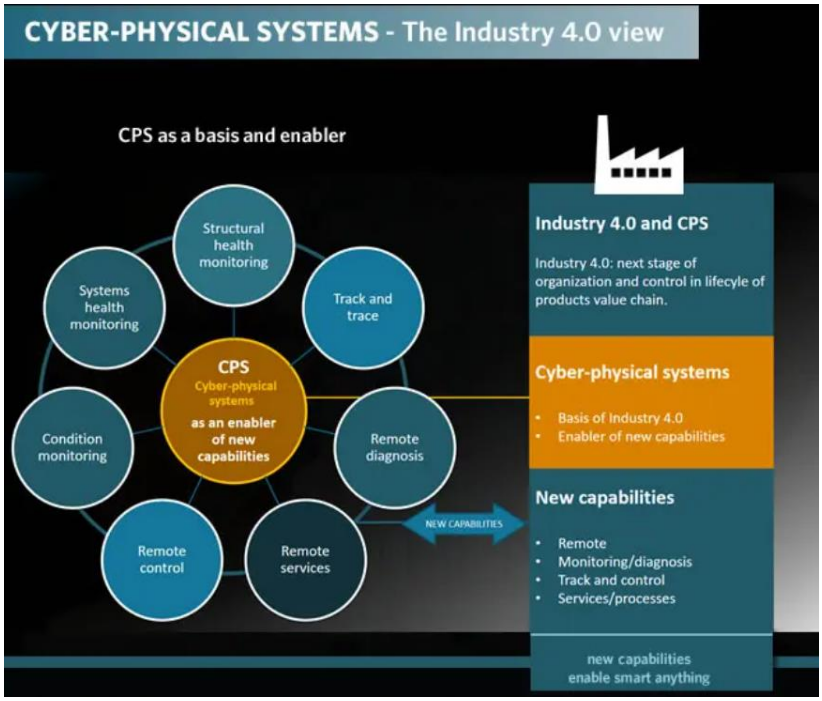


Рисунок 1.2 – Еволюція кіберфізичних систем

Дивлячись на Industry 4.0 як на наступний новий етап в організації та контролі ланцюга доданої вартості протягом життєвого циклу продуктів, це постійне вдосконалення, якому відповідає CPS, почалося з механічних систем і перейшло до мехатроніки (де використовуються контролери, датчики та приводи, більше терміни, які знайомі в IoT) і адаптроніка, а зараз переходить в стадію розвитку кіберфізичних систем.

Кіберфізичні системи, по суті, дозволяють нам створювати промислові системи, здатні спілкуватися між собою та працювати в мережі, що потім використовується у існуючих виробничих можливостях.

Рисунок 1.3 показує узагальнений вигляд кіберфізичних ситем.



Рисунко 1.3 – Загальний вигляд кіберфізичних систем в Індустрії 4.0

Вони створюють нові можливості в таких сферах, як моніторинг здоров’я конструкцій, відстеження, віддалена діагностика, віддалені служби, дистанційне керування, моніторинг стану, моніторинг справності систем тощо.

І саме завдяки цим можливостям, створеним мережевими та взаємодіючими кіберфізичними модулями та системами, можлива така реальність, як підключена або розумна фабрика, розумне здоров’я, розумні міста, розумна логістика тощо.

У 2008 році професор Едвард А. Лі з Каліфорнійського університету в Берклі дав наступне визначення кіберфізичних систем: “Кіберфізичні системи (CPS) – це інтеграція обчислень і фізичних процесів. Вбудовані комп’ютери та мережі відстежують і контролюють фізичні процеси, як правило, із зворотним зв’язком, де фізичні процеси впливають на обчислення, і навпаки”.

На своїй сторінці на веб-сайті Берклі професор Лі посилається на сайт cyberphysicalsystems.org, де можна знайти його визначення та концептуальну карту CPS у формі розумної карти, на якій можна натиснути різні компоненти, щоб прочитати більше.

Кіберфізичні системи також включають параметри симуляції та подвійних моделей, інтелектуальну аналітику, самосвідомість (самоналаштування) тощо.

Підсумуємо деякі ключові характеристики кіберфізичних систем, які пов’язані з Інтернетом речей:

– кіберфізичні системи розглядаються як наступна еволюція у виробництві, механіці та інженерії. Важливими вимірами є поєднання цифрового та фізичного, що стало можливо завдяки Інтернет-технологіям, а також поєднання/конвергенція інформаційних технологій та операційних технологій;

– кіберфізичні системи можуть спілкуватися. Вони мають інтелектуальні системи керування, вбудоване програмне забезпечення та комунікаційні можливості, оскільки їх можна об’єднати в мережу кіберфізичних систем;

– кіберфізичні системи можна однозначно ідентифікувати. Вони мають IP-адресу, що означає, що вони використовують Інтернет-технології та є частиною Інтернету всього, в якому вони можуть бути унікально адресовані (кожна система має ідентифікатор);

– кіберфізичні системи мають контролери, датчики та виконавчі механізми. Це вже було на попередніх етапах до кіберфізичних систем (мехатроніка та адаптроніка); однак, як можна побачити в Інтернеті речей, це відіграє важливу роль.

– кіберфізичні системи є основними будівельними блоками Індустрії 4.0 і забезпечують додаткові можливості у виробництві (і за його межами), такі як відстеження та дистанційне керування;

– можливості, які є завдяки кіберфізичним системам, дозволяють створювати розумні заводи, розумну логістику (Логістика 4.0) та інші інтелектуальні сфери застосування, зокрема в енергетиці, нафті та газі та комунальному господарстві.

Дуже часто Індрустрію 4.0 ототожнюють з IoT технологіями, оскільки вони безпосередньо пов’язані та доповнюють один одного.

1.4 Порівняння Індустрії 4.0 та IoT

Наявність IP-адреси за визначенням означає, що кіберфізичні системи, як об’єкти, підключені до IoT. IP-адреса також означає, що кіберфізична система може бути однозначно ідентифікована в мережі. Це також ключова характеристика Інтернету речей [21-30].

Кіберфізичні системи також оснащені датчиками, приводами та всіма іншими елементами, які є частиною Інтернету речей. Кіберфізичні системи, як і Інтернет речей, потребують підключення. Конкретні технології підключення, які будуть використані залежать від контексту в обох випадках.

Інтернет речей складається з об’єктів із вбудованими або підключеними технологіями, які дозволяють їм приймати дані, збирати їх і надсилати з певною метою. Залежно від об’єкта та мети це може бути збір даних щодо руху, розташування, наявності газів, температури, “здоров’я” пристроїв та ін. Ці дані як такі є лише початком, справжня цінність починається під час аналізу та дії на основі них у межах мети проекту IoT.

Пристрої IoT також можуть отримувати дані та інструкції, знову ж таки залежно від випадку використання. Все це стосується і кіберфізичних систем, які по суті є пов’язаними об’єктами.

Більше того, нові можливості, які надають кіберфізичні системи, такі як моніторинг здоров’я конструкцій, відстеження є тим, що називається випадками використання Інтернету речей.

Можливості відстеження та відслідковування на практиці призводять до багатьох варіантів використання IoT, зокрема, у сфері охорони здоров’я, логістики, складування, доставки, видобутку корисних копалин і навіть у випадках використання Інтернету речей, орієнтованого на споживача. Останній має широкі можливості застосування з численними рішеннями та технологіями. Можна відстежувати свій скейтборд, своїх домашніх тварин, що завгодно, за допомогою IoT.

Моніторинг здоров’я конструкцій також є повсюдним, головним чином у таких галузях, як машинобудування, технічне обслуговування будівель, управління об’єктами тощо. За допомогою правильних датчиків і систем можна контролювати стан конструкцій усіх видів об’єктів, від мостів і об’єктів у будівлях до виробничих активів і кіберфізичні активи у виробництві та Індустрії 4.0.

Підводячи підсумок: фактично можна назвати кіберфізичні системи (хоча й передовими) речами в промисловому Інтернеті речей у виробництві. Таким чином, CPS та IoT де-факто є більш ніж близнюками.

Основна ідея використання IoT в промислових мережах зводиться до надання розумності можливостям технологічного розвитку для забезпечення зростання суспільного добробуту і задоволеності користувачів.

1.5 Висновки до першого розділу

Перший розділ кваліфікаційної роботи описує роль індустрії четвертого покоління та місце технології IoT при технологічній трансформації промислового розвитку. Наведено переваги Індустрії 4.0, що показують важливість використання новітніх технологій для створення швидшого, продуктивнішого, надійнішого, адаптивнішого та безпечнішого середовища у промисловості. Як наслідок, отримується можливість формування нових моделей доходів. Розглянуто поняття кіберфізичних систем і подано визначення цього феномену разом з використанням IoT в ньому. Визначено, що кіберфізичні системи та IoT є нерозривно зв’язані та доповнюють один одного. Проведено порівняння кіберфізичних систем та IoT, що дало змогу узагальнити їх подібність через базування на промисловому Інтернеті та Internet of Everything для виконання функцій покладених на них в конкретних задачах.

2 ДОСЛІДЖЕННЯ РОЛІ ІОТ-ТЕХНОЛОГІЙ В ПРОМИСЛОВИХ КОМП'ЮТЕРНИХ МЕРЕЖАХ

2.1 Цифрова трансформація промисловості

Переробна промисловість є рушійною силою провідних індустріальних економік світу, на яку припадає майже 16% світового ВВП.

Понад десять років лідери виробництва та технологічні партнери працюють над прискоренням індустрії 4.0 і стратегій цифрової трансформації, щоб досягти бізнес-результатів: операційної ефективності, скорочення позапланових простоїв, стійкості безпеки, а також моніторингу навколишнього середовища [31-35].

Незважаючи на те, що комерційне обґрунтування інвестицій у цифрову трансформацію є переконливим, компаніям, звичайно, потрібно щороку збалансовувати свої рішення щодо капіталовкладень.

Оскільки країни в усьому світі миттєво припинили роботу, глобальне виробництво впало на 6% у першому кварталі 2020 року та на 3,6% за весь рік.

Навіть там, де обробна промисловість була оголошена основною, виробникам довелося призупинити або скоротити роботу протягом пандемії, щоб врахувати спалахи серед працівників, фізичне дистанціювання на виробництві, віддалену роботу та збої в громадському транспорті та ланцюгу поставок.

Виробничим компаніям потрібно було швидко переорієнтуватися, щоб дозволити працівникам, які працюють вдома, дистанційно керувати своїми системами. Їм потрібно було знайти нових постачальників. І їм потрібно було забезпечити безпеку цих з'єднань.

У результаті, як і в багатьох галузях промисловості, виробники майже миттєво збільшили свої інвестиції в цифрову трансформацію.

Частково завдяки цим інвестиціям фабрики змогли продовжити роботу, співробітники змогли працювати безпечно та, у багатьох випадках, віддалено, а вплив COVID19 був пом’якшений.

Насправді дані Всесвітнього центру конкурентоспроможності IMD показують нам K-подібне відновлення, коли компанії, які розуміються на цифрових технологій, відновлювалися швидше, ніж інші організації після економічного спаду в березні 2020 року.

Оскільки IT-фахівці та спеціалісти з операційної діяльності працюють над інноваціями традиційних виробничих потужностей і операцій, повинно бути враховано, що цифрове виробництво вимагає більше мереж.

Крім високої продуктивності та надійності, промислові маршрутизатори, комутатори та брандмауери повинні витримувати такі суворі умови навколишнього середовища, як екстремальні температури, удари, вібрація та вологість. Вони також повинні мати можливість контролювати доступ, підтримувати промислові протоколи в реальному часі та забезпечувати переміщення ключових операційних даних між додатками в хмарі. Крім того, робочі мережі, які вони будують, повинні бути масштабованими та високостійкими.

Виробнича мережа є спільним проектом команд IT та OT. Якщо це IT-команда, потрібне рішення, яке працюватиме з існуючими програмами для керування мережею та безпекою та не потребуватиме значного навчання чи перерв. Існує потреба автоматизувати технічне обслуговування мережі та швидко виявляти і вирішувати проблеми продуктивності, особливо в цьому критично важливому для бізнесу просторі. Якщо працівник в команді OT, ймовірно, він не IT-фахівець. Тоді потрібна видимість проблем, які впливають на доступність, якість продукції, ефективність робочої сили, і чіткі рекомендації щодо їх вирішення. Існують рішення, що автоматизує трудомісткі завдання вручну, постійно відстежує стан мережі та надає звіти та елементи керування на зручній інформаційній панелі.

Виробники одночасно розширюють виробництво, гіперналаштовують продукти, покращують операції та запускають нові продукти та послуги. Щоб досягти цих цілей, потрібна гнучкість, щоб масштабувати потужність продукту, змінювати асортимент продуктів і перерозподіляти ресурси за потреби. Для швидкого переміщення мережевих та виробничих ресурсів туди, куди вони потрібні, потрібно використовувати технологію Plug-and-Play.

Кібербезпека починається зі знання всього, що підключено до промислової мережі, хто спілкується один з одним і що вони говорять. Існують рішення, що автоматично проводять повну інвентаризацію. Команди ОТ використовують графічний інтерфейс для створення виробничих зон (так званих сегментів мережі), що містять усі активи, які потребують обміну даними.

2.2 Роль IoT в промислових мережах

Виробнича промисловість швидко трансформується завдяки впровадженню передових технологій, таких як штучний інтелект, машинне навчання та Інтернет речей. Ця цифрова трансформація значно покращила якість продукції та скоротила час простою процесів і машин. Промисловий Інтернет речей і автоматизація відіграють важливу роль у цьому процесі [36].

Промисловий Інтернет речей (Industrial IoT (IIoT)) приносить масштабні зрушення в промислові програми завдяки своїм унікальним функціям. Це суттєво сприяє підвищенню операційної ефективності та робочих процесів заводів завдяки моніторингу активів і процесів у реальному часі. IIoT дає багато можливостей, якими можуть скористатися промисловці, щоб покращити галузь у десятки разів [37-45].

До основних можливостей, що отримуються при впровадженні IoT можна віднести:

– автоматизація на заводах;
– оптимізація процесів;
– розумне виробництво;
– контроль продуктивності

IoT відповідає за надшвидку еволюцію індустрії 4.0, де все об’єднано в загальній мережі, а операції здебільшого автоматизовані, що усуває потребу в значному втручанні людини. Моніторинг даних у реальному часі покращує процес прийняття рішень, а передбачуваність допомагає зменшити ймовірність майбутніх небезпек у галузі, супроводжуючи управління активами для майбутньої працездатності. Основні етапи розвитку IoT та індустрії 4.0:

– підключення речей;
– генерування ідей;
– оптимізація операцій і процесів;
– інновація.

Основна мета IoT – зробити все розумним, будь то будинок, будівля, охорона здоров’я чи фабрика. З іншого боку, галузь 4.0 складається з кібербезпеки, доповненої реальності, автономних роботів, цифрових близнюків, хмарних обчислень, великих даних, підключених пристроїв і важкої техніки. Підключені пристрої, розумна фабрична мережа та важке обладнання є головною точкою перетину індустрії 4.0 та IoT. IoT рухається до концепції досконалості у виробництві, відіграючи життєво важливу роль у кожній промисловій діяльності та неймовірно покращуючи її. IoT є найкращою технологією для промисловості, оскільки вона генерує цінні результати завдяки поєднанню інформаційних технологій і операційних технологій для процесів.

Перевагами використання IoT у промисловості є:

– підвищена ефективність;
– прогнозне обслуговування;

– моніторинг даних в реальному часі;
– знижена вартість.

Підвищення ефективності є однією з найважливіших переваг IoT. Він має можливість підвищити ефективність роботи шляхом оптимізації промислового процесу. Він також має можливість автоматизації, що підвищує продуктивність і оптимізує функціонування заводів. Датчики, вбудовані у виробничі активи, використовуються для відстеження їх продуктивності з метою їх модифікації та вдосконалення відповідно до вимог.

Промислова продуктивність значною мірою залежить від продуктивності активу та його працездатності. Прогнозне технічне обслуговування, яке забезпечується впровадженням Інтернету речей, може допомогти менеджерам процесів прогнозувати працездатність активу та реагувати на нього, щоб не завдати серйозної шкоди продуктивності та роботі в довгостроковій перспективі. Датчики IoT, встановлені на заводських активах, контролюють їхню роботу в режимі реального часу та надсилають сповіщення менеджеру, якщо виявлено будь-яку несправність. Ці несправності усуваються в найкоротші терміни, що запобігає величезним збиткам компанії.

Роботу та продуктивність активів можна контролювати в режимі реального часу, вносячи відповідні зміни в процес, щоб продуктивність і якість продукції суттєво зросли. Крім того, моніторинг даних у режимі реального часу допомагає в процесі прийняття рішень і підвищує ефективність роботи на заводі.

Прогнозне технічне обслуговування та функції моніторингу даних у режимі реального часу IoT значно сприяють зниженню витрат, роблячи обладнання достатньо розумним, щоб виконувати операції самостійно без нагляду людини. Зменшення людського втручання автоматично зменшує кількість помилок; таким чином вартість також зменшується.

Незалежно від того, чи йдеться про нафту та газ, транспорт, виробництво, енергетику чи готельний бізнес, майже кожна галузь може впровадити інтелектуальні системи на основі Інтернету речей, щоб підвищити свою продуктивність із меншими витратами. Датчики, шлюзи, інформаційні панелі та додатки є основними частинами рішень IoT, розроблених і здатних працювати та контролювати в екстремальних умовах.

Четверта промислова революція значною мірою змінила те, як сприймаються речі у виробництві. Інтернет речей робить значний внесок у процес інтелектуалізації промисловості та значного покращення робочих процесів.

2.3 Дослідження відмінностей між IoT та IIoT

Промисловий Інтернет речей (IIoT) – це використання інтелектуальних датчиків і приводів для вдосконалення виробничих і промислових процесів. Він також відомий як промисловий Інтернет або Індустрія 4.0, IIoT використовує потужність розумних машин і аналітику в реальному часі, щоб скористатися перевагами даних, які “нерозумні машини” виробляли в промислових умовах роками. Філософія, що лежить в основі IIoT, полягає в тому, що розумні машини не тільки краще, ніж люди, збирають і аналізують дані в режимі реального часу, але вони також краще передають важливу інформацію, яку можна використовувати для швидшого й точнішого прийняття бізнес-рішень [46-50].

Підключені датчики та виконавчі механізми дозволяють компаніям швидше виявляти неефективність і проблеми та економити час і гроші, одночасно підтримуючи зусилля бізнес-аналітики. У виробництві, зокрема, IIoT має великий потенціал для контролю якості, стійких і екологічних практик, відстеження ланцюга постачання та загальної ефективності ланцюга постачання. У промисловому середовищі IIoT є ключовим для таких

процесів, як прогнозне технічне обслуговування (Predictive maintenance (PdM)), розширене обслуговування на місцях, управління енергією та відстеження активів.

IIoT – це мережа інтелектуальних пристроїв, підключених до систем, які відстежують, збирають, обмінюються й аналізують дані. Кожна промислова екосистема IoT складається з:

– підключених пристроїв, які можуть відчувати, передавати та зберігати інформацію про себе;

– державної та/або приватної інфраструктури передачі даних;

– аналітики та програми, які генерують бізнес-інформацію з вихідних даних;

– зберігання даних, які генеруються пристроями IIoT;

– люди.

Ці периферійні пристрої та інтелектуальні активи передають інформацію безпосередньо в інфраструктуру передачі даних, де вона перетворюється на актуальну інформацію про те, як працює певна частина техніки. Цю інформацію можна використовувати для прогнозного обслуговування, а також для оптимізації бізнес-процесів.

На рисунку 2.1 показано архітектуру IIoT.

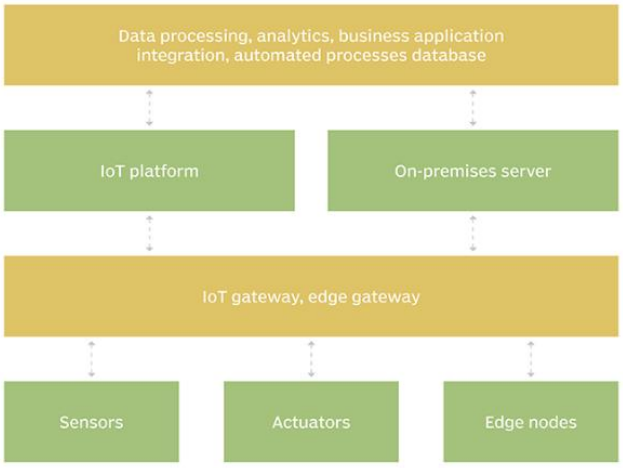


Рисунок 2.1 – Архітектура IIoT

Одна з найбільш рекламованих переваг пристроїв IIoT, які використовуються у виробничій промисловості, полягає в тому, що вони дають можливість прогнозного обслуговування. Організації можуть використовувати дані в реальному часі, отримані від систем IIoT, щоб передбачити, коли машину потрібно буде обслуговувати. Таким чином необхідне технічне обслуговування можна виконати до того, як станеться збій. Це може бути особливо корисним на виробничій лінії, де відмова машини може призвести до зупинки роботи та великих витрат. Завчасно вирішуючи питання технічного обслуговування, організація може досягти кращої операційної ефективності.

Ще одна перевага – ефективніше обслуговування на місцях. Технології IIoT допомагають фахівцям з виїзного обслуговування виявляти потенційні проблеми в обладнанні клієнта, перш ніж вони стануть серйозними проблемами, дозволяючи технікам вирішувати проблеми, перш ніж вони створять незручності клієнтам. Ці технології також можуть надавати технікам виїзного обслуговування інформацію про те, які деталі їм потрібні для ремонту. Таким чином технік матиме при собі необхідні деталі, коли звернеться до сервісного центру.

Відстеження активів – ще одна перевага Інтернету речей. Постачальники, виробники та клієнти можуть використовувати системи управління активами для відстеження місцезнаходження, статусу та стану продуктів у всьому ланцюжку постачання. Система надсилає миттєві сповіщення зацікавленим сторонам, якщо товари пошкоджені або ризикують бути пошкодженими, даючи їм можливість вжити негайних або превентивних заходів для виправлення ситуації.

IIoT також дозволяє підвищити рівень задоволеності клієнтів. Коли продукти підключено до Інтернету речей, виробник може отримувати та аналізувати дані про те, як клієнти використовують їхні продукти, що

дозволяє виробникам і дизайнерам продуктів створювати більш орієнтовані на клієнта дорожні карти продукту.

IoT також покращує управління об’єктами. Виробниче обладнання схильне до зносу, який може посилюватися певними умовами на заводі. Датчики можуть контролювати вібрацію, температуру та інші фактори, які можуть призвести до неоптимальних умов роботи.

Найбільші ризики, пов’язані з використанням Інтернету речей, стосуються безпеки. Відносно часто для пристроїв IIoT продовжують використовувати паролі за замовчуванням навіть після того, як вони були розміщені у виробництві. Подібним чином багато пристроїв IIoT передають дані у вигляді відкритого тексту. Ці умови дозволили б зловмиснику відносно легко перехопити дані, що надходять із пристрою IIoT. Подібним чином зловмисник може заволодіти незахищеним пристроєм IIoT і використовувати його як платформу для запуску атаки на інші мережеві ресурси.

Безпека є великою проблемою для тих, хто відповідає за пристрої Інтернету речей в організації, але також і керування пристроями. Оскільки організація використовує все більше і більше пристроїв IIoT, стає все більш важливим прийняти ефективну стратегію керування пристроями. Якщо говорити точніше, організації повинні мати можливість точно ідентифікувати пристрої IIoT, щоб запобігти використанню фальшивих пристроїв. Встановлення засобів ідентифікації кожного окремого пристрою також має вирішальне значення для таких завдань, як заміна несправного пристрою або виконання оновлення пристрою.

Управління виправленнями є ще одним великим викликом для пристроїв IIoT. Виробники пристроїв дедалі частіше випускають періодичні оновлення мікропрограми. Організації повинні мати ефективні засоби перевірки пристроїв, щоб дізнатися, чи встановлено на них останню версію мікропрограми, і розгортання нової мікропрограми, якщо це необхідно. Крім

того, такий інструмент повинен відповідати встановленому графіку технічного обслуговування організації, щоб не порушувати роботу.

Хоча IoT і IIoT мають багато спільних технологій, включаючи хмарні платформи, датчики, підключення, міжмашинний зв'язок і аналіз даних, вони використовуються для різних цілей.

Програми IoT з'єднують пристрої в різних вертикалях, включаючи сільське господарство, охорону здоров'я, підприємства, споживачів і комунальні служби, а також уряд і міста. Пристрої IoT включають розумні пристрої, браслети для фітнесу та інші програми, які зазвичай не створюють надзвичайних ситуацій, якщо щось піде не так.

Програми IIoT, з іншого боку, з'єднують машини та пристрої в таких галузях, як нафтогаз, комунальне господарство та виробництво. Системні збої та простої в розгортанні IIoT можуть призвести до ситуацій високого ризику або навіть до загрози життю. Програми IoT також більше уваги приділяють підвищенням ефективності та покращенням здоров'я чи безпеки, а не орієнтованим на користувача характером додатків IoT.

2.4 Дослідження безпеки IoT

Занепокоєння безпекою IIoT випливають із збільшення поверхні атаки та необхідності віддаленого доступу. Оскільки все більше пристроїв і датчиків підключаються до мережі, вони створюють більше каналів зв'язку, сховищ даних, портів і кінцевих точок. Цей підвищений взаємозв'язок створює більше вразливостей, якщо його залишити незахищеним [51-54].

Огляд промислових рішень IoT розбивається на три категорії: локальні мережі, обробка даних і керування кінцевими точками.

Виробники та інші промислові користувачі IoT повинні серйозно ставитися до безпеки навіть у межах своєї локальної мережі. У той час як меншій компанії доведеться лише налаштувати певною мірою однакові

заходи безпеки для комп'ютерів і серверів, об'єкт IIoT представлятиме унікальні проблеми через різноманітність обладнання, що використовується в різних місцях.

Багато пристроїв IIoT не створювалися з оптимальною системою безпеки. Для пріоритету безпеки в локальній мережі IIoT потрібно, щоб усі пристрої були захищені від несанкціонованого доступу незалежно від того, якими функціями вони володіють.

Іншою потенційною вразливістю для виробничих підприємств IIoT є збільшення обміну даними між мережами пристроїв і засобів IIoT.

Оскільки кількість інтелектуального обладнання продовжує зростати, створюється більше сховищ даних і шлюзів, які потрібно захищати. Порушення конфіденційних даних може призвести до загрози безпеці, несправності обладнання або простою самовідмови в обслуговуванні.

Мережеві порти можуть бути під загрозою атаки, якщо вони неправильно налаштовані, залишені відкритими або застосовуються неналежні методи автентифікації. Дані, що передаються через ці порти, можуть бути легко доступні кібератакам, а порти, які часто використовуються, можуть піддаватися більшому ризику, тому важливо захищати порти.

Хоча деякі аспекти IIoT вказують на підвищену автоматизацію, все ще є техніки, менеджери та інженери, які повинні взаємодіяти з обладнанням. Ці кінцеві точки є основними цілями для кіберзлочинців.

Якщо кінцеві точки не мають чітко визначених дозволів користувача та вбудованої багатофакторної автентифікації, мережа пристроїв IIoT вразлива до несанкціонованої діяльності та дорогих перебоїв. Подібно до того, як індустрія роздрібної торгівлі повинна зосередитися на безпеці POS, керування кінцевими точками має вирішальне значення для виробників, які намагаються досягти оптимальної безпеки.

Навіть незважаючи на те, що виробники зосереджуються на тому, щоб запровадити більше датчиків, більшість пристроїв IIoT, створених виробниками, все ще надають перевагу функціоналу операційних технологій над IT-безпекою. Однак безпечні віддалені з'єднання на виробництві – це те, що дозволяє безперебійно функціонувати операційній технології, тому їм слід відповідно розставити пріоритети.

На риснку 2.2 показано віддалений доступ при використанні IIoT прстроїв на виробництві.

Рисунок 2.2 – Віддалений доступ до IIoT пристроїв

Щоб забезпечити нульовий простой на заводах, виробники комплектного обладнання та промислові центри управління розумно інтегрують програмне забезпечення безпечного віддаленого доступу у свої мережі. Основні програми віддаленого входу, такі як RDP і VNC, не розроблені з урахуванням сумісності та безпеки IIoT. RDP і VNC не мають безпеки (особливо, коли мова йде про контроль доступу та автентифікацію користувачів у мережах) та інтелекту, які потрібні більшості OEM-машин. Для належного захисту OEM потрібне спеціальне, повністю масштабоване програмне забезпечення віддаленого доступу.

Багато об'єктів Інтернету речей уже беруть до уваги питання безпеки. Нещодавнє дослідження Kaspersky показало, що більше половини

промислових організацій вважають, що IoT змінить їхні погляди на безпеку, а 20% організацій вже інвестували в рішення безпеки для IoT.

Важливо розуміти, що незалежно від того, використовується локальна чи хмарна модель зберігання та аналітики даних IIoT, безпечний віддалений доступ має бути пріоритетом.

Кожна модель створює унікальні проблеми безпеки. Наприклад, у той час як датчики та контролери можуть бути обмежені однією локальною мережею, технічні спеціалісти та користувачі, які споживають дані, все частіше перебувають за межами підприємства. Пристрої IIoT можуть бути обмежені середовищем локальної мережі, але користувачі подорожують, тому надійний захист віддаленого доступу все ще є обов'язковим.

Завдяки хмарній моделі команда зможе більше зосередитися на оптимальній операційній технологічній функціональності пристроїв, оскільки більшість IT може бути передано хмарним додаткам. Однак це створює більшу поверхню для атаки та більше шлюзів, які необхідно захистити.

Також варто відзначити, що хмарні послуги більше не призначені лише для зберігання даних. Зараз значна частина хмарних обчислень – це активна обробка й аналітика, які можна виконувати в хмарі аж до межі вашої мережі, ця практика називається периферійними обчисленнями. Дозвіл хмари виконувати обробку, яка все ще може виконуватися на ваших пристроях або поблизу них, означає швидший аналіз і доступ до більш корисної інформації для техніків і менеджерів.

Програмне забезпечення віддаленого доступу може не тільки зменшити ризик, але й підвищити ефективність виробництва. Наведемо деякі з переваг використання програмного забезпечення віддаленого доступу в IIoT:

– покращене підключення без підвищеної вразливості;

– зниження витрат на дорогу (завдяки дистанційному моніторингу та виправленню поломок);

– покращена безпека для співробітників;

– налаштування, що підвищує продуктивність;

– широке відстеження та документація

Хоча деякі конкретні тактики безпечного віддаленого доступу залежать від сфери виробництва, багато стратегій залишаються характерними рисами програмного забезпечення віддаленого доступу незалежно від того, в якій галузі вони використовуються.

Заводи використовують пристрої, які вимагають частого доступу різних користувачів. Однак, якщо неавторизовані користувачі мають доступ до приватних областей мережі, вона може бути вразливою до кіберзагроз.

З такою кількістю користувачів, які працюють на різних типах пристроїв у виробничому середовищі, надзвичайно важливо мати можливість налаштовувати детальний контроль над дозволами користувачів. Таким чином можна дізнатися, хто має доступ, а хто ні, і чи було порушення цього доступу.

RDP і VNC пропонують обмежений контроль доступу, особливо для користувачів за межами локальної мережі. Вибір спеціального безпечного програмного забезпечення для віддаленого доступу дозволяє організаціям налаштувати доступ і контроль.

Багато розумних пристроїв, які відстежують і забезпечують живлення виробничих процесів, досі не мають основних функцій безпеки, таких як надійні паролі та оновлення програмного забезпечення.

Пристрої IIoT без належного контролю безпеки слід відокремити в спеціальні сегменти мережі, де їх не можна використовувати як плацдарм для атак на інші пристрої. Тоді програмне забезпечення для віддаленого доступу дозволить вам реалізувати надійну багатофакторну автентифікацію в усьому світі. Жоден пристрій не залишиться без захисту. На додаток до більш

надійної автентифікації пристрої можна перевіряти на наявність необхідних виправлень і оновлень за потреби.

Шифрування відноситься до складних алгоритмів, які відволікають неавторизованих користувачів, що намагаються отримати доступ до конфіденційних даних. Тим не менш, багато неймовірно послідовних пристроїв на виробництві обмінюються даними без шифрування або, принаймні, без достатнього шифрування.

Шифрування кінцевих точок і шлюзів дає програмному забезпеченню віддаленого доступу перевагу перед програмами віддаленого робочого стола, які створюють файли cookie. За допомогою 256-бітного шифрування дані, які передаються та зберігаються пристроями IIoT, будуть захищені від кіберзлочинців.

З розвитком промислового Інтернету речей багато виробників використовують можливість підвищити ефективність за рахунок покращення кібербезпеки. Більший час безвідмовної роботи у виробничій організації означає більшу продуктивність. І це неможливо без герметичних заходів безпеки, щоб зменшити ризики перебоїв у наданні послуг.

Для виробництва та за його межами безпечний віддалений доступ швидко стає ключем до максимізації продуктивності. Незалежно від того, в якій галузі працюєте, віддалений доступ дозволяє безпечно працювати в локальній мережі та поза нею. За допомогою спеціального програмного забезпечення можна створити багаторівневе рішення безпеки, яке підходить для підприємства та бездоганно інтегрується у стек технологій.

Така програма дозволяє організації централізувати віддалений доступ і підключитися до складних мережевих середовищ.

На даний час існує багато рішень від різних виробників для задоволення потреб IIoT безпеки і тому питання вибору конкретного варіанту має бути окремо досліджено.

2.5 Бездротові технології як основа роботи IoT

Wi-Fi відіграв основоположну роль у розробці інновацій IoT, забезпечуючи повсюдне підключення для під'єднання різноманітних речей один до одного, до Інтернету та до 18 мільярдів пристроїв Wi-Fi, які використовуються по всьому світу. Економічний потенціал Інтернету речей безмежний, а Wi-Fi надає широкий спектр можливостей у різноманітних секторах, включаючи розумні будинки, розумні міста, автомобільну промисловість, охорону здоров'я, підприємства, державні та промислові середовища IoT.

Wi-Fi дозволяє користувачам автоматизувати свої розумні будинки та підключати різноманітні побутові об'єкти, контролювати ланцюжки поставок та інші важливі функції в режимі реального часу на промислових об'єктах, а також розблокувати цінність бізнесу за рахунок підвищення продуктивності та ефективності як для підприємств, так і для гібридної роботи. Інтеграція та сумісність, які забезпечує Wi-Fi, дозволять рішенням Інтернету речей безпечно з'єднуватися між собою та з мільярдами орієнтованих на користувачів пристроїв, щоб розблокувати найбільшу цінність програм і середовищ Інтернету речей.

Рисунок 2.3 – Можливості Wi-Fi для задоволення потреб IoT

Wi-Fi є однією з найбільш широко використовуваних технологій у всьому світі, і інтеграція з існуючими мережами Wi-Fi, широкий спектр технологій і сильна спадщина взаємодії роблять очевидним вибір, щоб отримати найбільшу цінність від IoT (рисунок 2.3). Wi-Fi буде відігравати важливу роль майже в кожному середовищі IoT, окремо або разом із більш спеціалізованими протоколами чи технологіями. Кілька унікальних компетенцій, які унікально позиціонують Wi-Fi для IoT, включають:

Базована на стандартах сумісна технологія: перспективи IoT базуються на широкому діапазоні виробників пристроїв. Wi-Fi надає загальну платформу для доставки все більшої кількості додатків IoT, які відрізняються вимогами до продуктивності, потужності та затримки. Wi-Fi сертифікація забезпечує впевненість у тому, що мільярди пристроїв будуть взаємодіяти та забезпечувати якісну взаємодію з користувачем незалежно від бренду продукту.

Повсюдне підключення: системами IoT часто керують за допомогою мобільних пристроїв, а Wi-Fi дозволяє безперешкодно контролювати смартфони, планшети та 18 мільярдів пристроїв Wi-Fi, які вже використовуються сьогодні, щоб допомогти розкрити весь потенціал IoT. Поширене глобальне підключення дає змогу користувачам і мережевим операторам підключатися до єдиної системи та керувати нею.

Перевірена безпека WPA3™: конфіденційна державна, промислова та особиста інформація обмінюється через програми IoT. Wi-Fi забезпечує перевірену безпеку WPA3™ для захисту інформації, якою обмінюються в особистому та корпоративному середовищах. Вибір пристроїв IoT, сертифікоавних на основі Wi-Fi, гарантує захист даних за допомогою найновіших протоколів безпеки корпоративного рівня.

Економічне та просте розгортання: Wi-Fi є простим у розгортанні та економічно ефективним фундаментом, який не потребує окремих шлюзів або спеціальних навичок для доставки програм IoT. Користувачі в усьому світі

покладаються на Wi-Fi та його щоденне розгортання. Ращом з цим він продовжує розвиватися, щоб спростити підключення пристроїв, автентифікацію в мережі тощо.

Зворотна сумісність: Wi-Fi – це розумна інвестиція для архітекторів продуктів IoT, які враховують вартість, надійність і підтримку для перспективних інвестицій у свої технології. Wi-Fi витримав випробування часом, що мінімізує ризик передчасного старіння та гарантує, що старі пристрої можуть легко підключатися до домашніх мереж.

Розташування: Wi-Fi Location™ надає інформацію про місцезнаходження на субметровому рівні, що дозволяє використовувати низку IoT-сервісів із визначенням розташування для промислових і розумних міських середовищ, забезпечуючи розширені переваги, такі як управління активами, керування мережею та геозонування.

Надійне та складне підключення: домашні та промислові мережі IoT потребують постійного та надійного підключення. Мережі Wi-Fi 6 забезпечують ефективність мережі, діагностику, керування та можливості оптимізації. Wi-Fi 6 і Wi-Fi 6E обслуговують декілька одночасно підключених пристроїв і велику пропускну здатність даних, забезпечуючи високу продуктивність і низькі затримки для програм, включаючи потокове відео 4K і AR/VR. Wi-Fi 6 і Wi-Fi 6E також дозволяють таким пристроям, як виробничі роботи та дрони, залишатися на зв’язку, навіть коли вони рухаються або “кочують” по домашній або промисловій мережі.

Гнучка топологія мережі: на додаток до традиційного з’єднання Wi-Fi через точки доступу EasyMesh®, Aware™ і Direct® пропонують різноманітні мережеві топології для різних середовищ IoT, для масштабованих і настроюваних параметрів, для задоволення потреб мережі IoT і додатків IoT. Wi-Fi пропонує адміністраторам мереж гнучкіші варіанти топології для мережевих з’єднань IoT, ніж виключно зіркова або сітчаста топології.

Велике портфоліо Wi-Fi спрямоване на випадки використання IoT, які підтримують програми з високою пропускною спроможністю та малою затримкою, такі як AR/VR, а також вимоги до великого радіусу дії та низькі вимоги до енергоспоживання для програм відстеження активів або систем сільського зрошення. Сертифікати Wi-Fi, такі як Wi-Fi 6®, HaLow™, Easy Connect і QoS Management забезпечують здатність задовольняти унікальні IoT можливості у різних середовищах використання.

2.6 Дослідження типів бездротових мереж для IoT

Щоб запустити успішний IoT-проект, повинне бути надійне з'єднання (мережі IoT) між пристроями/сенсорами та платформою IoT. Для вибору найкращого рішення для IoT проекту потрібно дослідити наявні рішення і визначити їх характеристики.

Мережа IoT – це мережа з фізичними взаємопов'язаними об'єктами, вбудованими датчиками, розумними пристроями, які з'єднуються та обмінюються даними з іншими пристроями та системами без втручання людини.

Друге, на що слід звернути увагу – це розуміння бізнес-вимог і цілей додатків, після чого можна рухатися далі з вибором типу бездротової мережі та технології протоколу IoT на основі наступних критеріїв:

- зона покриття;
- споживання енергії;
- щільність об'єктів;
- обсяг і характер даних;
- витрати;
- безпека;
- середовище пристрою.

Беручи до уваги вищезазначені критерії, які мають бути визначальними для обраного рішення, потрібно зосередитися на конкретному випадку використання. Розглянемо основні типи бездротових мереж, щоб допомогти оцінити кожну з них для прийняття рішень і вибору найкращого стеку технологій (рисунок 2.4).

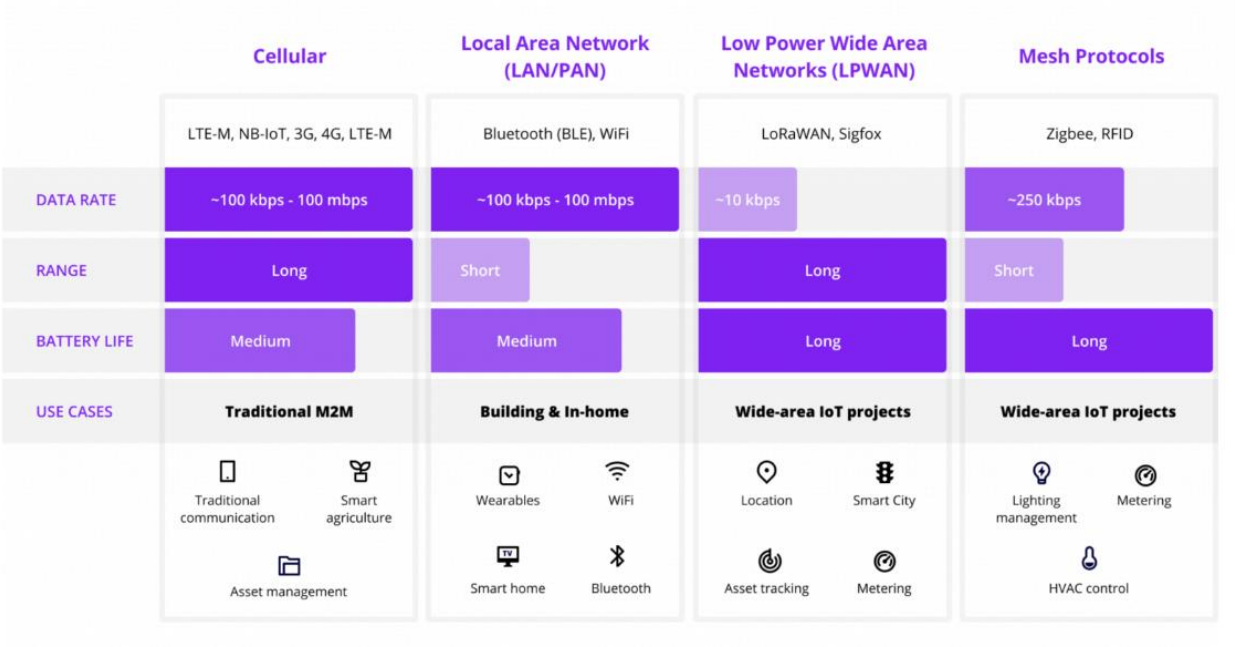


Рисунок 2.4 – Бездротові технології для IoT

LTE-M і NB-IoT належать до малопотужних глобальних мереж (low-power wide-area networks (LPWAN)) і можуть працювати в діапазоні 4G. Ці відкриті стандарти були запроваджені 3GPP (3rd Generation Partnership Project) і призначені для надійної, безпечної роботи з низьким енергоспоживанням, але вони відрізняються частотою, діапазоном, безпекою, вартістю та енергоспоживанням. Тим не менш, вони вважаються одними з найпопулярніших рішень для IoT, оскільки можуть охоплювати великі території.

Будучи надійним рішенням на споживчому ринку мобільних пристроїв, вони розвивалися, забезпечуючи надійне підключення до

Інтернету речей із високою пропускною здатністю. До 2026 року NB-IoT і LTE-M охоплять понад 60% з 3,6 мільярдів мережевих підключень LPWA.

LTE-M, також відомий як Cat-M1, є стандартом радіотехнології, який дозволяє повторно використовувати встановлені бази LTE і оптимізований для більш високої пропускної здатності та мобільних з'єднань, включаючи голос через мережу. Він вимагає більшої пропускної здатності та дорожчий, ніж NB-IoT, але підтримує високу щільність з'єднання та низьке енергоспоживання пристрою.

З іншого боку, стандарт LTE-M трохи дорожчий порівняно з NB-IoT, оскільки для нього потрібен шлюз.

Варіанти використання LTE-M: додатки для відстеження активів, носимих пристроїв, медицини, POS та додатків для домашньої безпеки.

NB-IoT, також відомий як Cat-NB1, є вузькосмуговим протоколом IoT, який потребує менших витрат і меншого споживання енергії акумулятора, однак він не використовує традиційний фізичний рівень LTE, а вже створені мобільні мережі. У порівнянні з LTE-M, він не підтримує повну мобільність, але також підтримує величезну кількість з'єднань. Він також забезпечує краще покриття в приміщеннях і під землею, ніж LTE-M.

NB-IoT дешевший, оскільки його пристрої мають довший час роботи від батареї та не потребують шлюзу (дані датчиків надсилаються безпосередньо на основний сервер).

Варіанти використання NB-IoT: управління активами, управління автопарком (логістика), розумне вимірювання, підключене землеробство та розумне обприскування, а також програми для розумного міста.

Локальні мережі та персональні мережі (Local area networks and personal area networks (LAN/PAN)) є економічно ефективними, однак передача даних обмежена через локальне середовище. WiFi і Bluetooth належать до цієї категорії і зазвичай використовуються для рішень підключення IoT.

Пристрої з підтримкою Bluetooth у поєднанні з іншими електронними пристроями передають дані в хмару завдяки низькому споживанню електроенергії. Можна побачити, що вони широко включені в медичні та фітнес-трекери, розумні домашні пристрої, дані з яких передаються на смартфони.

Ідеальним варіантом використання пристроїв BLE (Bluetooth-enabled devices (BLE)) є роздрібна торгівля. Вони використовуються для підвищення досвіду клієнтів у магазині та прийняття рішень про купівлю за допомогою цільового вмісту, що запускається маяками, на їхніх смартфонах (навігація в магазині, спеціальні пропозиції, знижки, події тощо, які надсилаються клієнтам у географічній близькості).

Варіанти використання Bluetooth: відстеження фізичної активності, маяки, пристрої домашньої автоматизації.

Через обмеження в охопленні, масштабованості та високому енергоспоживанні технологія Wi-Fi не настільки життєздатна для великих мереж сенсорів IoT, що працюють від акумуляторів. WiFi стосується програм, що працюють у локальному або розподіленому середовищі з кількома точками доступу, підключеними до розетки. Мережі WiFi можна застосовувати для:

– розумних домашніх гаджетів;
– цифрових підписів;
– камер спостереження.

Варіанти використання Wi-Fi: розумна будівля, відстеження стану здоров’я та фітнесу, маяки в магазинах.

Глобальні мережі з низьким енергоспоживанням (Low Power Wide Area Networks (LPWAN)) – це новий набір бездротових протоколів, які можуть буквально з’єднувати всі типи датчиків IoT і сприяти створенню численних програм, спеціально створених для підтримки широкомасштабних проектів IoT. Ці мережі можуть використовуватися пристроями для

спілкування на великих територіях за допомогою маленьких недорогих акумуляторів з низьким енергоспоживанням. У порівнянні зі стільниковими мережами LPWAN є економічно ефективним і довгостроковим рішенням.

Здається, що LPWAN є однією з найкращих мереж; однак, оскільки кожна мережа має свої плюси та мінуси, недоліком LPWAN є невеликі обсяги даних, які вона може надіслати в одному екземплярі, тому вона може добре підходити для випадків використання без високої пропускної здатності.

Враховуючи різні цілі, існують ліцензовані (NB-IoT, LTE-M) і неліцензійні (LoRa, Sigfox) типи LPWAN. Основною проблемою для ліцензованої LPWAN є енергоспоживання; Якість обслуговування та масштабованість належать до основних питань при впровадженні неліцензійних технологій.

З точки зору діапазону, можливості Sigfox включають Wi-Fi і стільниковий зв’язок. Sigfox не потребує отримання ліцензій через діапазони частот ISM (Industrial, scientific, and medical), які вони використовують (промислові, наукові та медичні).

Використовуючи технологію UNB (Ultra Narrow Band), основна увага Sigfox полягає в тому, щоб керувати низькою швидкістю передачі даних із надзвичайно низьким споживанням енергії, а також ця мережа здатна спілкуватися з мільйонами пристроїв, що працюють від акумуляторів, на відстані 30-50 кілометрів.

Варіанти використання Sigfox: розумні будівлі та міста: моніторинг води, моніторинг використання людей, моніторинг віддалених активів.

Розроблений для великих публічних мереж, покриття LoRaWAN становить до 15 км. Завдяки функції розширеного діапазону LoRaWAN є чудовим рішенням для галасливих промислових установок, що підтримує мільйони пристроїв. Низьке енергоспоживання LoRaWAN добре підходить

для пристроїв IoT з батарейним живленням, які підтримують їх протягом 10 років.

Варіанти використання LoRaWAN: дистанційний моніторинг і відстеження стану активів (температура, вібрація, тиск), розумні міста, розумне освітлення.

Завдяки ємності малого радіусу дії протоколи Mesh є чудовими рішеннями для IoT-проектів середнього рівня з передачею даних у безпосередній близькості. У сітчастих мережах зв’язок між сенсорними вузлами здійснюється розподіленим способом, щоб досягти місця втечі, що є контрастним підходом до передачі даних до центрального концентратора.

Меш-протоколи є надійними та популярними рішеннями для використання в будівлях і на вулицях, як-от інтелектуальна автоматизація будівель (розумне освітлення, HVAC операції, безпека та керування енергією тощо), вуличне освітлення.

Zigbee є одним із найвідоміших mesh-протоколів, які використовуються в програмах IoT. У порівнянні з LPWAN, Zigbee забезпечує більшу передачу даних із набагато меншою енергоефективністю завдяки своїй конфігурації підключення. Завдяки недорогим і малопотужним рішенням Zigbee програмами можна керувати за допомогою недорогих батарей протягом десяти років.

Взаємозв’язок мережі Zigbee дозволяє підключати кожен пристрій до сигналу, який передає його іншим пристроям через сітчасту мережу. Ризик збою сигналу в одній точці виключається завдяки здатності пристроїв Zigbee розширювати шляхи зв’язку, що сприяє сумісності та безперебійному з’єднанню з різними постачальниками.

Ще одна відмінна риса цього протоколу полягає в тому, що він доступний для неліцензійного використання в усьому світі.

Варіанти використання Zigbee: автоматичне зчитування лічильників, моніторинг резервуарів, інтелектуальне керування HVAC, керування медичними пристроями, керування освітленням.

Протокол RFID (радіочастотна ідентифікація) здебільшого використовується для відстеження активів. Через бездротові мікрочіпи, вбудовані в пристрої IoT, трансивери надсилають і приймають радіохвилі, щоб передавати невеликі обсяги даних у невеликих областях без прямої видимості. Діючи як точка доступу, зчитувачі RFID можуть отримувати та надсилати повідомлення на трансивери.

За допомогою чіпів RFID роздрібні продавці мають право покращити планування закупівель, оптимізувати транспортну логістику та отримати наскрізну видимість даних у всій екосистемі ланцюга поставок.

Варіанти використання RFID: відстеження автопарку та активів, автоматизована перевірка, моніторинг ліків, управління ланцюгом постачання, управління складом, електронний паспорт, людські імплантати, безпека контролю доступу, платежі.

Форма використання відіграє вирішальну роль у виборі відповідної мережі IoT для програми IoT. Отже, давайте розглянемо найважливіші критерії вибору технологій мереж для IoT:

Споживання енергії. Якщо потрібно довговічність і рішення без необхідності живлення пристрою, Bluetooth і LPWAN – це підходящі мережі для цього випадку. Технології з високим енергоспоживанням, такі як Wi-Fi, не рекомендуються.

Зона покриття. Розмір області, яку необхідно охопити, визначає тип протоколу, який буде застосовано для проекту IoT. У той час як LoRA обмежена національними кордонами, мережа Sigfox доступна в 60 країнах.

Обсяг даних. Якщо потрібно передати невелику кількість даних, існують такі рішення, як BLE на короткій відстані або LPWAN для передачі

даних на великі відстані. Для великих обсягів даних рекомендовано мережі Wi-Fi та GSM.

Щільність пристроїв. Вибір відповідного протоколу IoT залежить від потреби в географічній близькості чи від потреби з'єднання на великих віддалях. Якщо об'єкти потрібно з'єднати і вони знаходяться недалеко один до одного, хорошим варіантом буде WiFi; у випадку великих дистанцій рекомендуються мережі LPWAN і GSM.

На ринку існує різноманітність доступних варіантів мережі IoT. Ідеальне уніфіковане рішення для підключення підтримуватиме низьке енергоспоживання разом із можливістю передачі величезних обсягів даних на великі відстані, забезпечуючи високий рівень безпеки та низькі витрати.

Однак, не існує універсального рішення, яке б залишалося економічно життєздатним для всіх розумних підприємств; кожен варіант використання визначає критерії для вибору мережі IoT: пропускна здатність, діапазон, енергоспоживання. Таким чином, розуміння особливостей варіанту використання та визначення вимог до проекту IoT на кожному етапі розробки допоможе прийняти рішення щодо вибору мережевого протоколу IoT, який найкраще підходить для проекту.

2.7 Дослідження приватних 5G мереж для IoT

Приватний 5G із 5G New Radio забезпечує пріоритетний доступ на основі якості обслуговування порівняно з загальнодоступною мережею 5G. Це має величезний потенціал для цифрової трансформації організацій у промисловості, охороні здоров'я, роздрібній торгівлі, розумних містах, залізниці, транспорті, портах, гірничодобувній та енергетичній галузях, забезпечуючи безпечну, надійну, високошвидкісну мережу з низькою затримкою.

Приватна 5G – це виділена незалежна приватна мережа, розгорнута та керована на території організації, або може бути частиною публічно розгорнутої 5G із підтримкою QoS, або комбінацією локальних і зовнішніх мереж.

Залежно від варіанту використання спектр 5G може бути ліцензованим, обмежено ліцензованим або неліцензійним. Для приватних мереж 5G у США приватні спектри, такі як Citizens Broadband Radio Service, дозволяють компаніям будувати власні приватні мережі 5G.

Приватний 5G навряд чи замінить Wi-Fi. Але приватний 5G може забезпечити детерміновані варіанти використання в режимі реального часу, які раніше були неможливі через відсутність надійності, детермінізму, низьку затримку та високу швидкість, особливо для випадків використання Інтернету речей і периферійних обчислень.

Покращений мобільний широкосмуговий зв’язок, наднадійний зв’язок із низькою затримкою (Ultra Reliable Low Latency Communications (URLLC)) і потужні функції зв’язку машинного типу 5G відкривають широкий спектр варіантів використання.

URLLC із 5G Release 16 пропонує чутливу до часу мережу (time-sensitive networking (TSN)), яка забезпечує надійний Інтернет речей із низькою затримкою в промисловій автоматизації та таких галузях, як охорона здоров’я та логістика. Інші функції, такі як обслуговування, оркестровка політики, управління та корпоративна інтеграція, також забезпечують переваги даної технології.

Для того, щоб будь-яка проривна технологія отримала широке розгортання, простота розгортання, управління та пов’язані з цим витрати стають критичними факторами. І саме тут приватне розгортання керованої мережі 5G може змінити правила гри.

Складність розгортання приватної мережі 5G для підприємств значно зменшилася, особливо завдяки пропозиціям постачальників, які допомагають

планувати, розгортати та керувати приватними мережами 5G на території. Ці постачальники надають точки доступу, ядро 5G, керування SIM-картою та загальну оркестровку та керування системою. Деякі постачальники також пропонують приватний 5G як керовану послугу.

Порівняно з корпоративним розгортанням Wi-Fi, необхідна кількість обладнання, програмного забезпечення, ліцензій і кабелів може істотно зменшитися з приватним розгортанням 5G, з додатковою перевагою детермінованої продуктивності та низькою затримкою, меншим співвідношенням потужності до покриття і високою швидкістю.

Спостерігається раннє розгортання приватних мереж 5G. У квітні 2021 року Verizon оголосила про своє перше європейське розгортання приватної мережі 5G разом з Nokia для асоційованих британських портів (ABP) у порту Саутгемптона, одному з найбільш завантажених портів Великобританії, який щороку експортує з Великобританії промислових товарів на суму 40 мільярдів фунтів стерлінгів.

Іспанська транспортна інфраструктурна компанія Ferrovial запустила одну з перших у світі приватних автономних (SA) мереж 5G у жовтні 2021 року для підтримки низки варіантів використання на місці будівництва тунелю під річкою Темза.

Окрім технічних можливостей приватного 5G перед іншими альтернативами, однією з головних переваг приватного 5G є допомога в консолідації ряду комунікаційних рішень або інтерфейсів, розгорнутих на промисловому майданчику. Йдеться про можливість підтримувати кілька варіантів використання в одній мережі замість того, щоб керувати кількома різними рішеннями, кожне з яких часто пов’язане з одним варіантом використання, що призводить до більшої складності та вартості володіння.

Крім того, розширені можливості приватної мережі 5G, зокрема її надійність, пропускна спроможність, безпека та наднизька затримка, можуть уможливити нові варіанти використання та додатки, такі як командування та

контроль у реальному часі, аналітика, масовий Інтернет речей та машинний інтелект. Ці можливості, у свою чергу, можуть підготувати промислові майданчики до нових додатків із підтримкою 5G, які зможуть цифрово трансформувати їхню діяльність у майбутньому, наприклад, прогнозне технічне обслуговування, автономні мобільні роботи та відстеження активів.

Одним з варіантів використання приватних мереж 5G може бути розширене прогнозне обслуговування. Незапланований простій у виробництві коштує грошей (нижча продуктивність), але також є неефективним і запланований простій, який виконується “про всяк випадок”, тому що зупиняє роботу машин.

Йдеться про перехід від “профілактичного” до “прогнозного” технічного обслуговування та можливості виконувати завдання технічного обслуговування за потреби, а не за фіксованим графіком, що потенційно скорочує заплановані простої та запобігає майбутнім поломкам.

Розширене прогностичне технічне обслуговування використовує машинний інтелект на основі даних датчиків Інтернету речей, щоб визначити ймовірність відмови обладнання, і обслуговує лише машини, які потребують втручання.

Згідно з дослідженням 2018 року, прогнозне технічне обслуговування може збільшити вартість у 140 мільярдів доларів у всьому світі за рахунок підвищення продуктивності та економії витрат у виробничому секторі.

Прогнозне технічне обслуговування вимагає надійного та швидкого збору великих обсягів даних з датчиків, аналізу та реагування протягом мілісекунд, щоб запобігти несправності. 5G дозволяє централізувати алгоритми прогностичного керування в периферійній хмарі, а не в спеціальному, суміжному обладнанні.

Прогнозне технічне обслуговування – це рішення, яке використовувалося у виробничих налаштуваннях до приватного 5G, спочатку на приватному LTE. У міру того як підключається все більше і більше машин

і активів, приватний 5G може підтримувати щільність пристроїв із меншою затримкою в масштабі, більше, ніж приватний LTE.

Прикладом перспективнсості використання такого рішення може бути Telefónica Tech (підрозділ цифрових послуг Telefónica), що нещодавно підписала угоду з Grupo Álava, компанією з інженерних послуг в Іспанії, про запуск рішення для прогнозованого обслуговування для індустрії 4.0, яке працює в приватній мережі 5G.

Іншим варіантом застосування приватних мереж 5G можуть бути автономні мобільні роботи. Її використання підвищує ефективність, надійність і точність транспортування і переміщення деталей і матеріалів; знижує трудовитрати, підвищує безпеку робочого місця та гнучкість цеху.

Виникає більша гнучкість у переході від фіксованих маршрутів, тобто заздалегідь спланованих маршрутів або доріжок, які проходять до цеху, або тих, які використовують Wi-Fi, до більш інтелектуальної навігації для уникнення перешкод.

Краще підходить для більш гнучкого виробництва, де можна легко повторно розгорнути Autonomous mobile robots (AMR) у разі будь-яких модифікацій продуктів або виробничої лінії

AMR вимагає високої пропускної здатності, якою володіє приватна мережа 5G, щоб використовувати вбудовані датчики та навігаційні інструменти (наприклад, камери, сканери) для навігації по об’єкту за найефективнішим маршрутом, який він визначає.

Їм також потрібна менша затримка, щоб реагувати на перешкоди чи небезпеки на своєму маршруті

Коли використовуються AMR, що переміщуються великими дистанціями на території або, наприклад, із приміщення назовні через будівлі, приватний 5G має перевагу перед Wi-Fi, враховуючи переваги з точки зору мобільності та покриття (менше точок доступу, краще покриття як у приміщенні так і на природі).

Було проведено низку випробувань AMR у приватних мережах 5G, у тому числі Nokia, яка випробувала рішення AMR для покращення автоматизації матеріальних потоків на своїй “фабриці майбутнього” в Оулу, Фінляндія.

Недавнє розгортання відбулося на виробничому заводі в Таїланді, що належить компанії Yawata Eloctrode, де AMR працюють на приватній мережевій платформі 5G AIS.

Ще одним варіантом застосування може бути управління запасами в реальному часі. Використання цього рішення відстежує та контролює положення та використання активів у режимі реального часу, підвищує видимість з більшою точністю, щоб краще керувати активами протягом їх життєвого циклу. Автоматизує керування запасами, щоб запобігти будь-яким можливим затримкам з деталями чи матеріалами, необхідними для виробництва.

На виробничих підприємствах є багато елементів, які потребують моніторингу, і для кожного з них потрібен датчик. Така велика кількість датчиків, які відстежуються в режимі реального часу, займає велику пропускну здатність, з якою може впоратися тільки приватний 5G. Вища надійність, яку забезпечує приватна мережа 5G, також важлива для того, щоб речі не загубилися

На великих територіях, коли елементи переміщуються на відносно великі відстані, розширене покриття також є перевагою перед Wi-Fi, оскільки елементи не будуть втрачені під час переміщення з одного маршрутизатора на інший.

Наприклад, ADLINK має інтелектуальне складське рішення, яке може контролювати положення та статус піддонів. Це стало можливим, тому що їх крайове обладнання добре сумісне з 5G.

2.8 Висновки до другого розділу

Другий розділ кваліфікаційної роботи присвячений дослідженню впливу цифрової трансформації виробництва в умовах пандемії COVID-19. Виявлено, що впровадження IT технологій дало змогу продовжити роботу, створити безпечні умови праці на місцях та надати віддалений доступ до робочого місця. Проведено дослідження впливу промислового інтернету речей IIoT на роботу промисловості, що показало покращення якості продукції, скорочення часу простоїв, підвищення автоматизації на заводах, оптимізації процесів, створення розумного виробництва та контролю продуктивності. Здійснено дослідження відмінностей між IoT та IIoT, в результаті якого отримано висновок, що IIoT – це мережа інтелектуальних пристроїв, які відстежують, збирають і аналізують дані в промислових екосистемах. Подано архітектуру IIoT, що може бути використана для створення систем з прогнозним обслуговуванням, обслуговуванням на місцях, відстеженням активів для покращення управління об’єктами. Виявлено, що найбільші ризики для впровадження IIoT пов’язані з безпекою використання. Для задоволення ризиків безпеки потрібно захищати віддалений доступ до IoT пристроїв, а також до сховищ даних і каналів зв’язку. Проведено дослідження бездротових технологій, як основи роботи IoT технології. Виявлено ряд рішень, що відрізняються параметрами зони покриття, споживання енергії, щільності об’єктів, обсягом та храктером даних, які передаються, витратами на встановлення та обслуговування, безпекою. Як частковий випадок організації надійної та захищеної, високопродуктивної бездротової технології для IIoT, досліджено приватні 5G мережі. Рішення щодо їх впровадження мають базуватись на доступності технології в країні, необхідністю використання ліцензованого чи обмежено ліцензованого частостного простору.

3 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

3.1 Охорона праці

3.1.1 Безпечні умови праці при монтажі комп'ютерної мережі

Законодавчими актами, що визначають основні положення про охорону праці є загальні закони України, а також спеціальні законодавчі акти. До загальних законів належать: Конституція України, Закони України: "Про охорону праці", "Про охорону здоров'я", "Про пожежну безпеку".

Приміщення, в яких встановлені персональні комп'ютери, повинні мати природне та штучне освітлення відповідно до ДБН В.2.5-28-2006 [55].

Згідно з ДСанПіН 3.3.2-007-98 [56] та з Правилами охорони праці під час експлуатації ЕОМ НПАОП 0.00-1.28-10 [57] площа на одне робоче місце має становити не менше ніж 6,0 кв. м, а об'єм – не менше ніж 20,0 куб. м

До початку робіт у комплексній бригаді проводиться первинний інструктаж з безпечного виконання робіт з основної та суміжних професій та ознайомлення з правилами надання першої допомоги.

Особи з простудними і хронічними захворюваннями верхніх дихальних шляхів до роботи з монтажу комп'ютерних мережі та заготовки і монтажу пластмасових труб не допускаються.

Згідно ДНАОП 0.00-1.15-07 [58]. Правила охорони праці під час виконання робіт на висоті (при підйомі над поверхнею вище, ніж 1,3 м) виконуються тільки з риштувань або помостів. До виконання робіт на висоті допускаються особи, не молодше 18 років, та які пройшли:

– професійний добір відповідно до Переліку робіт, де є потреба у професійному доборі, затвердженого спільним наказом Міністерства охорони здоров'я України та Державного комітету України з нагляду за охороною праці від 23.09.94 N 263/121, зареєстрованого в Міністерстві юстиції України 25.01.95 за N 18/554;

– медичний огляд відповідно до вимог Положення про медичний огляд працівників певних категорій, затвердженого наказом Міністерства охорони здоров'я України від 31.03.94 N 45, зареєстрованого в Міністерстві юстиції України 21.06.94 за N 136/345;

– спеціальне навчання та перевірку знань з охорони праці відповідно до вимог Типового положення про порядок проведення навчання і перевірки знань з питань охорони праці, затвердженого наказом Державного комітету України з нагляду за охороною праці від 26.01.2005 N 15, зареєстрованого в Міністерстві юстиції України 15.02.2005 за N 231/10511 (далі - НПАОП 0.00-4.36-05 [59]).

Вимоги безпеки перед початком роботи передбачають, що до початку робіт з монтажу комп’ютерної мережі керівник зобов’язаний:

– перевірити ступінь готовності будівельних робіт;

– оцінити виробничі обставини, можливість взаємодії з іншими будівельно-монтажними організаціями у відповідності з проектом виконання робіт (ПВР); можливість безпечного застосування машин, механізмів, пристосувань, місця їх установки та порядок проїзду; можливість безпечного застосування піротехнічного інструменту, безпечної подачі електричних конструкцій, електротехнічних апаратів та інших блоків;

– узгодити з відповідними службами та, при необхідності, внести уточнення в ПВР.

– ознайомити працюючих з ПВР та технологічними картами на всі види робіт.

Керівник робіт повинен здійснити первинний інструктаж, який стосується:

– характеру та безпечних методів виконання робіт (у т.ч. за складних погодних умов); порядку проходів до кожного робочого місця;

– наявності небезпечних зон та відкритих каналів і траншей, відкритих прорізів, отворів у перекриттях та стінах;

– порядку розвантаження та складування матеріалів, устаткування та конструкцій;

– місць та порядку трансформаторів безпеки, електрифікованого інструменту, засобів електроосвітлення, випробувальних апаратів;

– порядку і місця установки вантажних лебідок та інших механізмів у монтажній зоні; порядку роботи з гідропідйомників, риштувань, підмостків, драбин; наявності діючих електроустановок та заборонених зон;

– надання першої допомоги, виклику швидкої медичної допомоги, пожежної охорони, керівника робіт чи роботодавця, представника служби охорони праці.

Перевірити наявність та термін дії посвідчень з охорони праці, електро-пожежобезпеки, посвідчень на право виконання спеціальних видів робіт (зварювання, монтаж кабельної арматури).

Видати наряд-допуск операторам на виконання робіт підвищеної небезпеки з проведенням цільового інструктажу та записом до журналу реєстрації інструктажів з питань охорони праці. Підписи інструкторів та інструктованих у журналі обов’язкові.

Попередити працюючих, що з’єднання та від’єднання від мережі обладнання, механізмів, інструменту, інвентарних шаф тощо (крім оперативного вмикання і вимикання) в умовах будівельного майданчика виконуються тільки службою експлуатації власника мережі, якщо не існує іншої письмової домовленості з власником.

Вимоги безпеки під час виконання роботи:

– прокладання кабелів слід виконувати тільки в рукавицях.

– працювати ручними ударними інструментами слід із застосуванням захисних щитків або окулярів з непробивним склом.

– переносити чи перевозити інструмент з гострими кутами треба лише в чохлах.

– не дозволяється розміщувати кабель, барабан з кабелем та без нього, механізми, пристрої та інструменти безпосередньо біля бровки траншеї.

– перекочувати барабан з кабелем слід у напрямку стрілки, нанесеної фарбою на щоці барабана.

– переміщувати барабан з кабелем вручну дозволяється тільки по твердому ґрунту або надійному настилу по горизонтальній поверхні на відстань не більше .

Не дозволяється працюючим чи стороннім особам перебувати на шляху барабана, що переміщується. Під час піднімання барабана необхідно слідкувати за тим, щоб не пошкодити щоки барабана та втулку. Перед розмотуванням барабан встановити на домкрати (чи інший підіймальний пристрій). Барабан встановити так, щоб кабель розмотувався з його верхньої частини. Розмотувати кабель з барабана слід тільки за наявності гальмівного пристрою.

Прокладання кабелів і монтаж мережевого обладнання слід виконувати у захисному одязі з можливістю використання електростатичних браслетів.

Згідно ДБН В.2.5-23:2010 [60]. Проектування електрообладнання об'єктів цивільного призначення установлена потужність робочого місця локальної обчислювальної мережі (ЛОМ) (без врахування периферійних пристроїв) приймається 250...300 Вт, сервера – 750... 1000 Вт або згідно з технічною документацією на ці електронні пристрої ЛОМ.

Граничні значення X електронних пристроїв різної потужності для закордонних виробників обмежується стандартом EN 61000-3-2, для більшості випадків значення можливо приймати 0,72.

Усі об’єкти ЛОМ мають як активну, так і реактивну складові навантаження, тобто повна потужність у вольт-амперах (ВА, англ. «VA») і активна потужність у ватах (Вт, англ. «W») зв’язані між собою коефіцієнтом cos φ. На приладах (блоці живлення комп’ютера) вказують їхню активну

споживану потужність у ватах. Щоб підрахувати повну потужність у ВА, потрібно активну потужність у Вт розділити на cos φ. Наприклад, якщо на блоці живлення комп'ютера написано «850 Вт» (cos φ зазвичай не вказаний), це означає, що для грубого розрахунку повної потужності, яка споживається насправді, можна активну потужність розділити на 0,7. Споживана повна потужність дорівнюватиме 850 Вт/0,7 ≈ 1200 ВА = 1,2 кВА. Необхідно визначити суму потужностей усіх споживачів, що мають потребу в одночасному постачанні електроенергії.

При проектуванні електрообладнання будинків та споруд слід також керуватись вимогами відповідних розділів правила улаштування електроустановок (ПУЕ), розділів 2, 3, 4.1, 4.2, 9 [61], та нормативно-правових актів охорони праці (НПАОП) 40.1-1.32 [62] та вимогами інших чинних нормативних документів.

Не можна застосовувати провід і кабель в ізоляції з вулканізованої гуми та інші матеріали, які містять сірку. У всіх приміщеннях із серверами та робочими місцями, обладнаними ЕОМ, повинні бути встановлені переносні вуглекислотні вогнегасники. Використання води для гасіння пожежі в приміщеннях, де встановлено електро- і радіоелектронне обладнання, недопустиме, не можна також користуватись і кислотно-лужними вогнегасниками. У громадських будинках та приміщеннях з наявністю ПЕОМ, приміщеннях обчислювальних центрів рекомендується використовувати вуглекислотні вогнегасники типу ОУ-5, ОУ-8, ОУ-25, ОУ-80, вуглекислотні бром-етилові вогнегасники типу ОУБ-3 і ОУБ-7, вуглекислотні вогнегасники від ВВК-1 до ВВК-5, які придатні до експлуатації при температурі повітря від мінус 20 до плюс 50°С.

Кількість вогнегасників для захисту приміщень визначають згідно з п. 3.8 норм належності, затверджених МНС України, та з урахуванням сумарної площі цих приміщень. Тобто слід передбачати по одному вуглекислотному вогнегаснику з величиною заряду вогнегасної речовини 3 кг і більше на

кожні 20 кв. м площі підлоги в офісних приміщеннях із ПЕОМ та електрощитових і на 50 кв. м площі підлоги приміщень машзалів.

Приміщення, в яких розміщуються робочі місця операторів сервера загального призначення, обладнуються системою автоматичної пожежної сигналізації та засобами пожежогасіння відповідно до вимог НАПБ Б.06.004-2005, ДБН В.2.5-56:2010 [63]. Установки порошкового пожежогасіння не застосовують для захисту приміщень із ЕОМ, апаратних залів АТС та інших приміщень із великою кількістю відкритих контактних пристроїв.

У приміщенні, де одночасно експлуатуються понад п’ять ЕОМ з ВДТ і ПП, на доступному місці встановлюється аварійний резервний вимикач, який може повністю вимкнути електричне живлення приміщення, крім освітлення. Електромережі штепсельних з’єднань та електророзеток для живлення ЕОМ з ВДТ і ПП потрібно будувати за магістральною схемою, по 3 – 6 з’єднань або електророзеток в одному колі.

3.2 Безпека в надзвичайних ситуаціях

3.2.1 Ультразвук та інфразвук, його вплив на організм людини

Ультразвук являє собою механічні коливання пружного середовища, що мають однакову зі звуком фізичну природу, але відрізняються більш високою частотою, що перевищує прийняту верхню межу чутності - понад 20 кГц, хоча при великих інтенсивностях (120 ... 145 дБ) чутними можуть бути і звуки більш високої частоти.

Ультразвук, як і звук, характеризується ультразвуковим тиском (Па), інтенсивністю (Вт/м2) і частотою коливань (Гц).

При поширенні в різних середовищах ультразвукові хвилі поглинаються, причому тим більше, чим вище їх частота. Низькочастотний ультразвук досить добре розповсюджується в повітрі, а високочастотний - практично не поширюється. У пружних середовищах (воді, металі та ін)

ультразвук мало поглинається і здатний поширюватися на великі відстані, практично не втрачаючи енергії. Поглинання ультразвуку супроводжується нагріванням середовища.

Специфічною особливістю ультразвуку, обумовлене великою частотою і малою довжиною хвилі, є можливість поширення ультразвукових коливань спрямованими пучками, які отримали назву ультразвукових променів. Вони створюють на відносно невеликій площі дуже велике ультразвукове тиск. Це властивість ультразвуку зумовило широке його застосування: для очищення деталей, механічної обробки твердих матеріалів, зварювання, пайки, прискорення хімічних реакцій, дефектоскопії, перевірки розмірів виробів, що випускаються, структурного аналізу речовин, гідролокації та ін Знайшов застосування ультразвук і в медицині для лікування захворювань хребта, суглобів, периферичної нервової системи.

При тривалій роботі з низькочастотними ультразвуковими установками, що генерують шум і ультразвук, що перевищують встановлені, можуть відбутися функціональні зміни центральної і периферичної нервової системи, серцево-судинної системи, слухового і вестибулярного апарату і т. п. У порівнянні з високочастотним шумом ультразвук значно слабше впливає на слухову функцію, але викликає більш виражені відхилення від норми вестибулярної функції, больової чутливості і терморегуляції. Те, що ультразвук впливає на різні органи і системи людини не тільки через слуховий апарат, підтверджується несприятливим його дією на глухонімих.

Для колективного захисту від дії підвищених рівнів ультразвуку можна використовувати такі напрями: зменшення шкідливого випромінювання ультразвукової енергії в джерелі її виникнення; локалізацію дії ультразвуку конструктивними і планувальними рішеннями, проведення організаційно-профілактичних заходів.

Для зменшення шкідливого випромінювання звукової енергії в джерелі рекомендується підвищувати робочі частоти джерел ультразвуку, що

забезпечує зменшення інтенсивності ультразвуку, а також виключати паразитні випромінювання звукової енергії.

Для локалізації ультразвуку обов'язковим є застосування звукоізолюючих кожухів, екранів. Якщо ці заходи не дають позитивного ефекту, то ультразвукові установки потрібно розміщувати в окремих приміщеннях і кабінах, облицьованих звукопоглинальними матеріалами.

Контактний вплив ультразвуку виключається автоматизацією виробничих процесів і застосуванням дистанційного управління. При особливої необхідності використовують спеціальний інструмент з віброізолюючий рукояткою і захисні рукавички.

Організаційно-профілактичні заходи полягають у проведенні інструктажу працюючих та встановлення раціональних режимів праці та відпочинку.

Інфразвук являє собою механічні коливання пружного середовища, що мають однакову з шумом фізичну природу, але поширюються з частотами менше 20 Гц. У повітрі інфразвук мало поглинається і тому здатний поширюватися на великі відстані. Інфразвук характеризується інфразвукових тиском (Па), інтенсивністю (Вт/м2), частотою коливань (Гц). Рівні інтенсивності інфразвуку і інфразвукового тиску виражаються в децибелах (дБ). Багато явищ природи (землетруси, виверження вулканів, морські бурі) супроводжуються випромінюванням інфразвукових коливань. У виробничих умовах інфразвук утворюється, головним чином, при роботі тихохідних великогабаритних машин і механізмів (компресорів, дизельних двигунів, електровозів, вентиляторів, турбін, реактивних двигунів і ін), які роблять обертальний або зворотно-поступальний рух з повторенням циклу менше ніж 20 разів на секунду (інфразвук механічного походження). Інфразвук аеродинамічного походження виникає при турбулентних процесах у потоках газів чи рідин.

Інфразвук справляє негативний вплив на весь організм людини, в тому числі і на орган слуху, знижуючи слухову чутливість на всіх частотах. Інфразвукові коливання сприймаються як фізичне навантаження: виникають стомлення, головний біль, запаморочення, вестибулярні порушення, знижується гострота зору і слуху, порушується периферичний кровообіг, з'являється відчуття страху і т. п. Тяжкість впливу залежить від діапазону частот, рівня звукового тиску і тривалості.

Низькочастотні коливання з рівнем інфразвукового тиску понад 150 дБ зовсім не переносяться людиною. Особливо несприятливі наслідки викликають інфразвукові коливання з частотою 2 ... 15 Гц у зв'язку з виникненням резонансних явищ в організмі людини, причому найбільш небезпечна частота 7 Гц, так як можливо його збіг з альфа-ритмом біострумів мозку.

Згідно з СН 22-74 - 80 рівні інфразвукового тиску в октавних смугах з середньогеометричними частотами 2, 4, 8 і 16 Гц не повинні перевищувати 105 дБ, а в смузі з частотою 32 Гц-102 дБ. Боротьба з несприятливим впливом інфразвуку повинна вестися в тих же напрямках, що і боротьба з шумом. Найбільш доцільно зменшувати інтенсивність інфразвукових коливань на стадії проектування машин або агрегатів.

3.3 Висновки до третього розділу

В даному розділі кваліфікаційної роботи розглянуто питання безпечних умов праці при монтажі комп’ютерної мережі. В безпеці в надзвичайних ситуаціях висвітлено питання ультразвуку та інфразвуку і їх вплив на організ людини.

ВИСНОВКИ

За результатами виконання кваліфікаційної роботи здійснено дослідження ролі IoT-технологій в промислових комп'ютерних мережах. Отримано наступні основні результати виконання роботи:

– наведено переваги Індустрії 4.0, що показують важливість використання новітніх технологій для створення швидшого, продуктивнішого, надійнішого, адаптивнішого та безпечнішого середовища у промисловості;

– розглянуто поняття кіберфізичних систем і подано визначення цього феномену разом з використанням IoT в ньому. Визначено, що кіберфізичні системи та IoT є нерозривно зв'язані та доповнюють один одного;

– досліджено вплив цифрової трансформації виробництва в умовах пандемії COVID-19. Виявлено, що впровадження IT технологій дало змогу продовжити роботу, створити безпечні умови праці намісцях та надати віддалений доступ до робочого місця;

– проведено дослідження впливу промислового інтернету речей IIoT на роботу промисловості, що показало покращення якості продукції, скорочення часу простоїв, підвищення автоматизації на заводах, оптимізації процесів, створення розумного виробництва та контролю продуктивності;

– здійснено дослідження відмінностей між IoT та IIoT, в результаті якого отримано висновок, що IIoT – це мережа інтелектуальних пристроїв, які відстежують, збирають і аналізують дані в промислових екосистемах;

– подано архітектуру IIoT, що може бути використана для створення систем з прогнозним обслуговуванням, обслуговуванням на місцях, відстеженням активів для покращення управління об'єктами;

– виявлено, що найбільші ризики для впровадження IIoT пов'язані з безпекою використання. Для задоволення ризиків безпеки потрібно

захищати віддалений доступ до IoT пристроїв, а також до сховищ даних і каналів зв’язку;

– проведено дослідження бездротових технологій, як основи роботи IoT технології. Виявлено ряд рішень, що відрізняються параметрами зони покриття, споживання енергії, щільності об’єктів, обсягом та храктером даних, які передаються, витратами на встановлення та обслуговування, безпекою;

– як частковий випадок організації надійної та захищеної, високопродуктивної бездротової технології для IIoT, досліджено приватні 5G мережі. Рішення щодо їх впровадження мають базуватись на доступності технології в країні, необхідністю використання ліцензованого чи обмежено ліцензованого частостного простору.

В розділі «Охорона праці та безпека в надзвичайних ситуаціях» розглянуто питання безпечних умов праці при монтажі комп’ютерної мережі та ультразвуку і інфразвуку, їх вплив на організм людини.

СПИСОК ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. Enabling Technologies for Industry 5.0 [Електронний ресурс]. – Режим доступу: https://research-and-innovation.ec.europa.eu/knowledge-publications-tools-and-data/publications/all-publications/enabling-technologies-industry-50_en – Назва з екрану. – Дата звернення: 4.11.2022.

2. Industry 5.0 – Towards a sustainable, human-centric and resilient European inustry [Електронний ресурс]. – Режим доступу: https://research-and-innovation.ec.europa.eu/knowledge-publications-tools-and-data/publications/all-publications/industry-50-towards-sustainable-human-centric-and-resilient-european-industry_en – Назва з екрану. – Дата звернення: 4.11.2022.

3. Industry 5.0, a transformative vision for Europe [Електронний ресурс]. – Режим доступу: https://research-and-innovation.ec.europa.eu/knowledge-publications-tools-and-data/publications/all-publications/industry-50-transformative-vision-europe_en – Назва з екрану. – Дата звернення: 5.11.2022.

4. A. D wankhade and P. N. Dr Chatur, “Comparison of Firewall and Intrusion Detection System,” Int. J. Comput. Sci. Inf. Technol., vol. 5, no. 1, pp. 674–678, 2014, URL: http://ijcsit.com/docs/Volume 5/vol5issue01/ijcsit20140501145.pdf/.

5. T. King et al., “BLACKHOLE Community,” Internet Engineering Task Force (IETF), 2016. [Електронний ресурс]. – Режим доступу: https://tools.ietf.org/html/rfc7999. – Назва з екрану. – Дата звернення: 5.11.2022.

6. D. S. Ms. Charjan, P. S. Ms. Bochare, and Y. R. Bhuyar, “An Overview of Secure Sockets Layer,” Int. J. Comput. Sci. Appl., vol. 6, no. 2, pp. 388–393, 2013

7. Industry 5.0 [Електронний ресурс]. – Режим доступу: https://research-and-innovation.ec.europa.eu/research-area/industrial-research-and-innovation/industry-50_en – Назва з екрану. – Дата звернення: 10.11.2022

8. M. Kozlova (AKA M. Kozlova, “7 luchshikh servisov zashchity ot DDoS-atak dlya povysheniya bezopasnosti [The 7 best services of protecting from DDoS- attacks for the increase of safety],” HOSTING.cafe, 2017. [Електронний ресурс]. – Режим доступу: https://habrahabr.ru/company/hosting-cafe/blog/324848/. – Назва з екрану. – Дата звернення: 10.11.2022

9. Industry 4.0 [Електронний ресурс] – Режим доступу: https://www.quuppa.com/industry-4-0/?gclid=Cj0KCQiAm5ycBhCXARI sAPldzoWU20ocJRPYn64SA4xbl_dJgOXqvXcCHd96pTFxRRYJMibIFGEu-7EaAmzaEALw_wcB – Назва з екрану. – Дата звернення: 10.11.2022

10. V. F. Shangin, Informatsionnaya bezopasnost [Information Security]. Moscow, Russia: DMK Press, 2014.

11. Кулаков Ю.О. Комп'ютерні мережі / Ю.О. Кулаков – Юніор, 2005. – 397 с.

12. Вишневський В. М. Теоретичні основи проектування комп'ютерних мереж / В. М. Вишневський – Техносфера, 2004. – 512 с.

13. Amobile solutions [Електронний ресурс]. – Режим доступу: https://www.amobile-solutions.com/en/?gclid=Cj0KCQiAm5ycBhCXAR IsAPldzoXq_gttAexROGuPD1BpFlttz_iRWPHwGHfJYkZCsHITrnzAGp00qRwa AkK_EALw_wcB – Назва з екрану. – Дата звернення: 11.11.2022

14. Digital transformation in manufacturing [Електронний ресурс]. – Режим доступу: https://blogs.cisco.com/manufacturing/how-is-digital-transformation-in-manufacturing-bridging-the-gap-to-productivity-security-resiliency-and-sustainability – Назва з екрану. – Дата звернення: 11.11.2022

15. Internet of Things [Електронний ресурс]. – Режим доступу: https://blogs.cisco.com/internet-of-things/modern-manufacturing-does-your-network-have-what-it-takes – Назва з екрану. – Дата звернення: 15.11.2022

17. Drath, R. Horch, A. “Industrie 4.0 Hit or Hype? IEEE Industrial Electronics Magazine.” June 2014, 56–58.

18. Беркман Л. Н. Архітектурна концепція побудови, принцип реалізації, ефективність застосування інтелектуальної телекомунікаційної мережі / Л. Н. Беркман, С. В. Толюпа // Зб. наук. праць ВІТІ НТУУ ―КПІ‖. – 2007. – №3. – С. 9-17.

19. Колченко В. О. Впровадження інтелекту в мережі наступного покоління (NGN) – перехід до мереж майбутнього покоління (FGN) / В. О. Колченко / Наукові записки УНДІЗ. – 2010. – №2(14). – С.80-85.

20. Беркман Л. Н. Проблеми створення сучасної конвергентної мережі на базі концепції FMC (Fixed-Mobile Convergence) / Л. Н. Беркман, О. І. Чумак, В. В. Григорович, П. Ю. Дещинський // Вісник УНДІЗ. – 2008. – №2. – С. 61-63.

21. Толюпа С. В. Структура інформаційної мережі та показники її ефективності / С. В. Толюпа, А. В. Сухін. // Зб. наук. праць КВІУЗ. – 2001. – №3. – С. 68-73.

22. Гребенніков В. О. Проблема загальнодоступності основних телекомунікаційних і інформаційних послуг в Україні та загальні підходи до її розв’язання / В. О. Гребенніков, Г. Ф. Колченко // Наукові записки УНДІЗ. – 2013. № 1(25). – С. 5-13.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

Автоматизація виробничих процесів за допомогою інтернету речей (IoT)

Виконав - Бондік Мирослав Дмитрович
Керівник роботи - К.ф.-м.н. Нафєєв Ровіл Касимович

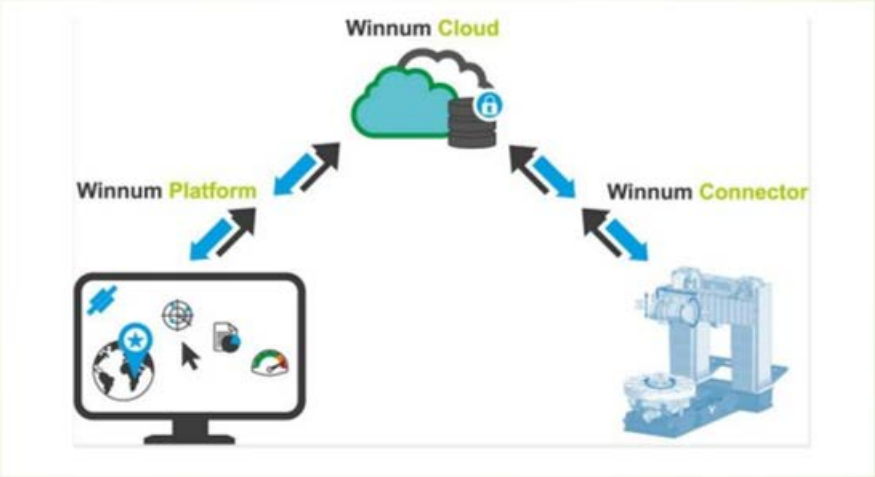
Актуальність

Автоматизація виробництва є актуальною задачею, яка вирішує ряд важливих проблем – це зниження ручної праці, мінімізація впливу «людського фактору» на якість готової продукції і виробничий процес, зниження частки браку при виробництві та зниження собівартості готової продукції. Існує безліч рішень, які допомагають автоматизувати виробництво серед яких перспективним є «Інтернет речей», за рахунок якого можна підвищити ефективність виробництва в кілька разів при незначному терміні окупності проектів, що в більшості випадків не перевищує декількох місяців.

МЕТА РОБОТИ - Проаналізувати існуючі системи IoT і технології автоматизації промислового виробництва.

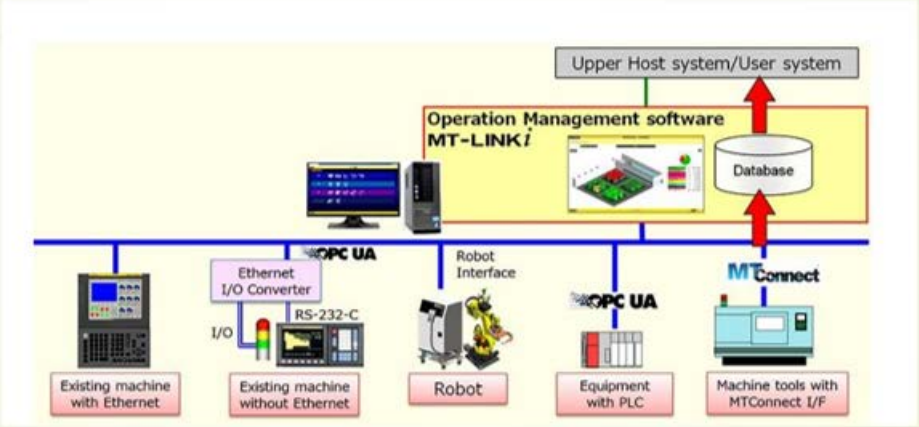
3

Основні програмні компоненти Winnum



4

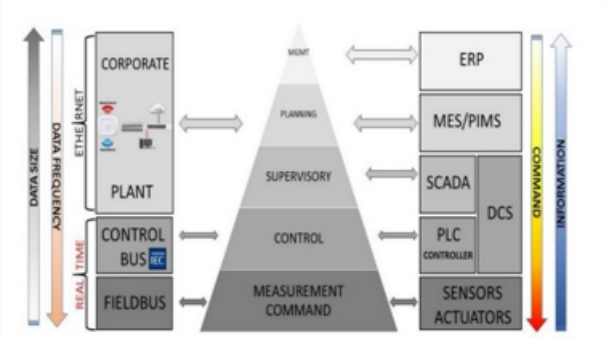
Комунікація на рівні системи MT-LINKi



OPC Unified Architecture (OPC) – специфікація, що визначає передачу даних в промислових мережах і взаємодію пристроїв в цих мережах

5

Ієрархічні рівні системи комплексного автоматизованого виробництва CIM



sensors, actuators– рівень датчиків, перетворювачів виконавчих механізмів;
PLC, DCS – рівень мікроконтролерів, розподілених систем керування або терміналів віддаленого управління мікропроцесорами (Remote terminal unit RTU);
SCADA – рівень систем збору, обробки, відображення та архівування інформації про об'єкт моніторингу або управління в реальному часі через людино-машинний інтерфейс;
MES – рівень синхронізації управління виробничої системи шляхом об'єднання рівнів планування і контролю для оптимізації процесівні ресурсів;
ERP – рівень програмного забезпечення управління та планування діяльністю

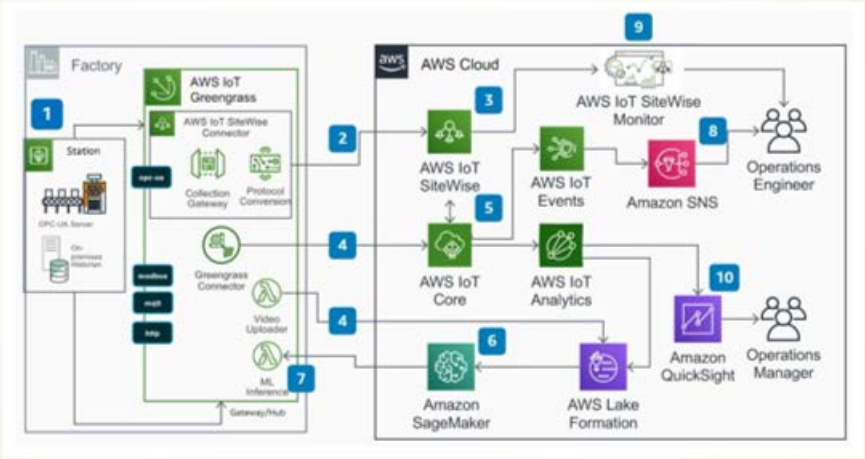
6

Сценарії використання промислового Інтернету речей компанії Amazon

- 1. Аналітика та прогнозування якості продукції і послуг компанії. Згідно даного сценарію, промислова компанія на своїх виробничих лініях повинна інтегрувати IoT у власне обладнання та здійснити підключення до локального сервісу AWS IoT Greengrass, який розміщується на серверах підприємства.
- 2. Архітектура системи моніторингу ресурсів дозволяє збирати дані про стан машин і устаткування, наприклад показники температури, вібрацій, коди помилок, які вказують, чи працює обладнання оптимальним чином та прогнозувати можливості використання ресурсу обладнання та заводу.
- 3. Архітектура система аналітики технічного обслуговування обладнання дозволяє збирати дані про стан промислового обладнання, виявляти потенційні несправності до того, як вони вплинуть на виробництво.

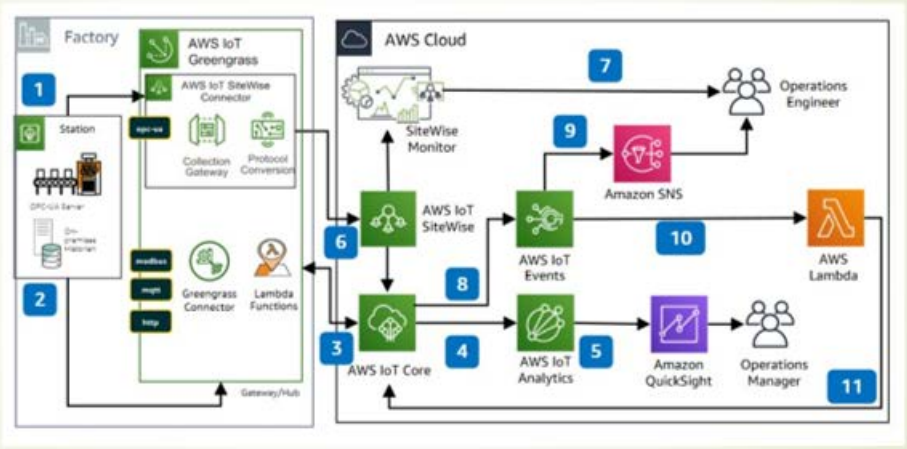
7

Архітектура сервісів AWS Cloud для рішення аналітики та прогнозування



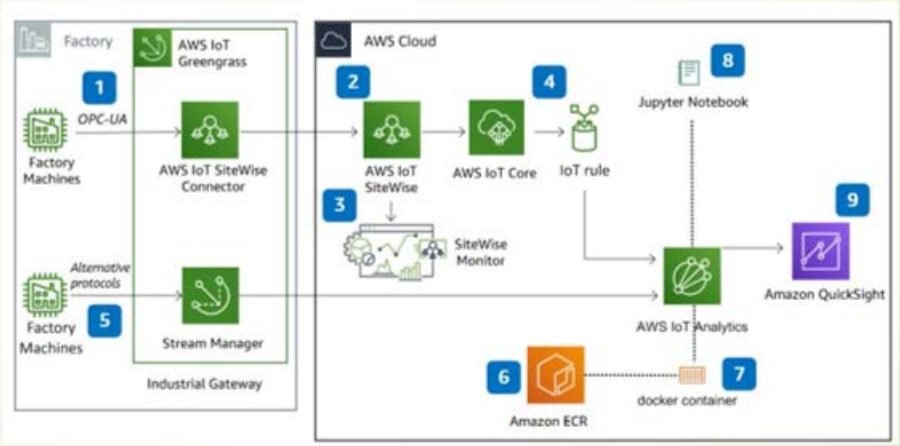
8

Архітектура системи AWS Cloud моніторингу ресурсів



9

Архітектура системи AWS Cloud аналітики технічного обслуговування



10

Висновки

Проведений аналіз розробок систем IoT дає підстави стверджувати, що для застосування подібних рішень в промислових системах потребує реалізації підключення промислового обладнання до засобів комунікації з Internet протоколами або з протоколами систем автоматики, як наприклад MQTT протокол. В подальшому таке обладнання легко підключається до готових промислових захищених сервісів.